Proceedings of the 8th Faculty of Science International Conference (FOSIC 2025), Delta State University, Abraka, Nigeria. 12th – 14th November, 2025. Pp. 290 - 299

DATA THEFT PROTECTION ARCHITECTURE FOR INTERNET OF THINGS (IoT) – INTEGRATED MEDICAL INFORMATION SYSTEM.

[1]Ikem, O. C. and [2]Akazue, M. I.

[1]Department of Computer Science, Faculty of Science, Delta State University, Abraka, Nigeria.
[2]Department of Computer Science, Faculty of Science, Delta State University, Abraka, Nigeria.
Corresponding Author's Email: cbi4u2012@gmail. com

ABSTRACT

This study focuses on IoT-integrated medical information system. Integrating internet of things devices into medical database is increasing rapidly on daily basis in our healthcare sector, especially in developing country like Nigeria but the task of securing patient's data is a concern with this innovation. Protecting data in medical database is very essential because of its confidentiality, integrity, privacy of patient data and diminution of unauthorized or unlawful access to the medical database. The main objective of this study is to protect data in integrated internet of things (IoTs) devices in medical database system by designing an algorithm that will secure data within the hospital and create hierarchy to access of information in the medical database system. Object-oriented system methodology for the medical database system and internet of things methodology for IoT devices were employed for this research. It was discovered that data from the integrated IoT devices can be secured in the medical database system. The research concludes that medical database provides medical professionals and personnel with considerate security for enhancing patient medical care and information.

INTRODUCTION

Ihama, *et al*. (2023) discussed that Internet of things also abbreviated as IoT; is the interconnection of several systems, devices or physical objects or things by sensors, software and other equipment in order to interconnect and interchange data with other devices and systems through the internet. IoT devices and appliances are of different dimensions and capacity of electrical or electronic devices that can link to the internet. IoT devices can be used in a diversification of settings.

Ihama, *et al.* (2025) states that IoT is an innovation that has improved the old way of system existence into an evolutionary high-tech system. Integration of Internet of Things (IoT) devices into medical systems such as wearables, blood sugar and BP machines, smart sensors, etc., has enhanced healthcare delivery. However, despite the benefits, integration exposes patients' data to internet threats particularly data theft in the course of data transmission and storage. The threats are prevalent in developing countries like Nigeria where the healthcare sector faces infrastructure weakness, regulatory gaps and low cybersecurity awareness, which exacerbate the sector's vulnerability. There is therefore need to develop a resilient data theft protection architecture for internet of things (IoT) – integrated medical information system. The basic objective of the study is to analyse common security threats in IoT-integrated medical systems and to design a layered architecture that prevents unauthorized access and theft of medical data in clinics and hospital during transmission, storage and processing stages.

Internet of Things (IoT) Architecture:

Generally, IoT architectural arrangement has four layers and they are perception layer (sensing data), network layer (channelling data), processing layer (manipulating data), and application layer (appliances and devices) as seen in Figure 1. Examples of the perception layer devices are different models and kinds of sensors, surveillance cameras, conveyor systems, GPS (Global Positioning System) modules, industrial robots, RFID (Radio-Frequency Identification) scanners, etc. Network layer consists of communication scheme like WiFi (wireless fidelity), Zigbee, LTE, Bluetooth, etc., with protocols like IPv4 (internet protocol version four), and IPv6 (internet protocol version six). Network layer transfers data to the processing layer. Ideally, cloud servers and databases, that are in the processing layer are obligated for data analysing, computing, processing, and stacking a large amount of data.

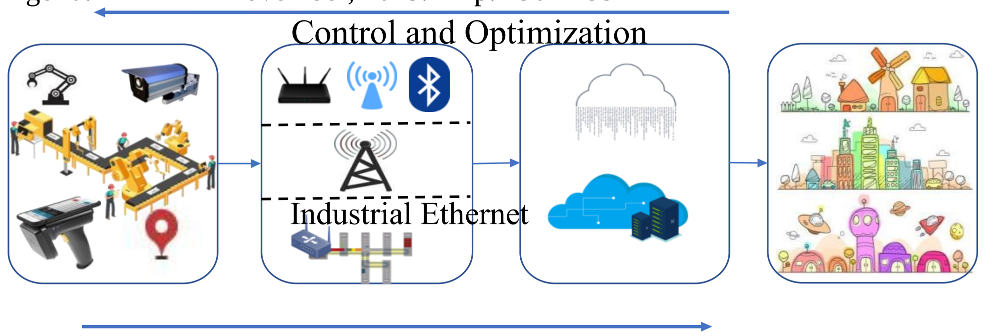


Figure 1: Generalized IoT Architecture (Sadhu, 2022)

The major reason for data theft protection is to secure communication. Data privacy is the process of gathering of data, saving it memory and using the same data, in such a way that personal record is safe and intact. Security can be enhanced using safe key management and physical unclonable operations. Figure 2 shows the fragments that explains the various security concept of IoT-based network.

