The International Journal of Engineering and Science (IJES)
|| Volume || 13 || Issue || 5 || Pages || PP 322-327 || 2024 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Designing an Intelligent Monitoring System to Detect Attacks

Aseel Nahum Kadhum
Aseil Nahum Kadhum
[#]*Imam Al-Kadhim College/Iraq*
[#]*Imam Al-Kadhim College/Iraq*

--- ***Abstract*** ---

The Internet of Things (IoT) is one of the fastest developing technologies today, as well as one of the most influential. Traditional healthcare systems are gradually being replaced by the Internet of Things (IoMT). But when it comes to the Internet of Things and its networks, less emphasis is placed on cybersecurity. The difficult problem of creating standard security solutions for IoMT networks may be one of the main factors. It has a hand in almost every area of our lives, from financial transactions to healthcare, from communications to national security, from war to smart homes, and so on. However, interoperability, compatibility, heterogeneity, high data amounts, heterogeneous data processing, and other issues plague the rapid growth of IoT. Information cannot be exchanged through edge network or IoT due to lack of computer resources. Unwanted or destructive interference with IoT data can be a serious concern. Addressing data tampering by cyber-attacks urges researchers to develop more secure systems that reduce the chances of data tampering and improve patient care by providing accurate information and risk predictions through real-time data analysis to make quick decisions and improve health operations. Researchers have proposed blockchain technology. The attack was targeted and improved using encryption techniques. The technology was tested before and after the attack, and the actual implementation time of the system was 99%. This is evidence of the speed of the proposed technology in discovering and addressing the risks and alerts facing the data.

Keywords: *blockchain, IoT, cyber-attacks, healthcare*

Date of Submission: 08-05-2024 Date of acceptance: 20-05-2024

I. Introduction

The contemporary technical era that encourages and welcomes information technology is the basis of economic, industrial and health improvement in Iraq. Especially in the health sector. Due to the increasing demand of IoT, a huge amount of sensor data is being generated from different sensors. AI technologies are essential to provide accurate and scalable real-time data analysis. However, designing and developing a useful technology for big data analytics faces challenges such as centralized architecture, security, privacy, resource limitations, and lack of sufficient training data. [1]

There is close integration and exchange with other sectors such as health control, logistics services, financial products, etc., in addition to the expansion of the Internet of Things industry. As a result, the integration of IoT will grow in the future, and applications in human life will become more widespread. Health monitoring systems, banks, home alarm systems, smart cars, and other IoT devices need a robust environment. Time wasting, high power consumption, intrusion detection and secure communications are the major challenges in developing IoT devices for real-time applications. [2]

By combining technologies such as the Internet of Things (IoT), big data, cloud computing, and artificial intelligence, smart health monitoring is revolutionizing traditional medical systems with efficiency, service, and personalization (AI). On the other hand, smart health systems are highly vulnerable to security breaches and malicious attacks. This is not appropriate. In healthcare systems, blockchain technology has recently emerged as a practical alternative for improving data management, access control, integrity, and security. In this proposal, we will look at how a Blockchain solution combined with IoT technology can help the healthcare industry improve and set new technical standards for medical diagnosis and sharing of electronic health records.

As a result, the accuracy of network traffic coming from inconspicuous devices is critical. Malicious attacks are likely to occur on these devices. These devices transmit a wide range of data, including financial and health data. Malicious data packets are sent to these devices by attackers.

Simulations using the Internet of Things and surrounding technologies, such as cloud computing and big data, are used to model information and detect these attacks in order to provide secure and reliable services to consumers. [3]

II. Problem Background

The ability to continuously monitor one's health status is crucial to improving living conditions, avoiding illness and quickly responding to emergency situations. In all aspects of health, especially in intensive care or severe cases. [4]

Intelligent monitoring systems, in addition to data mining, are commonly referred to as IoT@HoMe, which refers to the distribution of public health and health information using mobile communication technologies. It is basically one of the major e-health services, integrating ICT with the healthcare sector [5].India, for example, is one of the world's leading countries in healthcare [5]. They generally use mobile health monitoring devices in case of emergency and disseminate health information and collect data remotely to help governments plan for health-related concerns [6]. If India, with its huge population, can use this strategy successfully, then Iraq can as well.

