Check for updates

OPEN ACCESS

Volume: 4

Issue: Special Issue 1

Month: April

Year: 2025

ISSN: 2583-7117

Citation:

Mukesh Kumar, Dr. Navin Kumar “Exploring the Opportunities, Security Vulnerabilities, and Privacy Risks in Edge-Centric Health Monitoring Systems” International Journal of Innovations in Science Engineering and Management, vol. 4, no. Special Issue 1, 2025, pp. 66–72.

DOI:

10.69968/ijisem.2025v4si166-72

Exploring the Opportunities, Security Vulnerabilities, and Privacy Risks in Edge-Centric Health Monitoring Systems

Mukesh Kumar[1], Dr. Navin Kumar[2]

[1]Research Scholar, Department of Computer Science, Capital University, Koderma, Jharkhand
[2]Associate Professor, Department of Computer Science, Capital University, Koderma, Jharkhand.

Abstract
Human civilization has always been inventing new technologies that can make its way of living comfortable, efficient, and useful. Healthcare, smart homes, entertainment, transportation, education, and other industries have all adopted the Internet of Things (IoT). In recent years, there have been a lot of inventions in technology that have significantly transformed the healthcare sector. It has enabled more efficient, accurate, and real-time patient monitoring. The exponential growth of IoT wearable devices leads to the requirement to process results in real time and a better way to store data. However, the significant increase in IoT devices and the large amount of data they generate at the network's edge have added extra challenges that conventional cloud architecture with central repository is not able to handle properly. As a consequence, the Internet of Things (IoT) based on Edge Computing (EC) is evolving into a contemporary approach that provides storage and processing of data for near end users. It results in real-time response and the patient's life could be saved in critical situations. It has opened new avenues for continuous health monitoring, data collection, and analysis through the employment of various wearable devices. This paradigm presents significant privacy and security of data threats in addition to its distinctive characteristics and enhanced quality of service. Because location and health data are sensitive, it is critical to ensure that users have a high degree of security. In this paper, I have tried to conduct a comprehensive investigation into security and privacy issues in the context of Edge based health monitoring system, and explored possible solutions.

Keywords; IoT, Edge Computing (EC), Wearable Devices, Security and Privacy Risk.

INTRODUCTION

With the help of software, sensors, and other technologies, a vast network of linked objects called "the Internet of Things (IoT)" can gather and share data over the web. In recent years, the efficient integration of the IoT with healthcare systems has brought new avenues for continuous health monitoring. The IoT architecture for healthcare is a multi-layered architecture designed to ensure efficient data collection, data processing, data analysis, and secure transmission to enhance patient care [1]. The major components of multi-layered architecture are as following:

I. **Device Layer:** It includes wearable technology to measure vital indicators, including fitness trackers, smartwatches, and other sensors.

II. **Network Protocol Layer:** Numerous communication technologies, including Bluetooth, Wi-Fi, LTE, and Zigbee, are included. Connectivity to edge servers or the cloud is guaranteed to be seamless and effective.

III. **Cloud Computing Layer:** It consists of centralized cloud servers that provide scalable storage and computational power for data processing and analysis.

IV. **Application Layer:** It consists of user interfaces for healthcare providers, patients, and others to interact with the system.

V. **Security and Privacy Layer:** In order to encrypt data while transmission and storage, it is composed of a variety of mechanisms and algorithms.

These devices collect real-time data on vital signs such as glucose levels, heart rates, and other critical health metrics, and allow healthcare providers for real time interventions and more accurate diagnoses. The data may be accessed and evaluated from the cloud, which is typically linked to the wearable sensor device [Figure 1.1].

Once data is collected, it undergoes processing and analysis to extract valuable insights. Wireless networks might link medical sensors to external gateways, allowing all medical personnel to access data saved in the cloud. A significant section of India's population resides in rural regions with little regular access to high-quality medical care. IoT-based patient health monitoring can bridge this gap by providing remote monitoring and consultations. A research report published by "the Indian Council of Medical Research (ICMR)" estimates that the proportion of fatalities in India attributable to non-communicable diseases (NCDs) increased from 37.9% in 1990 to 61.8% in 2016 . The four main NCDs—diabetes, cancer, cardiovascular diseases (CVDs), and chronic respiratory diseases (CRDs)—are mostly brought on by poor nutrition, sedentary lifestyles, and alcohol and tobacco use. Cardiovascular diseases and hypertension are major concerns among the elderly, with prevalence rates of 34.6% and 32%, respectively. According to a report published by A. Minhas , there are very few hospitals available for such a large population in India. It is essential to address these challenges through improved healthcare infrastructure, policies, and support systems to ensure the elderly population receives adequate and timely medical care. The new paradigm of healthcare is adopting IoT devices.