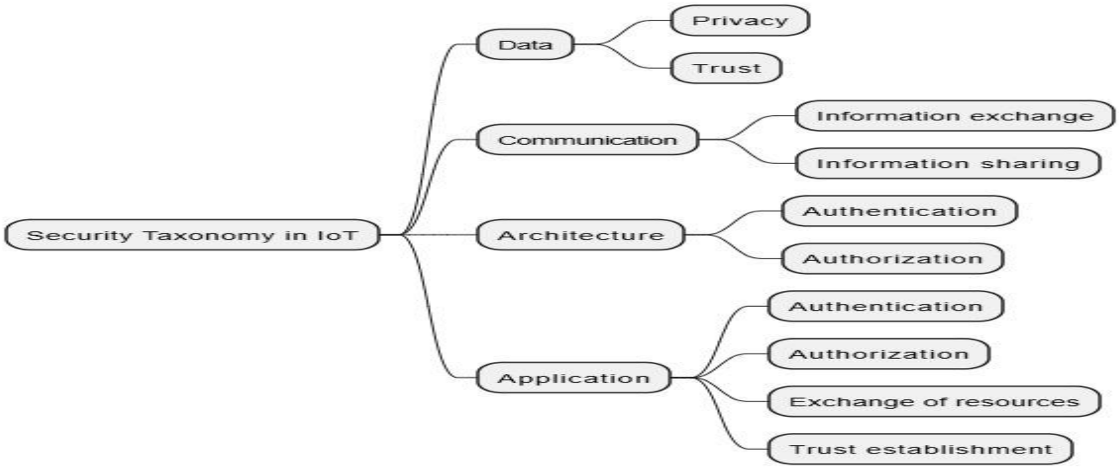


Figure 2: Security Taxonomy (Sadhu, 2022)

Medical information system is the electronic or non-electronic rendition of a patient's health history that a healthcare provider has recorded and stored for a space of time and is passed from one medical department to another or one medical staff to another (Zarei and Sadoughi 2015). It comprises all key administrative medical data that is provided with diligence associated to a patient by a unique provider; including demographic, progress reports, problem, medication, important sign, medical history, immunization reports, laboratory data, and radiology reports. Some clinics or hospitals still use paper-recording to safe patient medical information, whose consequence is symbolic paper trail (Zarei and Sadoughi 2015). The paper-based medical records can easily be erroneous due to poor lettering; they periodically malfunction and can naturally lost. It was difficult to track a patient's record; the clerk had to search through multiple files manually to get the certain file. Electronic medical database records are standard and has no messy script, adequate storage and access (Alanazi, *et al.* 2017). It also adds a high degree of safety that permits individuals to access patient information. Electronic medical database system has great capability to enhance healthcare processes and they are increasingly applicable in Nigeria and many advancing countries (Olukorode, *et al.* 2024).

Three-Layer and Five-Layer Architecture of IoT

The three-layered fundamental high-level architecture as generally accepted was presented in the early days of IoT evolution (Wu, *et al.* 2010). The three layers are namely: perception, network, and application layers.

i.

Perception or Sensing Layer:

The perception layer's major task is to observe the bodily properties of things surrounding us that are among the IoT ecosystem. This cognitive operation is based on a lot of sensing technologies such as RFID (Radio Frequency Identification), WSN (Wireless System Network), GPS (Global Positioning System), NFC (Near Frequency Connection), etc. This layer does the transformation of information into digital signals, that are more suitable and appropriate for network transmission. But some objects or things may not be perceived directly, microchips will be added to these objects to enable them to be sensed and processed (Sethi and Sarangi, 2017).

ii. Network Layer:

This layer will process the data received from the perception layer, transmit these data to the application layer through various network technologies such as wireless or wired networks and local area networks (LAN), FTTx (Fiber to the x), 3G (Third Generation) or 4G (Fourth Generation), WiFi, Bluetooth, ZigBee, UMB and infrared technology (Sethi and Sarangi, 2017).

iii. Application Layer:

The application layer used processed data from network layer. The front-end of the overall IoT architecture is the application layer, it allows IoT potential to be accomplished. This layer also arranges the requisite tools (e.g., actuating devices) for developers to accomplish and materialize the IoT vision (Wu, et al, 2010). In figure 3 showcase application layer, network layer and sensing layer of a simple three IoT architecture.

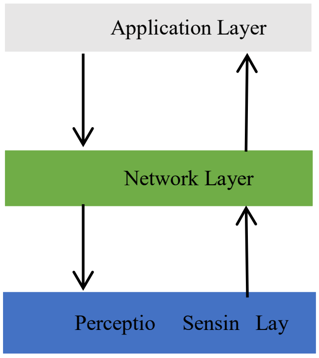


Figure 3: A three-layer IoT architecture adopted from (Wu, *et al.,* 2010)

More layers have been added overtime, with the rise in technological progression and symbolical advancements in IoT systems, more layers were added in IoT architecture model and they are processing layer and business layers summing it up to a five-layer architecture model (Mashal, *et al.* 2015). The most comprehensive explanation of IoT architecture is the five-layers' model. In this model, the perception and sensing layer, network layer and application layer corresponds as in the three-layered model.

iv. Processing Layer:

This layer receives, analyses, processes and stores numerous data from the network layer. Variety of technologies are used in this layer, which includes databases, cloud computing and big data processing modules.

v. Business Layer:

This layer moderates the whole IoT system, which includes all applications, business models and user privacy and security. The technologies used in this layer determines the success of device and how these technologies are delivered to their users. These tasks are carried out by the device's business layer. It helps in the development of flowcharts, graphs, analyses results, and defines how the device can be reformed (Sethi and Sarang, 2017). In Figure 4 the inter connectivity between five-layer model of Internet of Things (IoT) is displayed.

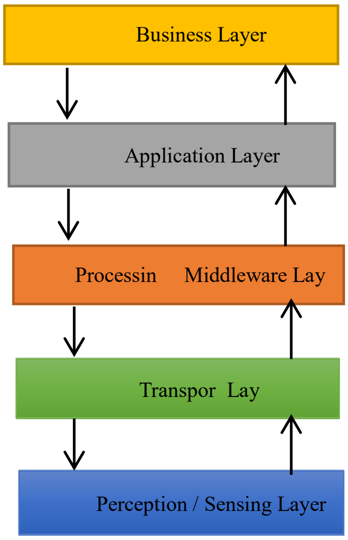


Figure 4: A Five-layer architecture models of IoT adopted from (Mashal, *et al*, 2015)

Data Theft Protection

As IoT devices and applications are speedily increasing, so data theft protection concerns have risen simultaneously. Available vulnerabilities and weaknesses in billions of devices is an open challenge for exploitation and hacking. There is risk that weakness and misconduct in the IoT devices can dominate all of its potential benefits if adequate protection is not put in place (Gubbi, *et al.* 2013).

Clinics and hospitals store patient data in a third-party cloud storage location. These vendors can comfortably have access to a great extent of patient sensitive data. Consequently, cloud service providers will have unlimited entrance to patient's information without the need for any privacy contract. Organizations, clinics and hospitals are the main customers of cloud service providers not the consumers. The wider the length between the data keepers (cloud services provider) and the real owner of the data (consumer), the higher the probability of unethical behaviour occurring and the risks of data theft will enhance (Priya, *et al.* 2018).

Components of Data Theft Protection

i. Authentication

Authentication validates the users. It confirms and approves the users and they are not viruses, spyware, or spiteful users simulating to be user. This authentication and identification process enables us to know whom we are communicating with. To determine that the right user have right to the system, sensors and devices for collection of data is a serious security issue. (Sicari, *et al.* 2014).

ii. Authorization

Authorization gives permission of device. (Seitz, *et al.* 2013).

iii. Privacy

This is the legal right of individuals to determine the quality and quantity of their personal information that can be revealed and communicated to other users. Wang, et al., 2015 states that privacy is one of the major
interest.

iv. Confidentiality

Ogunsanwo (2024) states that confidentiality means that personal key information will not be revealed without permission, either deliberately or accidentally. Ashraf and Habaebi (2015) revealed that this can be achieved by cryptographic and encryption mechanisms.

v. Integrity

Data integrity is the process of storing and collecting data and retaining its correctness, consistency, validity and reliability. Data integrity determines the quality of data in various systems (Sicari, *et al.* 2014). Duggineni (2023) explained that data integrity can be affected by institutions by encrypting their data, enforce regular backup of data, preserve audit trails to track origin of any data exploitation and implement access controls.

vi. Self Configuration

Skarmeta, *et al.* (2014) noted that it is important Internet of Things (IoT) devices should be able to self-configured and actively carry out access control systems on its own, or with minimal user intervention. Hamdi and Abie (2014) studied adaptive security as a virtual way to do this, as it empowers nodes to fit to its surrounding and its own state while implementing security mechanisms. Hallé, *et al.* (2021) states that rather than relying on manual configuration, inter-operation, and repair of computer systems; autonomic computing pushes forward the concept of mimicking properties of the autonomic nervous system.

vii. Availability

Availability means that the system should willing to serve rightful users at all times. The main attacks against availability are the denial of service (DoS) and distributed DoS (DDoS).

viii. Trust Management

Trust mechanism is implemented to determine if the system is working since it relies on sensor devices to collect data, send back accurate and valid data.

ix. Key Management

Jing, *et al.* (2014) explained that key management is the management of security keys that include key generation or development, key delivery, key change or modification, and key destruction or revocation, in addition to securely storing security keys. If an attacker knows or obtains the security keys, the attacker would be able to steal data from IoT devices.

x. Software Authenticity

Software authenticity is the security mechanism that ensures the genuineness and trustworthiness of software installed on devices and systems.

xi. Physical Security of Devices

Roman, *et al.* (2011) explained that attackers can easily gain access and tempers IoT devices and systems that run unattended in unprotected environments, such as city streets, parks, public buildings, and parking lots.

Security and Privacy Threats in Different Layers of Internet of Things Architecture

The internet of things architecture is structured as a layered architecture; each layer has its own functions, attributes and employ various engineering sciences to carry out those functions. The speedy growth of IoT devices gave raise to numerous types of security concerns. Cerullo, *et al.,* (2018) listed examples as authentication, authorization, confidentiality, integrity, privacy, self configuration, software authenticity, hardware anti-tampering, availability, key management and trust are potential threats.

i. Perception Layer Threats:

Owing to the wireless nature of this layer, criminals can attack its sensor nodes (Vashi et al., 2017). Alaba, et al. (2017) explained that this layer has two sections: Perception nodes (sensors, controllers) and the perception and sensing networks (this connects to the network layer).

ii. Network Layer Threats:

its obligation is network transmission, information security and spreading information in the perception layer. Li, *et al.* (2016) explained that this layer helps in the interaction between the application and the service. Examples of network layer threats are phishing site attack, access attack or man-in-the-middle attack, DoS attack, DDoS attack, sybil attack, routing attacks or sinkhole attack and hello flood attack.

iii. Processing Layer Threats:

Hassija, *et al.* (2019) states that this layer has the attributes of device discovery and management, big data analytics, security etc. Examples of processing layer threats are flooding attack in cloud, de-synchronization, SQL injection attack and man-in-the-middle attack.

iv. Application Layer Threats:

Alaba, *et al.* (2017) explained that the foundations of this layer are made up of different applications such as smart grid, smart city, smart government, smart healthcare, and smart transportation. Examples of application layer threats are data theft attacks, data corruption, sniffing attacks, DoS attacks, malicious code injection attacks and reprogram attacks.

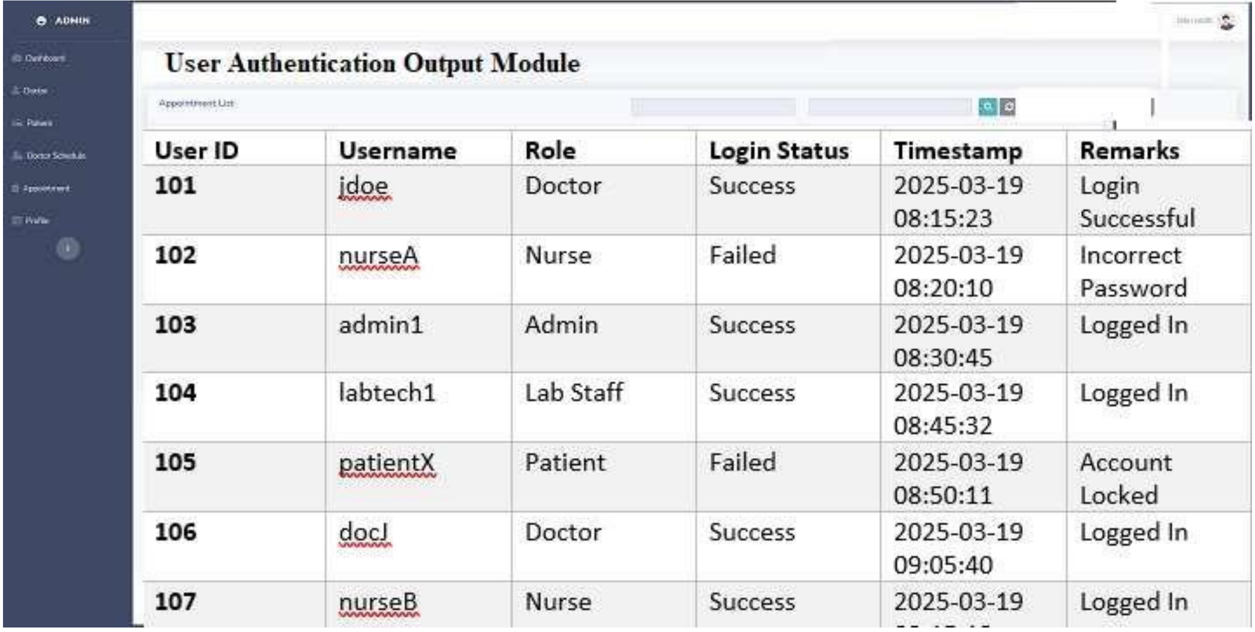
MATERIALS AND METHODS

The designed system used Role Based Access Control (RBAC) in the Microsoft Structured Query Language (SQL) Server as the database management system (DBMS); Class Diagram Modelling (CDM) to illustrate the relationship between the different classes and types of objects; IoT microcontroller Espressif System 32-bit (ESP32) was used for online data transmission, analogue files and documents were used for offline; ASP.NET (Visual Basic Studio 2022) was used in the frontend design because of its user-friendliness; Hypertext Mark-up language and JavaScript were used for programming the backend because of its high-profile security; and a Windows server operating system.

RESULTS AND DISCUSSION OF FINDINGS

The Program Output Module is responsible for displaying processed data and system responses based on user interactions within the medical information system. It ensures that relevant information is presented to the appropriate users in a structured and intuitive manner, enhancing system usability and efficiency. The outputs are designed to be role-based, ensuring that sensitive patient information is accessible only to authorized personnel, thereby enforcing data privacy and security. Additionally, the system integrates automated alerts, printable reports, and status updates to optimize decision making and patient care processes.

i. The User Authentication Output Module provides feedback on login attempts, displaying success messages for valid credentials and error messages for incorrect login details or unauthorized access attempts.