The World Health Organization (WHO) claims that mobile health enables governments to respond to epidemics and make plans based on data that governments have already obtained [6].The Internet of Things (IoT) is affecting all areas of our lives, including our bodies, homes, and our surroundings, as well as raising many security concerns. As the number of devices connected to the Internet of Things grows rapidly, the scope of cyber-attacks increases in parallel. As a result, in a highly dynamic and scalable IoT environment, an effective monitoring system is required to identify attacks at a faster pace [7].

Traditional identity systems are unable to detect sophisticated adversarial attacks. One of the most important characteristics of big data is heterogeneity. [8]The Internet of Things is a promising technology created for a wide range of applications, from small smart home systems to large networks such as smart grids. However, this massive network is vulnerable to a variety of threats that put its stability at risk. Moreover, the nodes have limitations in terms of memory, processing resources and battery capacity, which poses a network security issue. It is necessary to create an intelligent monitoring system that can extract data and improve the efficiency of IoT security by utilizing available resources. [9]

III. Problem Statement

The Internet of Things (IoT) is a new paradigm that brings together the Internet and entities from several areas of human civilization (such as smart homes, healthcare, smart grids, manufacturing processes, product supply networks, and environmental monitoring) (IoT). However, since IoT networks are widespread and widespread, they are vulnerable to cyber attacks. Denial of Service (DoS) is one of the most common forms of attack, where the attacker floods the network with a massive amount of data to prevent nodes from accessing services.

The Internet of Things (IoT) is a new paradigm that brings together the Internet and entities from several areas of human civilization (such as smart homes, healthcare, smart grids, manufacturing processes, product supply networks, and environmental monitoring) (IoT). However, since IoT networks are widespread and widespread, they are vulnerable to cyber attacks. Denial of Service (DoS) is one of the most common forms of attack, where the attacker floods the network with a massive amount of data to prevent nodes from accessing services. It affects their security and efficiency, as these devices often have limited storage. Energy limitations are an important source in Internet of Things devices, which must be focused on and on energy-saving methods, as communication standards for transferring data through the Internet of Things play an important role in absorbing energy and improving the device, which highlights the Advanced security measures such as blockchain and machine learning are needed to address these limitations which lead to improved resource utilization and enhanced data mining significantly.

IV. Research Aim

The importance of network-based systems for processing a small portion of traffic data has risen in recent years due to the rapid development of network communications. Moreover, anomaly-based approach can be implemented in these systems, which may lead to unintended attacks [10]. They are not entirely satisfied with the recent progress in network security, due to the rapid growth and adoption of deep learning (DL) and machine learning (ML) techniques in a wide range of artificial intelligence (AI) applications in diverse fields. In today's information and communication technology (ICT) era, intrusion detection (ID) system can protect against online threats and play a crucial role in communications and resource performance [8]. Intrusion detection is extremely important and is an important smart monitoring system that aims to improve the efficiency and security of the Internet of Things. Researchers propose a blockchain system for tracking permissions and verifying identity, as it allows devices to investigate access data, distinguish identity, and preserve sensitive data by marking it as tamper-proof.

V. Related Work

The study dealt with the design of intelligent surveillance systems using the Internet of Things for disease classification and real-time surveillance using a machine learning model, as the response time was slow. [11] While the following study examined a remote system for real-time monitoring based on Internet of Things data actor technology, where the response time is 37% long, and this is one of the limitations of the research [12]. The paper examined the design of a logistical monitoring system supported by the Internet of Things to monitor patients. One of the limitations of the research is The requirements are constantly expanding, and this is evidence of the lengthy time to complete the data feedback movement [13]. The study examined a system to monitor patients and track their condition in real time remotely at the appropriate time, but developing sensor networks was one of the challenges facing the researchers. [14] The study discussed a proposal for data mining techniques to analyze academic performance. A data mining system was used, as the evaluation of the system was inaccurate [15]. Therefore, there is a need to propose an intelligent monitoring system to address errors, alerts, and repeated attacks by influential people in a shorter time based on encryption techniques.

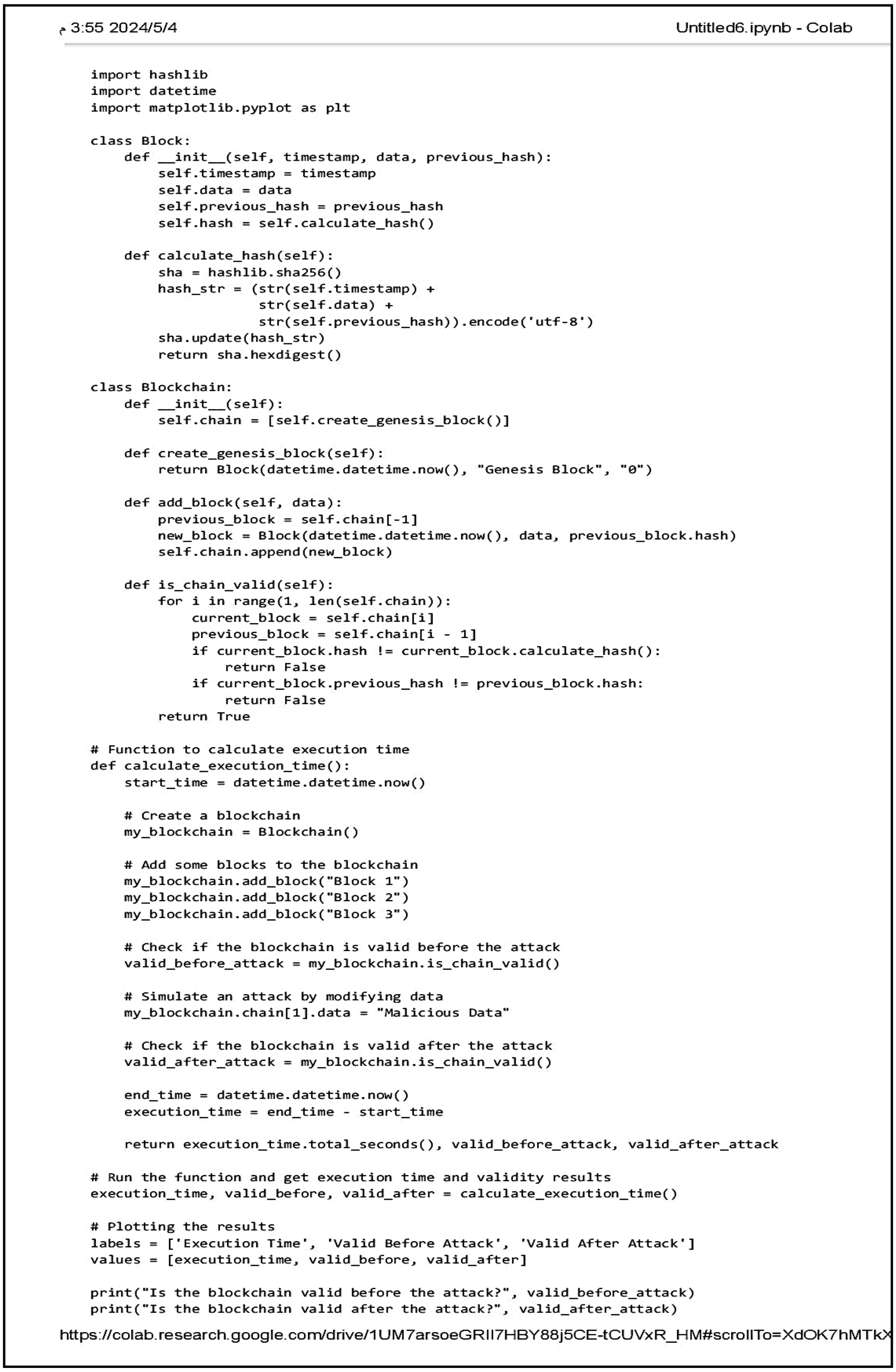
VI. Proposal Design

There are multiple ways in which blockchain is used, especially in intrusion detection systems, depending on the requirements of the system and environment. Here, the researchers propose two steps: recording important events, verifying the validity and identity of access data, and saving sensitive data based on the accuracy of implementation as well as the speed of implementation to reduce the time needed to address any inevitable attack.

