DESIGN OF VIENNA RECTIFIER

Chetan Lakade[1], Anil Ingole[2] and Sanskar Raut[3],
Sujit Mohurle[4], Rutwik Kothale[5], Nandini Dharpawar[6] and Sandeep K. Mude[7]

Department of Electrical Engineering[1234567],Student UG[123456], Assistant Professor[7],
K.D.K. College of Engineering, Nagpur, India
chetanplakade.ee@kdkce.edu.in

ABSTRACT

Vienna rectifiers are widely used in high-power applications due to their excellent performance in terms of power factor correction, low harmonics, and high efficiency. In this research paper, a design and analysis of a Vienna rectifier for high-power applications is presented. The proposed design is based on a three-phase AC input voltage and utilizes a combination of two capacitors and two diodes to achieve power factor correction and harmonic reduction. Theoretical analysis of the circuit is carried out, and simulation results are presented to validate the design. The impact of different parameters, such as input voltageand load variations, on the performance of the circuit is investigated. The simulation results show that the proposed design achieves high power factor correction and lower harmonic distortion under different operating conditions.

Keywords: *Vienna rectifier, AC-DC rectifier, synchronized switching, pulse width modulation, current distortion*

1. Introduction

Vienna rectifier is a power electronics circuit used for power factor correction and AC to DC power conversion. It consists of a diode bridge and an active front-end that uses MOSFETs or IGBTs. The design of a Vienna rectifier is critical as it affects the overall performance of the circuit. In this research paper, we will discuss the design of the Vienna rectifier and its various parameters.

The three-level Vienna rectifier is a very attractive boost-type power factor converter (PFC) because of its lower total harmonic distortion (THD) of input current and high power density and high efficiency. The three-level Vienna rectifier is used for various applications, such as telecommunication power system, wind turbine systems, motor drives. This rectifier is much convenient for volume and weight limited. Many scientists recommend a control method for three-level Vienna rectifier in order to obtain power factor will be unity and meet input current harmonics requirements.

As three-level Vienna rectifier is compared with three-level neutral-point clamped (NPC) rectifiers, the three-level Vienna rectifier consists of fewer full-controlled semiconductor switches, higher power density. Unlike the NPC converters, the terminal voltage of Vienna rectifier is determined by the switching states and polarity of the line current. The three-level Vienna rectifier topologies, which are range from a topology using the bi-directional switches, which is similar to the three-level T- type topology, from Fig.1 the Vienna rectifier has three- phase bidirectional switches. The Vienna rectifier, which is a non-generative boost type rectifier. The Vienna rectifier has different types of bidirectional phase-legs, which connects AC-side to neutral-point of the dc-link. The mostly used current control method with varying Switching frequency has relatively high input current, total harmonic distortion and brings the difficulty to design input inductance.

In order to achieve unity power factor and neutral-point voltage balancing, the normal carrier- based pulse width modulation method and space vector modulation method are widely used.

2. Design Considerations

The design of the Vienna rectifier involves several considerations, including the power rating, voltage rating, current rating, switching frequency, and thermal management. The power rating of the circuit is determined by the load power requirements. The voltage rating of the circuit is determined by the input voltage of the AC source. The current rating of the circuit is determined by the load current requirements. The switching frequency of the circuit is determined by the control strategy used for the active front-end. The thermal management of the circuit is criticalas it affects the reliability of the circuit.

3. Circuit diagram

The Vienna rectifier is a type of three-phase rectifier that has a unique circuit topology, which allows for high efficiency and low harmonic distortion. Here's a brief circuit diagram explanation of the Vienna rectifier:

The circuit consists of three AC input phases (L1, L2, and L3) and two DC output terminals (+Vdc and -Vdc). The AC input is first connected to a three-phase diode bridge rectifier, which converts the AC voltage into the pulsating DC voltage. This pulsating DC voltage is then fed into the Vienna rectifier stage, which consists of two switches (S1 and S2) and twocapacitors (C1 and C2).

Switches S1 and S2 are controlled by a PWM (Pulse Width Modulation) signal, which ensures that the switches are turned on and off at specific intervals to maintain the desired DC output voltage. The capacitors C1 and C2 act as filters, smoothing out the pulsating DC voltage and reducing harmonic distortion.

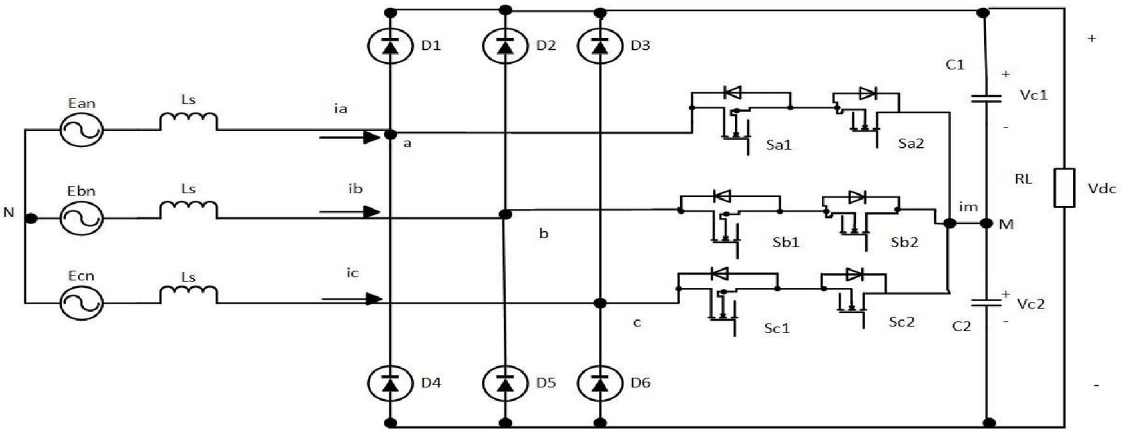


Fig.1: Three-phase Vienna Rectifier

4. Conclusion

The design of the Vienna rectifier is critical for its overall performance and reliability. The power rating, voltage rating, current rating, switching frequency, and thermal management must be carefully considered during the design process. The active front-end of the Vienna rectifier is critical for power factor correction and DC output voltage regulation. Thermal management is critical for the reliability of the circuit. The Vienna rectifier is extensively used in industrial applications for power factor correction and AC to DC power conversion.