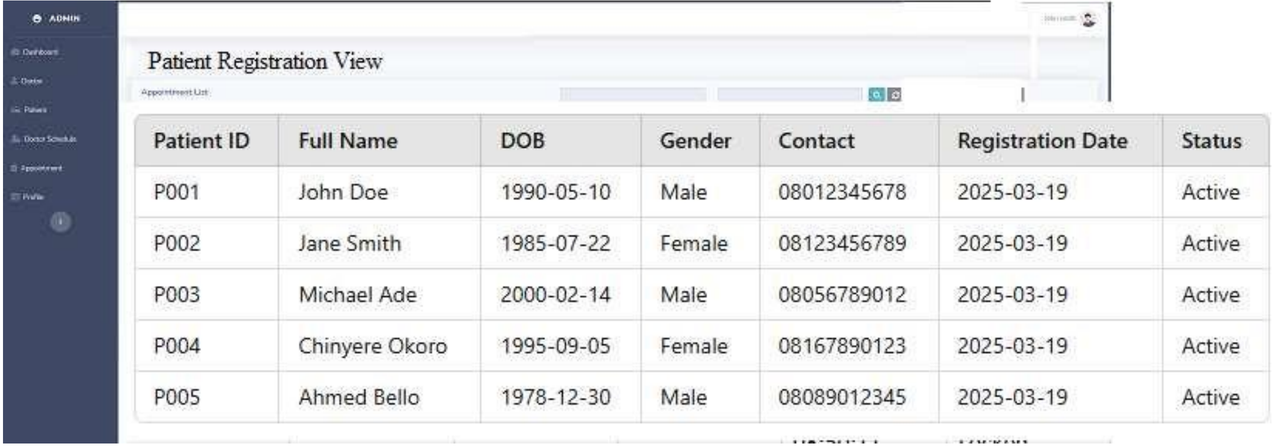


User Authentication Output Module

User ID	Username	Role	Login Status	Timestamp	Remarks
101	jdoe	Doctor	Success	2025-03-19 08:15:23	Login Successful
102	nurseA	Nurse	Failed	2025-03-19 08:20:10	Incorrect Password
103	admin1	Admin	Success	2025-03-19 08:30:45	Logged In
104	labtech1	Lab Staff	Success	2025-03-19 08:45:32	Logged In
105	patientX	Patient	Failed	2025-03-19 08:50:11	Account Locked
106	docJ	Doctor	Success	2025-03-19 09:05:40	Logged In
107	nurseB	Nurse	Success	2025-03-19	Logged In

Plate 1: Program Output Module

The Patient Registration Output Module generates confirmation messages upon successful registration, assigns a unique patient ID, and provides a printable or downloadable summary of patient details for future reference. It also displays error messages for incomplete or duplicate entries.

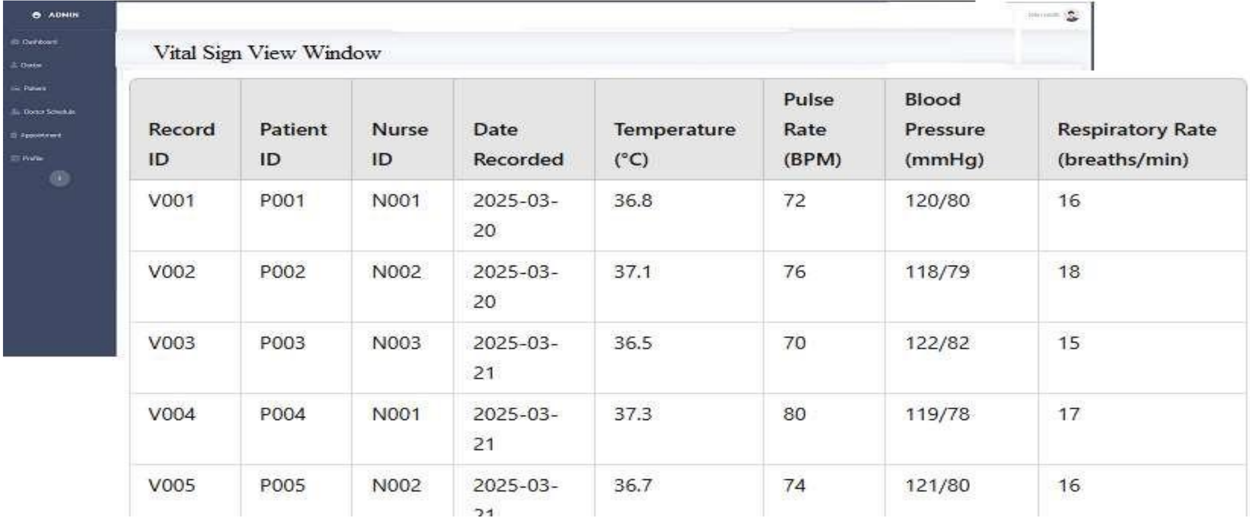


Patient Registration View

Patient ID	Full Name	DOB	Gender	Contact	Registration Date	Status
P001	John Doe	1990-05-10	Male	08012345678	2025-03-19	Active
P002	Jane Smith	1985-07-22	Female	08123456789	2025-03-19	Active
P003	Michael Ade	2000-02-14	Male	08056789012	2025-03-19	Active
P004	Chinyere Okoro	1995-09-05	Female	08167890123	2025-03-19	Active
P005	Ahmed Bello	1978-12-30	Male	08089012345	2025-03-19	Active

Plate 2: Patient Registration Output Module

iii. The Vital Signs Output Module presents recorded vital sign data in a structured format, allowing doctors to view patients' temperature, pulse rate, blood pressure, and oxygen saturation levels in tabular or graphical representation for quick assessment. It also triggers alerts for abnormal readings.