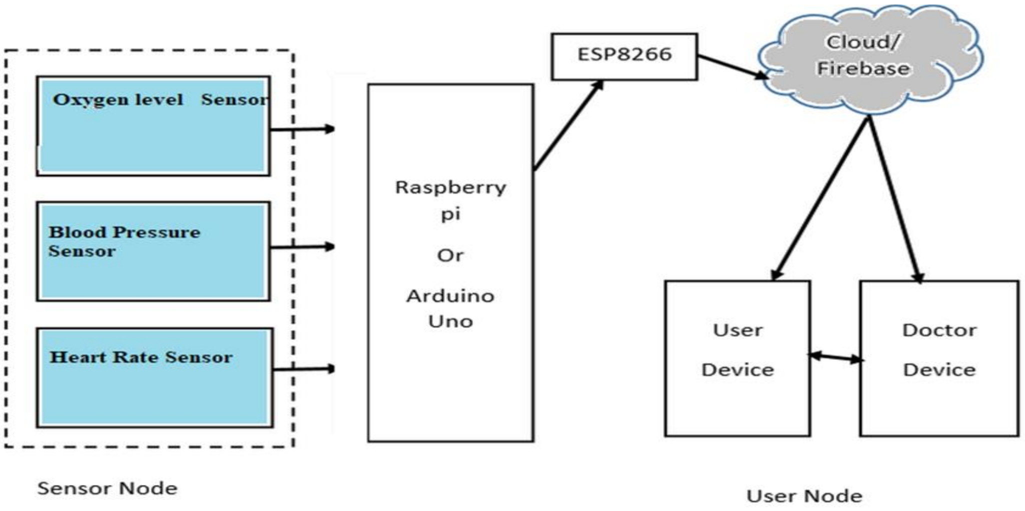

Figure 1.Raspberry Pi model for Health Monitoring System

REAL TIME HEALTH MONITORING WITH EDGE COMPUTING FRAMEWORK

The amount of information generated by IoT devices is massive; hence cloud computing has virtually infinite storage potential to accommodate such loads efficiently. Large datasets may be managed and stored efficiently with the help of cloud storage systems such "Amazon S3, Google Cloud Storage, and Azure Blob Storage". The cloud service providers are responsible for faster analysis and further propagation of data to the concerned people. However, this is not always possible to get everything on time in the case of cloud services [2]. It is anticipated that by 2023, the percentage of Machine-to-Machine (M2M) links would increase from 33% in 2018 to 50%. M2M connections will make up 50% of all connections, with a total of 14.7 billion connections projected . In the M2M category, “Internet of Things (IoT)” devices hold the largest share and are growing rapidly. It may become life-threatening if the system response time is delayed for a few seconds for heart patients. On average, 70-71 milliseconds are required to transfer 1 KB data generated by a sensor with 10 Mbps effective upload speed. Medical sensors generate a vast amount of data. For example, Heart Rate Monitors often collect data around 1 HZ and each heart rate reading might be a single integer, approximately 16-bits (2 bytes).

Therefore,

1 sample/second×2 bytes/sample=2 bytes/second

This indicates that in a day, around "24x60x60x2=172800 bytes of data" must be moved to the cloud storage. It is obvious that patient monitoring needs more such types of sensors or wearables like temperature sensors, fitness trackers, gyroscopes, etc. GPS sensors may also be attached to detect patients' location and exact position. The data generated can vary from a few megabytes to tens or even hundreds of megabytes depending on the number of sensors, their sampling rates, and the specific use case [3]. In Edge-based or Edge-assisted computing everything related to a patient is not transferred to the central repository. Some processing is done at the edge of the network and then only part of the processed data is sent to the central repository. If something related to a patient needs to be responded to in real-time then that information is directly transferred to the connected hospital or doctor through edge computing [Figure 2.1]. By lowering the volume of data transferred between end systems and centralised cloud servers, edge computing increases resource efficiency by bringing "computational and processing resources" close to end users and devices for essential real-time decision-making and data analysis tasks. [4].

Edge based computing doesn't mean to complete removal of cloud storage. Actually, Edge computing is simply placed in between cloud and IoT devices for most efficient use of the whole system [5]. More quickly than traditional technologies, wearable technology may identify irregularities in "blood pressure, heart rate, body temperature, or glucose levels". In edge computing applications, sensor data is often sent across greater distances to a server. Edge computing is transforming the conventional method of data gathering and provides notable benefits such as:

Lower latency: Certain aspects of the system architecture enable edge-based solutions to have a lower latency than standard cloud solutions. The processing of data at the edge leads to the elimination or reduction of data travel.

Reduced cost: In contrast to cloud computing, local area networks provide businesses more "bandwidth and storage" at a cheaper cost when used for data processing.

High Level Security/Privacy: Providing consumers with a high degree of security is crucial since health and location data are sensitive. On edge devices, certain encryption methods utilise less energy than others. Elliptic-curve cryptography (ECC) is a widely used encryption method for smart edge devices.

Model accuracy: For edge use cases that need real-time reaction, healthcare systems depend on high-accuracy models.

Location Awareness: For IoT applications connected to health, location awareness is especially essential since it makes it possible to locate the patient in the event of an emergency.

Wider reach: For conventional cloud computing, it is indispensable to have access to the internet. However, periphery computing does not require internet access to analyse data locally.