References

1. Jene-Seok Lee, IEEE, and Kyo-Beum Lee, “Carrier-Based Discontinuous PWM Method for ViennaRectifier”, Aug. 2014
2. B. Kedjar, H. Y. Kanaan, and K. Al-Haddad, “Vienna Rectifier with Power Quality Added Function,” IEEE Trans. Ind. Electron., Vol. 61, No. 8, pp. 3847-3856, Aug. 2014
3. Songhee Yang, Jin-Hyuk Park, and Kyo-Beum Lee, “A Carrier-Based PWM with Synchronous Switching Technique for a Vienna Rectifier”, Mar. 2016, IEEE
4. J. W. Kolar and T. Friedli, “The Essence of three-thase PFC rectifier system Part-I,” IEEE Trans.Power Electron., Vol. 28, No. 1, pp. 176-198, Jan. 2013.
5. T. Friedli, M. Hartmann, and J. W. Kolar, “The Essence of three-phase PFC rectifier systems Part- II,” IEEE Trans. Power Electron., Vol. 29, No. 2, pp. 543-560, Feb. 2014.
6. D. O. Neacsu, “Principle of a Novel Component Minimized Active Power Filter for High-Power Magnet Supplies,” in Proc. IECON, pp. 3786 – 3791, 2012.

DIGITALLY VERIFIED KNOW YOUR CUSTOMER

Vaishali Surjuse, Leena Sawarbandhe, Akanksha Pawar, Prianshu Bhagat, Samiksha Ambekar and Purva Deshmukh
Department of Computer Science & Engineering, KDK college of Engineering, Nagpur
surjuse.vaishu@gmail.com, leen26sawarbandhe@gmail.com, akankshapawar22051@gmail.com, bhagatprianshu18@gmail.com, samikshaambekar07@gmail.com, purva5411@gmail.com

ABSTRACT

A critical yet minor issue in the monetary business right at present is the way long and costly the traditional Know-Your-Customer (KYC) process is. We propose a project considering advancement which will diminish the standard KYC affirmation process cost for Foundations and cut off the general course of occasions of the summit of the cycle while making it smoother for the clients. Critical improvement in our response over the customary techniques is that the whole check process is driven only a solitary time for each client, paying little mind to number of establishments the individual wishes to be associated with.

I. Introduction

The communication to affirm the person and various capabilities of a financial organizations client. The Know Your Client (KYC) or Know Your Client (KYC) is a communication to really take a look at the character and various certificates of a financial organizations client. The Know your Client (KYC) process helps against tax avoidance and prevents the supporting of mental oppressor works out. Banks were urged to follow explicit client conspicuous confirmation framework for opening of records and really taking a look at trades of a questionable sort to report it to fitting power. Electronic person check is rapidly creating as a quick result of cutting edge change drives and has seen extending improvement due to the Covid pandemic. Account opening is continuing on the web, and expert associations demand a strong and safe procedure to affirm character and for e-KYC. The key objectives of this report is to endeavor an examination of the mechanical progressions for e-KYC and take a gander at the changed strategies countries have taken on to do e KYC and give information about specific rules that could be completed to achieve interoperability at the level of the modernized character really look at process. These 'Know Your Client' rules have been gotten back to concerning the Ideas made by the Financial Movement Group (FATF) on Foe of Tax avoidance (AML) standards and on Battling Subsidizing of Mental fighting (CFT). The objective of KYC/AML/CFT rules is to hold banks back from being used, deliberately or suddenly, by criminal parts for tax avoidance or mental aggressor subsidizing works out. KYC frameworks moreover enable banks to know/understand their clients and their financial dealings better which accordingly help them with managing their risks prudently.

· To give client redesigned security.

· It will likely use web to accomplish paperless character check. · Its organization is totally robotized and available on the web. It can send data logically.

· Any misappropriation, unlawful approach to acting can be followed back to the individual or get-togethers drew in with such trade or organization use

II. Background

Know your client (KYC) is a term that implies the pattern of supervising clients and affirming their characters. The client presents this record to a relationship to spread out trust between the two social occasions. Since there was no framework to check clients characters by then, KYC was introduced in the US in 1990. The goal of KYC by then was to hinder dread based oppressor supporting and money washing through banks. The bank is the fundamental monetary sponsor in KYC. Clients are drawn nearer to wrap up a KYC record with the objective that their characters may be checked. To hinder unlawful duty aversion, dread based oppressor supporting, and financial deception, the bank twofold checks the information given by clients. In this manner, banks don't right now enable any record holder to open a record without KYC confirmation. The KYC regulatory work contains the going with information: client information, ID check, address affirmation, and photograph. In this current situation, the potential outcomes of the paper getting lost were higher. In this manner, a modernized KYC structure known as e KYC was proposed. The client wraps up the KYC report through the affiliation's web application in this strategy. The information surrendered was kept with in concentrated informational indexes. Client information can be gotten to by the business while by using the client id. Regardless, since data is stayed aware of in a united informational index, consolidated system deserts like failure point, data unmistakable tedium, pariah check actually remain. