Journal of Multidisciplinary Innovations and Perspectives (JMIP)
ISSN: 3141-2319; **EISSN:** 3141-2300
www.fedpodjournal.com
Volume 3; Issue 1; June 2026; Page No. 1-12.

Development of a Zero -Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications.

BARTHOLOMEW IDOKO[1], HARRISSON ALI[2], ANDREW ADAMA[3]
[1,2]Department of Computer Science, Federal Polytechnic Ohodo, Enugu-Nigeria.
[3]Department of Computer Science, Imo State University, Owerri-Nigeria.
bartholomew.idoko@fedpod.edu.ng

Abstract:
IoT continue to gain momentum, and its application has widened since the concept was coined . Industries, businesses and homes are interminably adopting the deployment and application of IoT. Recent research has attributed the wide application of IoT in agriculture, environmental management and monitoring, industries, healthcare and smart homes to the low cost of sensors and relevant technologies. Application of IoT has made information sharing and communication from machine to machine (M2M) easier. Devices can now be connected to the internet along with sensors to monitor and report plant growth, pest infestation, and condition of animals. In the healthcare IoT application, wearable sensors are connected via wireless communication to the patients' mobile device to collect and share data with healthcare practitioners or care providers. Several security challenges arose from the proliferation of devices and interconnection of things. However, an identity of things (IDoT) management approach is necessary to provide each device or thing with a unique identifier. The study proposed a robust and acceptable security framework that manages, categorizes and recognises identities of things in the IoT paradigm with a single solution. This solution involves combining different frameworks that enable the identification of objects within the IoT environment due to differences in types and architecture of various things that are interconnected. Data from primary sources were extrapolated. Extrapolated data sets are, sensors names, communication methods in eHealth IoT architectures in the deployment of healthcare sensors, vulnerabilities that sensors and communication networks possess, threats to sensors and networks and a list of potential or reported attacks to sensor resources (data and physical attack).

Keywords: IoT, Trust; Security; Application, Frameworks.

1. Introduction

The age of Information and Communication Technology has paved way for several breakthroughs and innovations in developing, designing and producing devices, things and objects. As the number of these devices continues to grow, there is need to harness their individual capabilities to optimize the maximum advantage that could be derived from these connections; this concept is known as "Internet of Things" (IoT). IoT refers to the interconnection of devices, vehicles, sensors, buildings and other things within a physical network to collect exchange and communicate data from one machine to machine (M2M). IoT is the interconnection of uniquely identifiable devices, objects, actuators and other embedded computing devices which are within an internet infrastructure (Choi, 2024). Similarly, research has shown that the concept of Internet of Things aims to integrate communication of heterogeneous technologies both wired and wireless (Kortuem, et al., 2020; Mainetti, et al., 2021).

Cite this article as:
Idoko, B. et al. (2026). Developing of a Zero-Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications. *Journal of Multidisciplinary Innovations and Perspectives (JMIP), 3*(1) 1- 12.

Challenges within the IDoT are existential and acts as a de facto to other challenges in IoT. IDoT faces series of challenges including but not limited to ownership and the identity relationship, object identification and name spacing, authentication and verification and device to device identification (Friese, et al., 2014). While IoT boast connections of things on a scalable figure of billions of connections, the conventional naming policy will not be able to accommodate the wide variety of connected devices (Zhang, et al., 2025). The ability of a device to identify another device within or outside its security boundaries with a more adaptable naming system for Identifying things is still an open research issue (Gofwen et al., 2023).

IoT adoption by most developed nations has been applied to the Healthcare service by managing and improving patients' wellbeing. The application of IoT in healthcare is mostly referred to as eHealth which involves using sensors (mostly wearable) with devices (mobile-with internet connection) to monitor patients' sugar level, insulin level, heartbeat etc. which has greatly improved the treatment of cardiovascular diseases in elderly patients. The sensors collect data regarding patients' wellbeing and communicate it to a data reservoir usually managed by a hospital or clinic (Idoko et al., 2025).