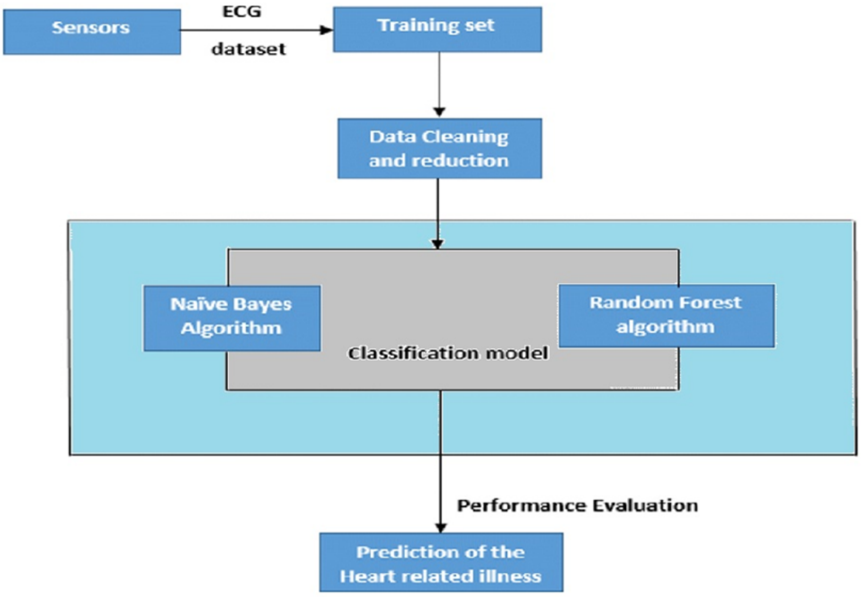

Figure 2. Edge Based Health Monitoring System

WEARABLE DEVICES FOR HEALTH MONITORING

Healthcare providers can use wearable devices for continuous monitoring of patient's health metrics to monitor different health metrics either continuously or periodically [6] [7]. The wearable devices provide personalized data that reflect the unique health status and needs of each user. A medical-grade wristwatch called CardicSense was recently approved by "the Central Drug Standard Control Organisation (CDSCO)", which is part of the Indian Health Ministry. The ECG is the first line of reference for the diagnosis and management of "cardiovascular arrhythmias" like bradycardia and tachycardia. Skin-based devices are wearable technologies designed to capture health parameters directly through the skin. Electronic skins (tattoo) are extensively utilized to detect electrical and physical parameters, including ECG. The ECG is easiest to detect as it has a very high amplitude and can capture electronic frequencies through skin directly. A tattoo-based ECG monitor has electronic components built on graphene [8][9] [Figure 3.1]. It is also possible to get blood pressure reading continuously using graphene-based e- tattoos. The optical transparency and stretchability of graphene are high. Because of this characteristic, it is sufficiently light to appear tattoo-like when engraved on skin. The necessary power could be generated by ultra-thin batteries embedded with tattoos or by techniques such as piezoelectric to convert body movement and heat into electrical energy. The FDA has approved the TempTraq, a Class II medical device that provides healthcare providers with a disposable, soft, and comfortable patch that provides a continuous temperature monitoring solution. There is one more skin patch, FreeStyle Libre, it is the most effective and painless way to monitor blood glucose levels. A very thin patch is applied under your skin, preferably on back of your upper arm, and measures your interstitial fluid. Your blood glucose level can be monitored without having to prick your finger every time. For this purpose, microfluidic devices based on polymers, microfluidic devices based on paper, and microneedles, which are microsized needles, are frequently employed [10]. Sensors that are self-powered, such as piezoelectric nanogenerators (PENG) and triboelectric nanogenerators (TENG) are revolutionizing the healthcare devices [11].

Now I am going to discuss the four main desirable features of wearable devices required for standard healthcare systems:

Wireless Mobility: The wearable gadgets may send data to other gadgets thanks to wireless technologies such Bluetooth, Wi-Fi, and sometimes cellular connection. Patients can wear these devices and move freely without being tethered to stationary equipment.

Interactivity and Intelligence: The wearables must have user interfaces (like touchscreens or physical buttons) that allow users to interact with the device, input data, receive feedback, and adjust settings. The wearable devices are typically designed to be easy to use, with intuitive interfaces and minimal setup required.

Sustainability and Durability: The wearable gadgets necessitate durability and reliability. They must be capable of managing daily wear and tear. The devices are generally water resistant with robust casing and with energy efficient functioning.

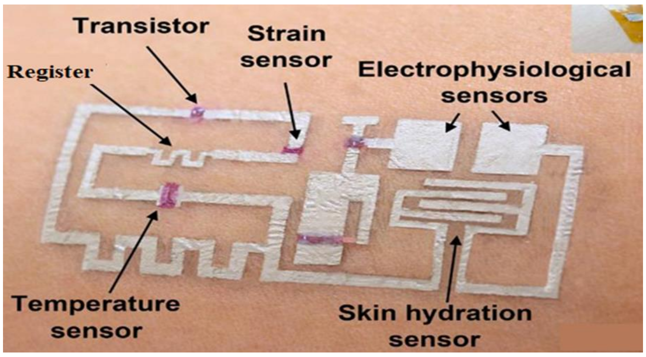

Figure 3.Graphene Tattoo Based Sensors

PRIVACY AND SECURITY CHALLENGES IN EDGE-CENTRIC HEALTH MONITORING SYSTEMS

Edge-Centric (EC) IoT based health monitoring systems offer real-time data analysis and reduced latency, but they also present several security concerns. These systems are the primary target of intrusions, including data breaches, unauthorised access, and ransomware, due to the collection of sensitive health data. By adding false data sets, attackers may potentially alter how EC node machine learning models are trained. The healthcare industry is the most targeted industry for data breaches, with over 470 healthcare breaches reported in 2020, exposing over 37.5 million sensitive records. Due to a hack, the "names, social security numbers, and medical IDs" of around 78.8 million people were made public by Anthem, one of the biggest health insurers in the US. As part of the investigation by the state attorneys general, "Anthem will pay a $39.5 million settlement". The year 2023 witnessed an unrelenting surge in cyberattacks targeting healthcare organizations, resulting in two significant milestones: the highest number of reported data breaches and the largest volume of breached records. During this period, a total of 725 data breaches were reported to the OCR, compromising or unlawfully exposing over 133 million records. Security threats may affect edge-centric IoT-based health monitoring devices at several levels, including the perception, network, and application layers [12].

“Perception Layer”: Data collection via sensors, RFID tags, GPS, and other smart sensors is the responsibility of this layer. Unencrypted data at this layer can be intercepted easily. IoT health devices have limited power supply and resources for processing [13][14]. Encrypting data before transmission may slow down the communication speed.