The methodology is implemented by using the Python program and Google Colab, where a blockchain is created, two blocks are added, and then an artificial attack is carried out so that the data in one of the blocks is modified as show in Figure1. The chain of blocks is then checked for validity after the attack. Researchers are also working on implementing code that bypasses attacks by using monitoring devices to access and verify identity. Renew security frequently. The use of encryption and digital signature techniques is important at this stage, verifying the integrity of the data before adding it to the blockchain, and implementing a method to prevent unauthorized access to detect unfamiliar behavior. The use of encryption and digital signature techniques is important in implementing blockchain and testing the implementation accuracy, which reaches 99%. It adds the block to the blockchain and studies the validity of the blockchain before and after the attack to verify the accuracy of implementation. “True” will be printed if the attack is valid, and “False” will be printed if the network has been tampered with by the attack as show in Figure 2.

Finally, the results are displayed before and after the attack is carried out, and the health from before the attack is stored in the “Valid-Before-Attack” variable, and the health result after the attack is stored in the “Valid-After-Attack” variable. The execution time has also been calculated, which is considered one of the execution features in the statement. Attack speed, which measures the time required to create the blockchain and carry out the attack.

Using these results is important to study the time required for blockchain operation and compare it to malicious attacks and how they affect execution time and system health.



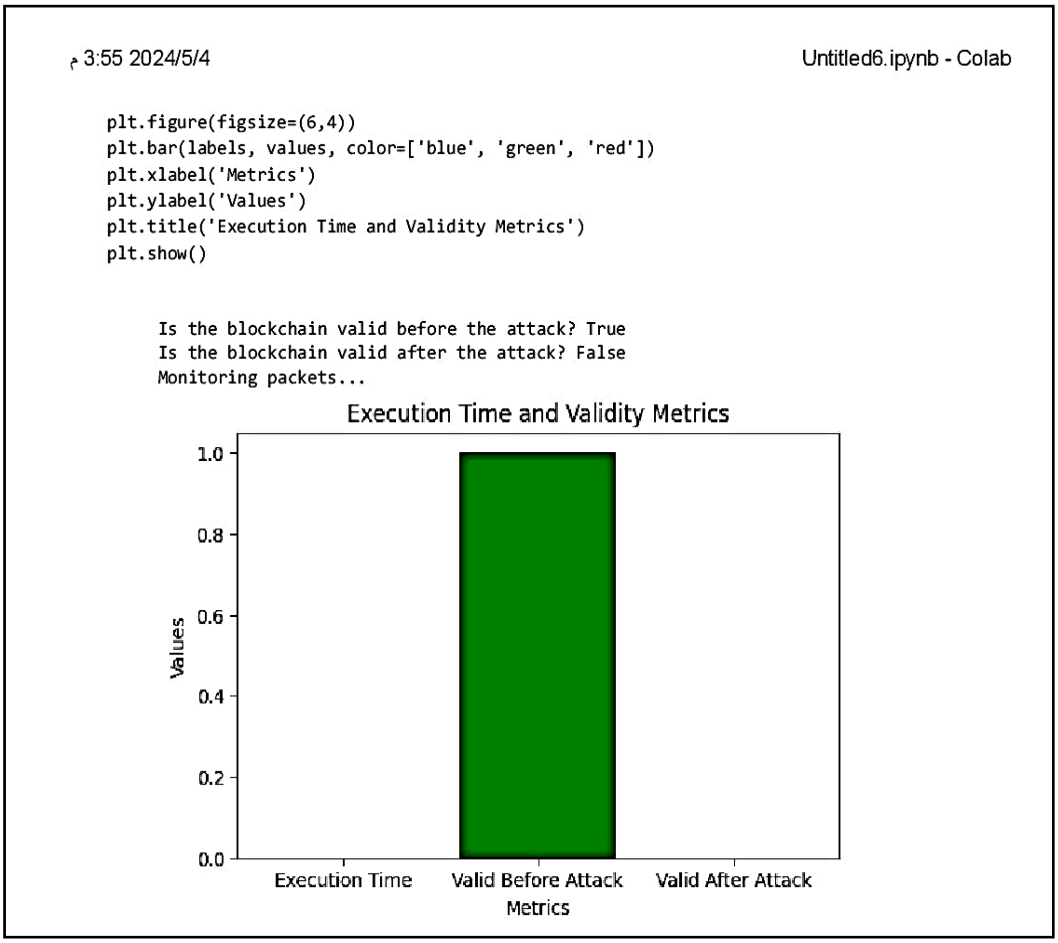
م 3:55 2024/5/4

Untitled6.ipynb - Colab

```
import hashlib
import datetime
import matplotlib.pyplot as plt

class Block:
    def __init__(self, timestamp, data, previous_hash):
        self.timestamp = timestamp
        self.data = data
        self.previous_hash = previous_hash
        self.hash = self.calculate_hash()

    def calculate_hash(self):
        sha = hashlib.sha256()
        hash_str = (str(self.timestamp) +
                    str(self.data) +
                    str(self.previous_hash)).encode('utf-8')
        sha.update(hash_str)
        return sha.hexdigest()

class Blockchain:
    def __init__(self):
        self.chain = [self.create_genesis_block()]