With the advantages derived from the application of IoT in eHealth, it poses a lot of concerns to patients as to the data collected and transferred through unsecured communication channels and protocols which requires some security measures to be deployed to ensure data confidentiality, integrity, availability, nonrepudiation and preferential anonymous preservation (Gofwen et al., 2023). Privacy preservation has been identified as one of the critical areas in IoT that needs attention to research and design efficient authentication methods as well as a well-designed cryptographic mechanism for the security of data shared among things in a healthcare scenario (Zhang, et al., 2025).

The Zero trust network or zero knowledge proof approach works with a "never trust, always verify" approach (Gofwen et al., 2023). The level of trust devices and things place on each other has created vulnerable path for threats and attacks to be launched which compromises the security of sensitive data. Currently, the deployment of IoT devices relies on various trust frameworks in defining trustworthiness of things and humans in the context of allowing smart objects take decisions and trust an entity which has seen a number so-called fine-grained trust negotiation mechanisms developed (Miorandi, et al., 2025).

Assigning sensors within the eHealth application a Unique Identifier (UI) has been a research challenge to the application of IoT in various environments (Gofwen et al., 2023). However, an identity management approach that can accommodate sensors with different peculiarity is therefore imperative to this research as well as a Zero-Trust approach to further enhance security and privacy of data over the internet and vulnerable transport layer protocols.

2. Empirical Review

Cite this article as:
Idoko, B. et al. (2026). Developing of a Zero-Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications. *Journal of Multidisciplinary Innovations and Perspectives (JMIP), 3*(1) 1- 12.

One of the approaches used in balancing level of aggregation is the k-anonymity privacy-preserved aggregation for published data that is in wide usage in that it provides a degree of secrecy that individual's identity cannot recognized in a set of k users by anonymizing data (Chabridon, 2014). The design of their approach EEXCESS which provides data preferential anonymity and privacy preservation consist of content anonymity which guarantees data privacy be it that in an event of attack, the identity of the data provider should not be gained by an attacker, request unlinkability to maintain user privacy making it impossible to link two or more independent data from originating request and origin unlinkability to hide the origin of a request and not revealed by application level protocol. (Chabridon, 2014) Extended anonymity to include communication process by ensuring the identity of various communicating parties in a communication protocol and traffic is concealed. However, k-anonymity location-based privacy model fails to provide users' preferential query requirement due to its reliance on dynamic users' distribution (Chabridon, 2014; Ni, et al., 2016). In their proposed solution for preserving location privacy the authors argued that the solution display high scalability with (s, e)-anonymity model specifically and location protection as against other cloaking solutions such as the Casper architecture which achieve location privacy preservation queries by emulating a brute-force approach resulting to a high workload and scalability of deployment (Gofwen et al., 2023).

An experiment to measure the accuracy of security on data communicated over Wireless Sensor Networks (WSN) within IoT implementation has been performed (Fisher, et al., 2016). The experiment adopted two popular encryption algorithms to achieve this desired results (i.e. Elliptic Curve Diffie-Hellman (ECDH) and Integrated Factorization Scheme (IFES) algorithms). As proved in their experiments, the ECDH algorithm provides some high-level security due to the mathematical operations required to implement key generation for two communicating parties within a network which makes it difficult for attackers to calculate the key pair required for the communication even if they monitor the communication channel. On the other hand, the IFES algorithm operates in the same way with RSA encryption algorithm as for any communication to materialize, the sender must generate a public key to encrypt data to be transmitted (which is shared with the receiver) and a private key to decrypt the data and so also the receiver must generate both a public key and private key. Though with the level of security these two algorithms provide, it lacks an overarching application to the sort of devices in a WSN such as RFIDs (Perera, et al., 2025; Hasan, 2023).