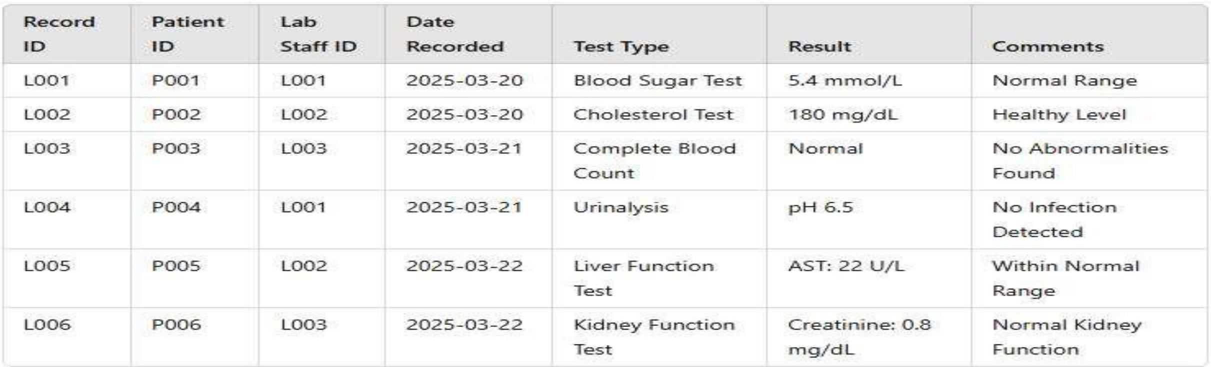


Vital Sign View Window

Record ID	Patient ID	Nurse ID	Date Recorded	Temperature (°C)	Pulse Rate (BPM)	Blood Pressure (mmHg)	Respiratory Rate (breaths/min)
V001	P001	N001	2025-03-20	36.8	72	120/80	16
V002	P002	N002	2025-03-20	37.1	76	118/79	18
V003	P003	N003	2025-03-21	36.5	70	122/82	15
V004	P004	N001	2025-03-21	37.3	80	119/78	17
V005	P005	N002	2025-03-21	36.7	74	121/80	16

Plate 3: Vital Signs Output Module

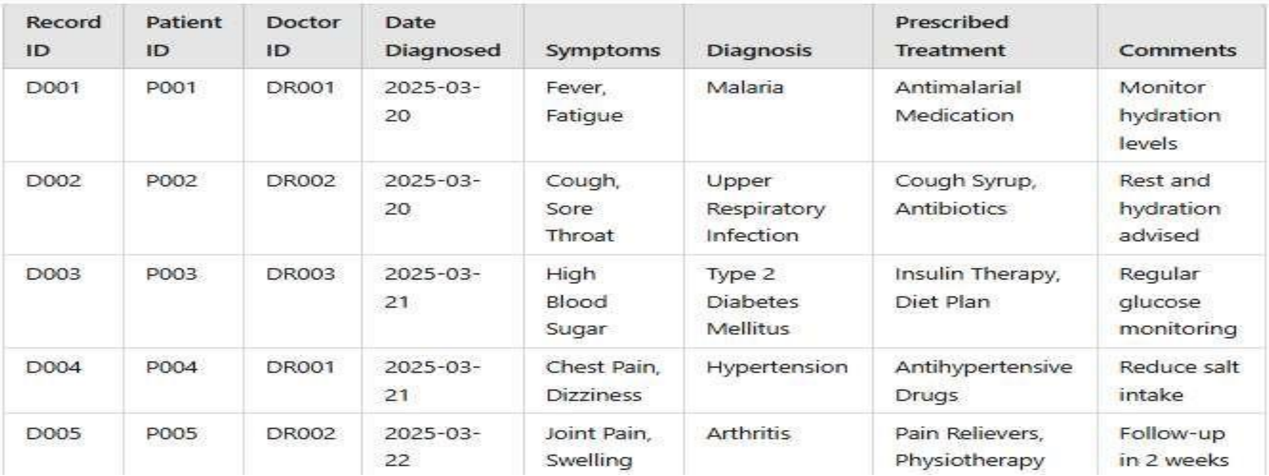
iv. The Lab Test Result Output Module displays test results entered by Lab Staff in a well-organized format, linking them to the respective patient's medical record for doctors' review.



Record ID	Patient ID	Lab Staff ID	Date Recorded	Test Type	Result	Comments
L001	P001	L001	2025-03-20	Blood Sugar Test	5.4 mmol/L	Normal Range
L002	P002	L002	2025-03-20	Cholesterol Test	180 mg/dL	Healthy Level
L003	P003	L003	2025-03-21	Complete Blood Count	Normal	No Abnormalities Found
L004	P004	L001	2025-03-21	Urinalysis	pH 6.5	No Infection Detected
L005	P005	L002	2025-03-22	Liver Function Test	AST: 22 U/L	Within Normal Range
L006	P006	L003	2025-03-22	Kidney Function Test	Creatinine: 0.8 mg/dL	Normal Kidney Function

Plate 4: Lab Test Result Output Module

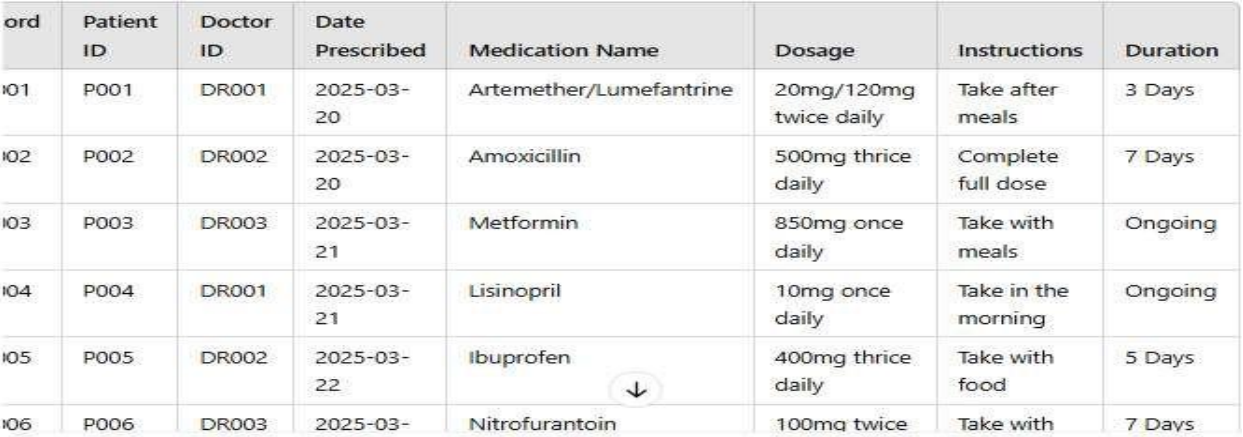
v. The Doctor's Diagnosis Output Module provides a detailed summary of doctors' assessments, including symptoms, test interpretations, diagnoses, and recommended treatments. The module ensures that all medical findings are accessible to authorized personnel while maintaining patient confidentiality.