“Network Layer”: Through the use of communication protocols such Wi-Fi, Bluetooth, Zigbee, NFC, or 5G, this layer manages the transfer of gathered data to additional devices or the cloud. Attackers may intercept data during transmission or disrupt communication by overloading the network (DoS). In medical IoT devices, each device is capable of re-routing and amplifying, and therefore it creates new opportunities for attackers.

Application Layer: User interfaces such as dashboards, mobile applications, or notifications are enabled by this layer, which also processes the data. In this layer, attackers may inject false data to be shown on user’s dashboard. The human factor is also very important at this layer [15][16].

STRENGTHENING SECURITY IN EDGE-CENTRIC IOT DEVICES

Here, I will discuss the strategies and solutions that could be used for security enhancement and to avoid privacy attacks. First, we should detect hardware/software intrusion with edge devices. One such method would be to observe anomalous node activity, such as a notable increase in execution time, power usage, or heat emission. The circuit that recognises trojan activity may also be modified to include a physically unclonable function (PUF). Other mechanisms that could be employed are listed below [17]:

a) Frequent updates for the firmware

b) Authentic and reliable routing protocol

c) Use of energy efficient encryption/decryption techniques especially designed for edge devices

d) Decentralisation of information or even combining edge computing with blockchain technology

e) Multifactor Authentication

Safeguarding Privacy in Edge-Centric IoT Devices

The next bigger concern is related to privacy. Edge devices that constantly monitor our activities can create detailed profiles of our behaviour, preferences, and routines. Data pertaining to health is very sensitive and governed by stringent privacy laws. One notable example of a data leak in India related to health information is the "Aarogya Setu" app incident. In an effort to stop the spread of COVID-19, the Indian government released the Aarogya Setu app in April 2020 as a contact tracking tool. In some of the media publications, it was reported that a security vulnerability in the Aarogya Setu app exposed the personal health data of millions of users. The event sparked worries about the possibility of abuse or illegal access to health-related data stored on digital health platforms, as well as its security and privacy [18]. Manufacturers of health monitoring edge devices should prioritize transparency and provide clear and explicit consent mechanisms.

CONCLUSION

Edge-based healthcare monitoring devices have revolutionized the industry by enabling real-time data analysis, personalized insights, and better patient care. However, these benefits come with security risks that need attention. Protecting sensitive health data is crucial, as these devices can have vulnerabilities that may expose patient information and compromise privacy. Ensuring transparency in data handling, enforcing clear privacy policies, and educating users play a key role in safeguarding edge-based healthcare monitoring devices. Artificial Intelligence (AI) can greatly enhance security by detecting patterns, identifying anomalies, and predicting vulnerabilities in systems. There should be continuous improvements, stronger collaboration, and robust regulations to protect patient privacy and data instead of discouraging the use of such a transformative technology.

REFERENCES

[1] Gulraiz J. Joyia, Rao M. Liaqat, Aftab Farooq, and Saad Rehman, Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain, Journal of Communications Vol. 12, No. 4, April 2017.

[2] Botta, A., De Donato, W., Persico, V., et al.: ‘Integration of cloud computing and internet of things: a survey’, Future Gener. Comput. Syst., 2016, 56, pp. 684–700

[3] Salah, K., El Kafhali, S.: ‘Performance modelling and analysis of hypoexponential network servers’, J. Telecommun. Syst., 2017, 65, (4), pp. 717–728

[4] Li, J., Cai, J., Khan, F., Rehman, A. U., Balasubramaniam, V., Sun, J., & Venu, P. (2020). A secured framework for sdn-based edge computing in IOT-enabled healthcare system. IEEE Access, 8, 135479-135490.

[5] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," IEEE Access, vol. 6, pp. 18 209–18 237, 2018.

[6] Jeong IC, Bychkov D, Searson PC. Wearable devices for precision medicine and health state monitoring. IEEE Trans Biomed Eng 2019 May;66(5):1242-1258.