The low computational power of embedded devices and microprocessors in some IoT devices plays an important role in the usage of internet infrastructure and information exchange in the field of IoT. Thus, draws the need for algorithms to facilitate a secure information exchange for things with low computational capability (Kumar, et al., 2015). It is worthwhile to mention that though a number of novel and already existing algorithms (implemented on a few platforms) have been introduced and are being tested for a wide coverage of use in the environment of IoT, there is still more to be done as a result of the growing privacy and security concerns to the sensitive data collected

Cite this article as:
Idoko, B. et al. (2026). Developing of a Zero-Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications. *Journal of Multidisciplinary Innovations and Perspectives (JMIP), 3*(1) 1- 12.

within the usage and deployment environment of IoT (Gofwen et al., 2023). The deployment of a scalable identity management approach to enable sensors without IP capabilities to be identified precisely and a network architecture that will enable sensors and other devices within its deployment to operate a two-way authentication process that must always verify each other before a transmission or any exchange of data takes place. Secondly, the identification of Sensors and Actuators in eHealth has been a thing of great concern and as such a need for zero trust in IoT networks.

3. Methodology

A hybrid research methodology precisely the dominant-less-dominant research methodology is implemented in this study to investigate and identify challenges and approaches related to data security and communication between M2M in eHealth IoT adoption. The choice of this design method is to explicitly present findings as investigated in the study. Hybrid research methodology compliments the weaknesses of either quantitative or qualitative analysis methodology (Gray, 2024). The proposed model incorporates stages of carrying out the assessment similar to other researchers and that of the standard model but specifies the model on IoT paradigm and more precisely in eHealth application (Atamli & Martin , 2024; ISO/IEC, 2021). The proposed lightweight PriMa risk assessment is categorised into four phases as shown in figure 1.

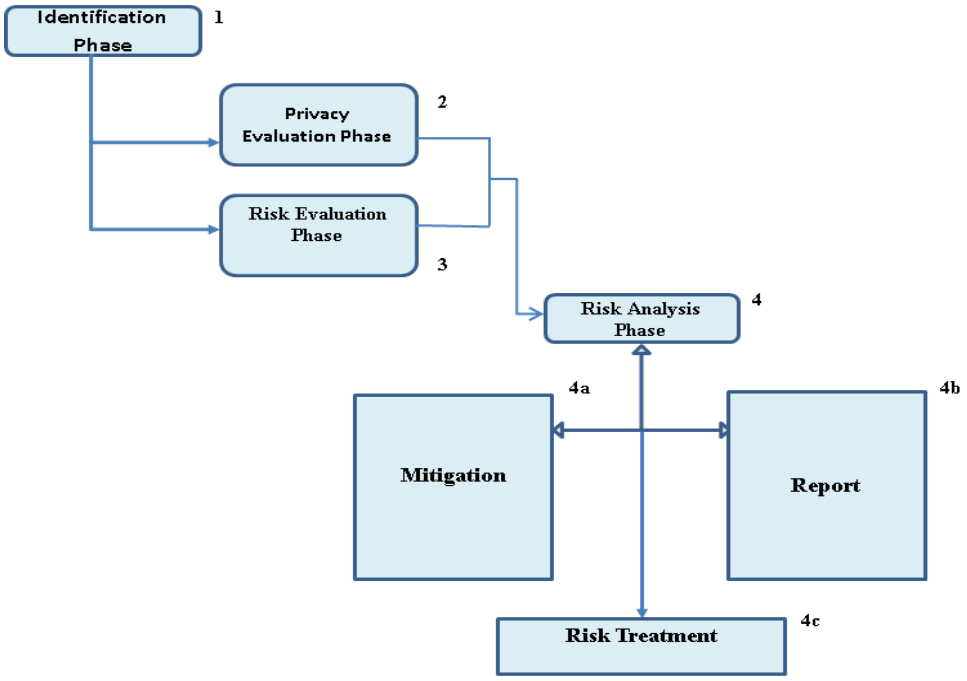

Figure 1: The proposed system Architecture

Phase 1: Identification phase

Phase 2: Privacy Evaluation Phase

Cite this article as:
Idoko, B. et al. (2026). Developing of a Zero-Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications. *Journal of Multidisciplinary Innovations and Perspectives (JMIP), 3*(1) 1- 12.