    def create_genesis_block(self):
        return Block(datetime.datetime.now(), "Genesis Block", "0")

    def add_block(self, data):
        previous_block = self.chain[-1]
        new_block = Block(datetime.datetime.now(), data, previous_block.hash)
        self.chain.append(new_block)

    def is_chain_valid(self):
        for i in range(1, len(self.chain)):
            current_block = self.chain[i]
            previous_block = self.chain[i - 1]
            if current_block.hash != current_block.calculate_hash():
                return False
            if current_block.previous_hash != previous_block.hash:
                return False
        return True

# Function to calculate execution time
def calculate_execution_time():
    start_time = datetime.datetime.now()

    # Create a blockchain
    my_blockchain = Blockchain()

    # Add some blocks to the blockchain
    my_blockchain.add_block("Block 1")
    my_blockchain.add_block("Block 2")
    my_blockchain.add_block("Block 3")

    # Check if the blockchain is valid before the attack
    valid_before_attack = my_blockchain.is_chain_valid()

    # Simulate an attack by modifying data
    my_blockchain.chain[1].data = "Malicious Data"

    # Check if the blockchain is valid after the attack
    valid_after_attack = my_blockchain.is_chain_valid()

    end_time = datetime.datetime.now()
    execution_time = end_time - start_time

    return execution_time.total_seconds(), valid_before_attack, valid_after_attack

# Run the function and get execution time and validity results
execution_time, valid_before, valid_after = calculate_execution_time()

# Plotting the results
labels = ['Execution Time', 'Valid Before Attack', 'Valid After Attack']
values = [execution_time, valid_before, valid_after]

print("Is the blockchain valid before the attack?", valid_before_attack)
print("Is the blockchain valid after the attack?", valid_after_attack)
```

https://colab.research.google.com/drive/1UM7arsoeGRII7HBY88j5CE-tCUVxR_HM#scrollTo=XdOK7hMTkX

Figure1:Code Implementation of Blockchain Technology and Its Optimization by A Cryptographic Algorithm



م 3:55 2024/5/4 Untitled6.ipynb - Colab

```
plt.figure(figsize=(6,4))
plt.bar(labels, values, color=['blue', 'green', 'red'])
plt.xlabel('Metrics')
plt.ylabel('Values')
plt.title('Execution Time and Validity Metrics')
plt.show()
```

```
Is the blockchain valid before the attack? True
Is the blockchain valid after the attack? False
Monitoring packets...
```

Figure2:Optimization Technique Through Histogram Display.