Record ID	Patient ID	Doctor ID	Date Diagnosed	Symptoms	Diagnosis	Prescribed Treatment	Comments
D001	P001	DR001	2025-03-20	Fever, Fatigue	Malaria	Antimalarial Medication	Monitor hydration levels
D002	P002	DR002	2025-03-20	Cough, Sore Throat	Upper Respiratory Infection	Cough Syrup, Antibiotics	Rest and hydration advised
D003	P003	DR003	2025-03-21	High Blood Sugar	Type 2 Diabetes Mellitus	Insulin Therapy, Diet Plan	Regular glucose monitoring
D004	P004	DR001	2025-03-21	Chest Pain, Dizziness	Hypertension	Antihypertensive Drugs	Reduce salt intake
D005	P005	DR002	2025-03-22	Joint Pain, Swelling	Arthritis	Pain Relievers, Physiotherapy	Follow-up in 2 weeks

Plate 5: Doctor's Diagnosis Output Module

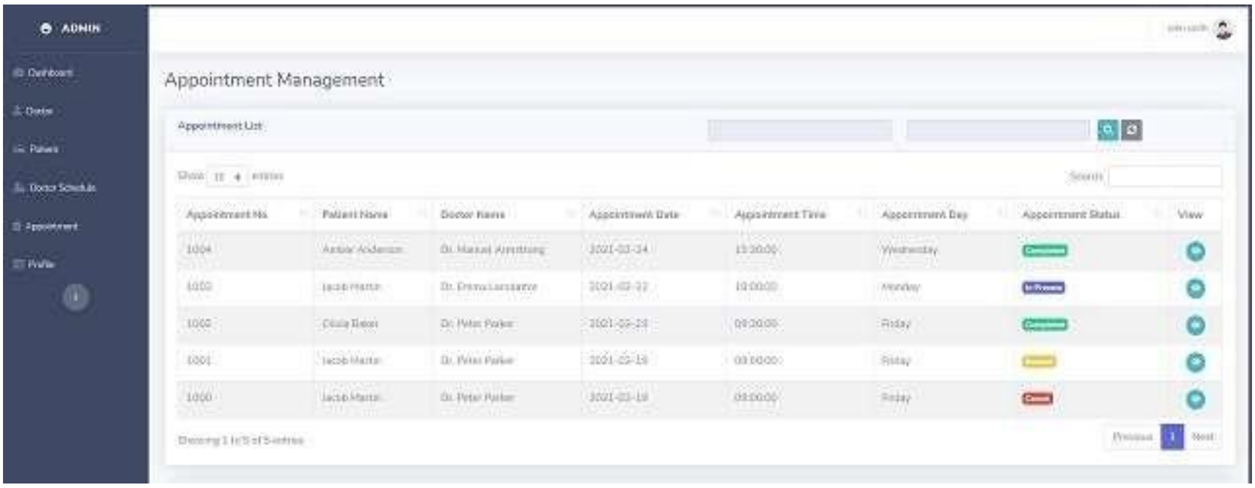
The Prescription Output Module generates structured medication prescriptions, displaying drug names, dosages, usage instructions, and refill requirements.



ord	Patient ID	Doctor ID	Date Prescribed	Medication Name	Dosage	Instructions	Duration
01	P001	DR001	2025-03-20	Artemether/Lumefantrine	20mg/120mg twice daily	Take after meals	3 Days
02	P002	DR002	2025-03-20	Amoxicillin	500mg thrice daily	Complete full dose	7 Days
03	P003	DR003	2025-03-21	Metformin	850mg once daily	Take with meals	Ongoing
04	P004	DR001	2025-03-21	Lisinopril	10mg once daily	Take in the morning	Ongoing
05	P005	DR002	2025-03-22	Ibuprofen	400mg thrice daily	Take with food	5 Days
06	P006	DR003	2025-03-	Nitrofurantoin	100mg twice	Take with	7 Days

Plate 6: Prescription Output Module

vi. The Appointment Scheduling Output Module confirms booked appointments, showing assigned doctor details, scheduled time, and status updates.



Appointment Management

Appointment List

Show 10 entries

Search:

Appointment No.	Patient Name	Doctor Name	Appointment Date	Appointment Time	Appointment Day	Appointment Status	View
1004	Amber Anderson	Dr. Manuel Armstrong	2021-03-24	13:30:00	Wednesday	Completed	●
1003	Jacob Martin	Dr. Emma Lanzarre	2021-03-22	10:00:00	Monday	In Process	●
1002	Olivia Baker	Dr. Peter Parker	2021-03-26	09:30:00	Friday	Completed	●
1001	Jacob Martin	Dr. Peter Parker	2021-03-19	09:00:00	Friday	[illegible]	●
1000	Jacob Martin	Dr. Peter Parker	2021-03-19	09:00:00	Friday	[illegible]	●

Showing 1 to 5 of 5 entries

Plate 7: Appointment Scheduling Output Module

The data theft protection architecture for IoT – integrated medical information systems performed efficiently in terms of security, speed, role-based access control, and real-time IoT monitoring. The security framework effectively restricted unauthorized access, ensuring strict patient data privacy. Additionally, the system demonstrated high reliability and scalability, making it suitable for clinic environments of varying sizes. Future enhancements may include AI-driven anomaly detection for security threats and further performance optimizations.