Phase 3: Risk Evaluation Phase

Phase 4: Risk Analysis Phase

3.1 Research Instrument

The Data that was used for the study is mainly secondary data from columns, health statistics, websites of healthcare providers (manufactures of sensor devices, hospitals, clinics, and care homes), vulnerability database, blogs and data from other publications.

3.2 Sampling Technique

The inclusion criteria are; reported sensor nodes, devices and network vulnerabilities and threats, list of various sensor nodes for monitoring vital signs in the eHealth IoT application and network architectures (communication protocols and principles) from selected sources was used.

3.3 Data Processing and Analysis

The data collected was used to perform a risk assessment of sensor nodes with known vulnerabilities and threats associated with the deployment of sensors in healthcare industry. The result is presented using tables identifying sensors, networks, things, vulnerabilities, and threats so as to test the performance of the proposed PriMa risk assessment model.

3.4 Validation Techniques

The model was tested using data collected from secondary sources to validate the output of the lightweight model in performing a risk assessment in the deployment of IoT in the healthcare environment.

4. Model Development and Implementation

Phase 1- Identification: The first phase identifies the required information to begin assessing risk associated with the deployment of sensors and other things in an IoT context such as; assets identification threat identification and associated Vulnerability Identification

Assets Identification: This involves identifying assets in eHealth deployment. The assets identification covers tangible to intangible objects, things and nodes. In this model, an asset can be classified valuable under a number of criteria which include the sort of data collected and communicated and the privacy protection that must be assigned to the data or data set. This translates assessing each sensory note, network, communication gateway and protocol and database on the sensitivity of content held or transmitted (data) and performance requirement of assets. The asset value is the quantitative scoring scale based on the trust level assigned to assets to communicate with other devices within and outside the BAN parameters indicating the sensitivity of assets value with the following dependencies;

i. Service interruption – Availability
ii. Confidentiality properties
iii. Integrity properties
iv. Privacy maintainability
v. Preferential anonymity preservation

Threat Identification: Threats associated to the deployment of sensor nodes are identified. The treat identification involves collecting information about reported threats in the past (threat history) and also information gathered from reporting forums of threats. Adopting [42], the threat model classifies the threats causes into either one or combination of the following; deliberate (D), accidental (a). Deliberate actions that are targeted at gaining unauthorised access to data while accidental actions are considered to me human related resulting from oversight and negligence that will result to destroying data or sensors nodes and associated valuable resources.

Cite this article as:
Idoko, B. et al. (2026). Developing of a Zero-Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications. *Journal of Multidisciplinary Innovations and Perspectives (JMIP), 3*(1) 1- 12.

Identification of Vulnerabilities: This stage involves identifying [43] of WSN, sensor nodes and databases which are reported in online databases and users experience to the deployment of sensors. This stage follows similar procedures to identifying threats stage.

Phase 2- Privacy Evaluation Phase: This phase determines the privacy requirements of each sensor node, device, communication protocols and gateways on an individual level. This phase provides information as to what aspect of privacy is exposed. This phase targets on Privacy maintainability and sensors privacy requirements (anonymity preservation which could be in form of location hiding from unauthorised access, an intercepted/stolen data or data set should not be tied to a particular individual) are determined with a Privacy impact matrix (calculated as critical outcome resulting from privacy violation against sensitivity of data or sensory nodes) as shown in the figure 2.

CRITICALITY	SENSITIVITY								
	Low	Medium	High	Low	Medium	High	Low	Medium	High
Very Low	0	1	2	1	2	3	2	3	4
Low	1	2	3	2	3	4	3	4	5
Medium	2	3	4	3	4	5	4	5	6
High	3	4	5	4	5	6	5	6	7
Highly Critical	4	5	6	5	6	7	6	7	8

SCORE

Privacy Violation 0 - 2 = Low

Privacy Violation 3 - 5 = Medium

Privacy Violation 6 - 8 = High

Figure 2: Quantitative Privacy Impact Matrix

Phase 3: Risk Evaluation: The risk evaluation phase is determined by calculating the impact that vulnerabilities and threats could have on an asset through a risk matrix. The matrix is assigned quantitative values to measure the consequences a threat and vulnerability could pose against the likelihood of its occurrence which is described as the profiling of a risk. The consequence of a threat or vulnerability is considered from the loophole's sensors, networks and communication protocols or gateways have when deployed and the likelihood of those threats and vulnerabilities being exploited (using historical data and reports that actually occurred). This is illustrated in figure 3.