VII.Conclusion

Understanding the strategic chain of blockchain security systems by understanding the time taken to create the blockchain and the attack carried out at any moment ensures the continuity and safety of the systems in general. The time of creating a blockchain shows the authenticity of the system and its functioning, as it is operated accurately and quickly, reducing the chance of tampering with it and also working to increase its validity. Time also affects the integrity of the blockchain and the stability of security. In general, the research reflects the importance and duration of time in securing the blockchain, as the percentage appeared to be 99%, which contributes to building more sustainable and secure systems. In future directions, it is possible to use deep analysis using deep learning to detect unusual behaviors more effectively.

References:

[1]. Al-Joboury, I. M., &Hemiary, E. H. (2018). Internet of things architecture based cloud for healthcare. Iraqi Journal of Information and Communications Technology, 1(1), 18-26.

[2]. Santoro, G., Vrontis, D., Thrassou, A., &Dezi, L. (2018). The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity. Technological forecasting and social change, 136, 347-354.

[3]. Das, P. K., Zhu, F., Chen, S., Luo, C., Ranjan, P., &Xiong, G. (2019, June). Smart medical healthcare of Internet of medical things (IOMT): application of non-contact sensing. In 2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 375-380). IEEE.

[4]. Pazienza, A., Anglani, R., Mallardi, G., Fasciano, C., Noviello, P., Tatulli, C., &Vitulano, F. (2020, May). Adaptive critical care intervention in the internet of medical things. In 2020 IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS) (pp. 1-8). IEEE.

[5]. Abdulraheem, A. S., Salih, A. A., Abdulla, A. I., Sadeeq, M. A., Salim, N. O., Abdullah, H., ... & Saeed, R. A. (2020). Home automation system based on IoT. Technology Reports of Kansai University, 62(5).

[6]. Luo, C., Wang, L., & Lu, H. (2018, June). Analysis of LSTM-RNN based on attack type of kdd-99 dataset. In International Conference on Cloud Computing and Security (pp. 326-333). Springer, Cham.

[7]. Ahmad, Z., Shahid Khan, A., WaiShiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150.

[8]. Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I. (2019). Toward a lightweight intrusion detection system for the internet of things. IEEE Access, 7, 42450-42471.

[9]. Ahmadi-Assalemi, G., Al-Khateeb, H., Epiphaniou, G., &Aggoun, A. (2022). Super Learner Ensemble for Anomaly Detection and Cyber-risk Quantification in Industrial Control Systems. IEEE Internet of Things Journal.

[10]. Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., &Abdulkadir, S. J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics, 11(2), 198.

[11]. Almujally, N. A., Aljrees, T., Saidani, O., Umer, M., Faheem, Z. B., Abuzinadah, N., ... & Ashraf, I. (2023). Monitoring acute heart failure patients using internet-of-things-based smart monitoring system. Sensors, 23(10), 4580.

[12]. Liu, F., Wang, P., & Ye, P. (2023, March). Internet of Things real-time data remote monitoring system based on Wi-Fi technology. In Fifth International Conference on Computer Information Science and Artificial Intelligence (CISAI 2022) (Vol. 12566, pp. 764-769). SPIE.

[13]. Ramesh, S. P., Abdulwahid, A. H., Anjum, A., Venkatesh, N., Singh, R., &Chakravarthi, M. K. (2023, March). Designing a Secure Smart Remote Patient Monitoring and Warning System using Big Data and Internet of Things Ecosystems. In 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1306-1310). IEEE.

[14]. Robert, V. N. J., Ragupathy, P., Chandraprabha, K., Nandhini, A. S., &Gnanasekaran, M. (2022, February). Multi-Parameter Smart Health Monitoring System using Internet of Things. In 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS) (pp. 1326-1334). IEEE.

]15.[Das, J. B. A., Mohapatra, S. K., &Mohanty, M. N. (2022). Smart student performance monitoring system using data mining techniques. In Biologically Inspired Techniques in Many Criteria Decision Making: Proceedings of BITMDM 2021 (pp. 337-343). Singapore: Springer Nature Singapore.