CONCLUSION AND RECOMMENDATIONS

The research has illustrated that data theft protection architecture for IoT – integrated medical information system is feasible. This is a result of harsh functions and tools becoming effective in creating architecture for data protection. Additionally, the result of the modified IoT devices shows the possibility of close monitoring of patients from anywhere by the doctor or care-giver in real-time. This will drastically reduce sudden death, stroke and heart attack by BP patients.

REFERENCE

Alanazi, F., Othman, M., Hashem, I. and Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer* Applications, 88, pp.10-28.

Ashraf, Q. M. and Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in internet of things, *Journal of Network and Computer Applications,* 49(0), pp. 112-127.

Cerullo, G., Mazzeo, G., Papale, G., Ragucci, B., and Sgaglione, L. (2018). IoT and Sensor Networks Security. *ResearchGate* 2018 DOI 10.1016/b978-0-12-811373-8.00004-5

Duggineni, S. (2023). Data integrity and risk. *Open Journal of Optimization,* 12, 25-33. https://www.scrip.org/journal/ojop

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements and future directions. *Future Generation Computer System* 29 (7), 16451660.

Hallé, S., Villemaire, R. and Cherkaoui, O. (2011). Logical methods for self-configuration of network devices. *African Journal of Emerging Issues*. DOI:10.4018/978-1-60960-845-3.ch008

Hamdi, M. and Abie, H. (2014). Game-based adaptive security in the internet of things for e-health, in Communications (ICC), 2014 *IEEE International Conference on.* IEEE, 2014, pp. 920_925.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access,* 7, pp.82721-82743.

Ihama, E.I.; Akazue, M.I.; and Obahiagbon, K.O. (2025). A survey of smart city development and the role of internet of things. *FUPRE journal of scientific and industrial research.*

Ihama, E.I.; Akazue, M.I.; Omede, E.; and Ojie, D. (2023). A framework for smart city model enabled by Internet of Things (IoT). *International Journal of Computer Applications.*

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., and Qiu, D. (2014). Security of the internet of things: perspectives and challenges, *Wireless Networks,* 20(8), pp. 2481-2501.

Jones, C. (2003). The utilitarian argument for medical confidentiality: A pilot study of patients' views. *Journal of Medical Ethics,* 29, 348-352. Doi: 10.1136/jme.29.6.348

Li, S.; Tryfonas, T. and Li, H. (2016). The internet of things: a security point of view. *Internet Research,* 26(2), pp.337-359. DOI: 10.1108/IntR-07-2014-0173

Mashal, I.; Alsaryrah, O.; Chung, T. Y.; Yang, C. Z.; Kuo, W. H. and Agrawal, D. P. (2015). Choices for interaction with things on internet and underlying issues. *Ad Hoc Networks,* vol. 28.

Ogunsanwo, S. and Bello, I. (2024). Principles of informed consent and confidentiality. *SSRN journals,* 2024. http://dx.doi.org/10.2139/ssrn.4857301

Olukorode, O.; Adedeji, O.J.; Adetokun, A. and Abioye, A. I. (2024). Impact of electronic medical records on healthcare delivery in Nigeria: A Review. *PLOS Digit Health.* https://doi.org/10.1101/2023.12.05.23299498

Priya; Pathak, I. and Tripathi, A. (2018). Big data, cloud and IOT: An Assimilation. *2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T).* D01:10:1109/IAC3T.2018.8674024

Roman, R.; Najera, P. and Lopez, J. (2011). Securing the internet of things. *IEEE Computer,* vol. 44, pp. 51 - 58. http://doi.org/10.1109/MC.2011.291

Sadhu, P.K. (2022). Prospect of internet of medical things: A review on security requirements and solutions. *Sensors 22(15).* DOI:10.3390/s22155517

Sadhu, P.K.; Yanambaka, V.P. and Abdelgawad, A. (2022). Internet of things: Security and solutions survey. *Sensors 22(19),* 7433

Seitz, L.; Goran, S. and Christian, G. (2013). Authorization framework for the Internet of Things. DOI: 10.1109/WoWMoM.2013.6583465

Sicari, S.; Cappiello, C.; De Pellegrini, F.; Miorandi, D. and Coen-Porisini, A. (2014). A security-and quality aware system architecture for internet of things. *Information systems frontiers.*

Skarmeta, A.; Hernandez-Ramos, J. and Moreno, M. (2014). A decentralized approach for security and privacy challenges in the internet of things. *2014 IEEE World Forum on Internet of Things (WFIoT).* DOI: 10.1109/WF-IoT.2014.6803122.

Vashi, S., Ram, J., Modi, J., Verma, S. and Prakash, C., (2017). Internet of things (IoT): A vision, architectural elements, and security issues. 2017 *International Conference on*

ISMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).

Wang, H.; Jiang, X.; and Kambourakis, G. (2015). Special issue on security, privacy and trust in network-based big data. *Information Science International Journal* 318(C), 48–50

Wu, M., Lu, T.J., Ling, F.Y., Sun, J. and Du, H.Y. (2010). "Research on the architecture of internet of things," (ICACTE '10), vol. 5, pp. V5-484–V5-487, IEEE, Chengdu, China.

Zarei, J, and Sadoughi, F. (2015). Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk Management and Healthcare Policy.* http://doi.ortg/10.2147/RMHP.S99908