LIKELIHOOD	CONSEQUENCE								
	Low	Medium	High	Low	Medium	High	Low	Medium	High
Low	0	1	2	1	2	3			
Medium	1	2	3	2	3	4			
Hligh	2	3	4	3	4	5			
Very High	3	4	5	4	5	6			
Critical	4	5	6	5	6	7			

SCORE

Privacy Violation 0 - 2 = Low

Privacy Violation 3 - 5 = Medium

Privacy Violation 6 - 8 = High

Figure 3: Quantitative risk impact matrix

Cite this article as:
Idoko, B. et al. (2026). Developing of a Zero-Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications. *Journal of Multidisciplinary Innovations and Perspectives (JMIP), 3*(1) 1- 12.

Phase 4: Risk Analysis: The risk analysis phase presents the overall assets and their values, threats to individual asset, vulnerabilities appropriately linking it to an asset(s), CIA (Confidentiality, Integrity and Availability) violation, Risk score (mean of privacy impact and risk impact). The risk analysis will be registered in the table below.

Table 1: Risk analysis

set	reat	lnerability	A Violation			sk Score
			fidentiality	grity	ilability	*an score of privacy impact and risk impact(pi+ri/2)*

To carry out an extensive risk analysis, factors such as Mitigation, reporting and risk treatment was considered;

Mitigation: critically presenting steps and methods to take to prevent, minimize or avoid the impact of an attack/ threat to sensor nodes and other resources in the eHealth deployment. Mitigation to the threats identified in the first phase of the model will be presented and analysed in the next session.

Report: Parties involved with the usage, collection, handling, designing and manufacturing of sensors and other things should be notified of results of the risk assessment.

Risk Treatment: Risk in the deployment of sensors and other things can be owned, rejected or transferred to relevant third parties. Owning the risk requires employing necessary measures to control the risk and residual outcome.

5. Results

The risk evaluation provides scores to risk associated with each asset. Assets risks are presented in the form of likelihood and consequences. The vulnerabilities and threats identified are mapped to asset (eminent or by historical data and risk profile). The Risk score is the mean value of privacy impact score and risk impact score as illustrated in table 2.

Table 2: Risk analysis and evaluation

Asset		Threat	Vulnerability	CIA Violation	Risk Score

Cite this article as:
Idoko, B. et al. (2026). Developing of a Zero-Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications. *Journal of Multıdıscıplınary Innovatıons and Perspectıves (JMIP), 3*(1) 1- 12.

				Confidentiality	Integrity	Availability	*Mean average score of privacy impact and risk impact(pi+ri/2)*
ADAMM		Location discovery, DoS	Unpatched software	s	s	Y	pi = 8, ri = 6 8+6/2 = 7
HELIUS		Man-in-the middle, WNS routing	Unpatched software, weak encryption		s	Y	pi = 8, ri = 8 8+8/2 = 8
ITBRA		Man-in-the, DoS, Physicat tempering	Weak encryption		s	Y	pi = 5, ri = 3 5+3/2 = 4
rdioCore		Man-in the middle, location discovery, DoS,	Node capturing, weak encryption, unpatched software	s	s	Y	pi = 8, ri = 8 8+8/2 = 8
Google Contact Smart Lens		DoS, Man-in-the middle attack	Protocol level capturing	s	s	Y	pi = 5, ri = 5 5+5/2 = 5
Mobile devices		Man-in-the middle	Physical security, Unpat	s	s	Y	pi = 7, ri = 8 8+6/2 =

Cite this article as:
Idoko, B. et al. (2026). Developing of a Zero-Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications. *Journal of Multıdıscıplınary Innovatıons and Perspectıves (JMIP), 3*(1) 1- 12.