[7] Guk K, Han G, Lim J, Jeong K, Kang T, Lim E, et al. Evolution of wearable devices with real-time disease monitoring for personalized health care. Nanomaterials (Basel) 2019 May 29;9(6)

[8] Yapici, M. K. & Alkhidir, T. E. Intelligent medical garments with graphene functionalized smart-cloth ECG sensors. Sensors 17, 1–12 (2017).

[9] Kabiri Ameri, S. et al. Graphene electronic tattoo sensors. ACS Nano 11, 7634–7641 (2017)

[10] Someya, T. & Amagai, M. Toward a new generation of smart skins. Nat. Biotechnol. 37, 382–388 (2019)

[11] Li, Z., Zheng, Q., Wang, Z. L. & Li, Z. Nanogenerator-based self-powered sensors for wearable and implantable electronics. Research 2020, 1–25 (2020).

[12] Sethi, P.; Sarangi, S.R. Internet of things: Architectures, protocols, and applications. J. Electr. Comput. Eng. 2017, 2017, 9324035

[13] Williams, P.A.; Woodward, A.J. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Med. Devices 2015, 8, 305.

[14] Aghili, S.F.; Mala, H.; Kaliyar, P.; Conti, M. SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. Future Gener. Comput. Syst. 2019, 101, 621–634.

[15] Sun, Y.; Lo, F.P.W.; Lo, B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. IEEE Access 2019, 7, 183339–183355

[16] J. Lin et al., "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet Things J.,vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.

[17] V. Hassija et al., "A survey on IoT security: Application areas, security threats, and solution architectures," IEEE Access, vol. 7, pp. 82721–82743, 2019, doi:10.1109/ACCESS.2019.2924045.

[18] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted internet of things: From security and efficiency perspectives," IEEE Network, vol. 33, no. 2, pp. 50–57, March 2019.

[19] Health Statistics Of India, Report of the National Commission on Macroeconomics and Health, Ministry of Health & Family Welfare, Govt. of India August 2005, retrieved from: https://www.indushealthplus.com/health-statistics-of-india.html Accessed on 26th December 2024.

[20] PIB Delhi, (2022, February 8), Status of Non-Communicable Diseases (NCDs) in India, retrieved from: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1796435 Accessed on 27th December 2024.

[21] A. Minhas, (2023, Jul 12), Estimated number of public and private hospitals in India 2019, retrieved from: https://www.statista.com/statistics/1128425/india-number-of-public-and-private-hospitals-estimated/ Accessed on 27th December 2024.

[22] Cisco Annual Internet Report (2018–2023) White Paper, March 9, 2020, retrieved from: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html, Accessed on 28th December 2024.

[23] Amft O, Lukowicz P. From backpacks to smartphones: past, present, and future of wearable computers. IEEE Pervasive Comput 2009 Jul;8(3):8-13

[24] Medical-grade Smartwatch CardiacSense receives approval in India, February 17, 2023, retrieved from: https://www.financialexpress.com/business/healthcare-medical-grade-smartwatch-cardiacsense-receives-approval-in-india-2983982/ Accessed on 28th December 2024.

[25] Identity Theft Resource Center, "2020 End-of-Year Data Breach Report", retrieved from:https://www.idtheftcenter.org/2020-data-breaches/ Accessed on 29th December 2024.

[26] Anthem to pay $39M to state AGs to settle landmark 2015 data breach, September 30, 2020, retrieved from:

https://www.fiercehealthcare.com/tech/anthem-to-pay-39m-to-state-ags-to-settle-landmark-2015-data-breach Accessed on 28th December 2024.

[27] Richmond, S. Stopping the Attacks: Cybersecurity In Healthcare Manufacturing, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/08/17/stopping-the-attacks-cybersecurity-in-healthcare-manufacturing/?sh=4db312231a8d Accessed on 1st January 2025.

[28] Healthcare Data Breach Statistics, Posted by Steve Alder on 3oth December 2024, https://www.hipaajournal.com/healthcare-data-breach-statistics/, Accessed on 4th January 2025.

[29] Kesavan, E. 2023. Internet of Things (IoT): A Review of Security Challenges and Solutions. International Journal of Innovations in Science, Engineering And Management. 2, 4 (Dec. 2023), 65–71. DOI:https://doi.org/10.69968/ijisem.2023v2i465-71.