		attack, WNS routing, Location Discovery	ched system, physical security				7.5
CGM		DoS, Man-in-the middle attack, location discovery	Privilege escalation, weak encryption algorithm		s	Y	pi = 8, ri = 8 8+8/2 = 8
Communication Networks (WBAN, WSN, Mobile Network, Hospital Network)		WNS routing, DoS, WSN packet routing, Session hijacking, Network Injection	Privilege escalation, Physical security, protocol level capturing	s		Y	pi = 6, ri = 5 6+5/2 = 5.5
Protocols (ZigBee, Bluetooth, MICS)		WNS routing, DoS, Man-in-the middle atack	Protocol Level capturing	s	s	Y	pi = 6, ri = 6 6+6/2 = 6

6. Conclusion

The study analyses and presents data collected from various secondary and primary sources relating to the ehealth devices. The proposed lightweight model was tested with the data collected and findings reported accordingly. Data from primary sources were extrapolated. Extrapolated data sets are, sensors names, communication methods in

Cite this article as:
Idoko, B. et al. (2026). Developing of a Zero-Trust Risk-Framework for IoT Security: Ensuring Security of eHealth Devices and Applications. *Journal of Multıdıscıplınary Innovatıons and Perspectıves (JMIP), 3*(1) 1- 12.

eHealth IoT architectures in the deployment of healthcare sensors, vulnerabilities that sensors and communication networks possess, threats to sensors and networks and a list of potential or reported attacks to sensor resources (data and physical attack).

There are wide ranges of sensor and actuators nodes, devices and networks designed and deployed for use in the healthcare industry and all perform various purpose in monitoring key vitals and carrying out specific functions at predetermined times (also when sensors triggers an abnormality in body activities) and wellness progress in hospitals, clinics and some care homes. The assets identified in this stage are categorised into; Sensor and actuator nodes/devices and systems and Communication Networks and Protocols. The risk associated to the aforementioned sensors after carrying out the risk assessment using the proposed PriMa model were reported to relevant stakeholders involved with the deployment. The stakeholders are the users (patients) of the sensors, healthcare providers, care homes and manufactures of the sensors.

The risk associated with the application of these sensors were managed by patients who are in charge of reporting any loss or damage to the healthcare provider. Software issues regarding security and key privacy violations were relayed to manufactures to design more sophisticated update to curb any threat or noticeable vulnerability. Issues regarding privacy violation risks is to be shared between healthcare providers and sensor manufactures.

Acknowledgement
The author would like to acknowledge the Tertiary Education Trust Fund (TETFUND) Nigeria for providing the funds for the institution-based research (IBR).

References
Al Ameen, M., Liu, J. & Kwak, K. (2022). Security and Privacy Issues in Wireless Sensor

Networks for Healthcare Applications. *Journal of medical systems,* 36(1), pp. 93-101.

Atamli, A. W. & Martin, A. (2024). Threat-based Security Analysis for the Internet of Things.

International Workshop on Secure Internet of Things, pp. 35-43.

Borgia, E. (2016). Special issue on "Internet of Things: Research challenges and Solutions".

Computer Communications.

Chabridon, S. 2014. A survey on addressing privacy together with quality of context for context

management in the Internet of Things. *annals of telecommunications,* 69(1-2), pp. 47-62.

Choi, A. (2024). Internet of Things: Evolution towards a hyperconected society. *Solid-State*

Circuits Conference (A-SSCC), IEEE Asian, pp. 5-8.

Francis, T., Madiajagan, M. & Kumar, V. (2015). Privacy Issues and Techniques in E-Health

Systems. *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research ACM,* pp. 113-115.

Doukas, C. (2022). Enabling Data Protection through PKI encryption in IoT m-Health Devices.

12th International Conference on Bioinformatics & Bioengineering (BIBE) IEEE , pp. 25-29.

Fisher, R., Lyu, M., Cheng, B. & Hancke, G. (2016). Public Key Cryptography: Feasible for

Security in Modern Personal Area Sensor Networks? *IEEE International Conference on Industrial Technology (ICIT),* pp. 2020-2025.

Friese, I., Heuer, J. & Kong, N. (2014). Challenges from Identities of Things- Introduction of

the Identities of Things Discussion Group within Kantara Initiative. *IEEE World Forum on Internet of Things (WF-IoT).*

Gofwen, M., Idoko, B., Idoko, J. (2023): Application of Zero-Trust Networks in e-Health

Internet of things (IoT) Deployment. Machine Learning and Internet of Things in Education: Models and Applications. Pp.209-233 © 2023 Springer Nature.

Gray, D. E. (2024). *Doing research in the real world.* 3rd ed. London: Sage.

Hasan, O. (2023). A Discussion of Privacy Challenges in User Profiling with Big Data

Techniques: The EEXCESS Use Case. *IEEE International Congress on Big Data,* pp. 25-30.

Idoko, B., Okoro, D., Agada, S., Olofu, S. (2025): Detection of Malware Attacks in Medical

Mechatronics Distribution System Using Support Vector Machine. Africa Multidisciplinary Journal of sciences and Artificial Intelligence. Volume 2, Issue 3, Pp 466-477. https://doi.org/10.58578/AMJSAI.v2i3.7231

ISO/IEC, 2021. *Information security risk management technical report ISO/IEC 27005:2021,*

Washington DC: International Organization for Standardization.

Kortuem, G., Kawsar, F., Sundramoorthy, V. & Fitton, D. (20200. Smart objects as building

blocks for the Internet of Things. *IEEE Internet Computing,* 14(1), pp. 44-51.

Kraijak, S. & Tuwanut, P. (2015). A Survey on Internet of Things Architecture, Protocols,

Possible Application, Security, Privacy, Real-World Implementation and Future Trends. *International Conference on Communication Technology (ICCT) IEEE,* pp. 26-31.

Kumar, U., Borgohain, T. & Sanyal, S. (2015). Comparative Analysis of Cryptography Library

in IoT. *International Conference on Communication Technology (ICCT) IEEE,* pp. 52-61.

Matharu, G. S., Upadhyay, P. & Chaudhary, L. (2024). The Internet of Things: Challenges &

Security Issues. *International Conference on Emerging Technologies (ICET) IEEE,* pp. 54-59.

Mainetti, L., Patrono, L. & Vilei, A. (2021). Evolution of Wireless Sensor Networks towards

the Internet of Things: A Survey. *Software Telecommunications and Computer Networks (SoftCOM),* pp. 1-6.

Mcdonald, N. (2016). Biometric Data Emulation and Encryption for Sport Wearable

Devices (A Case Study). *Annual IEEE Systems Conference (SysCon) IEEE,* pp. 1-6.

Miorandi, D., Sicar, S., Pellegrini, D. F. & Chlamtac, I. (2025). Internet of things: Vision,

applications and research challenges. *Ad Hoc Networks 10,* p. 1497–1516.

Ni, W., Gu, M. & Chen, X. (2016). Location privacy-preserving k nearest neighbor query under

user's preference. *Knowledge-Based Systems,* Volume 103, pp. 19-27.

Perera, C., Ranjan, R. & Wang, L. (2025). End-to-End Privacy for Open Big Data Markets.

IEEE Cloud Computing, 2(4), pp. 44-53.

Singh, S. & Singh, N. (2015). Internet of Things (IoT): Security Challenges, Business

Opportunities and Reference Architecture for E-commerce. *International Conference on Green Computing and Internet of Things (ICGCIoT) IEEE,* pp. 1577-1581.

Yao, X., Chen, Z. & Tian, Y. (2015). A lightwirght attribute-based encryption scheme for the Internt of Things. *Future Generation Computer Systems,* Volume 49, pp. 104-112.

Zhang, Z.-K., Cho, M. C. & Shieh, S. (2025). Emerging Security Threats and Countermeasures in IoT. *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security,* pp. 1-6.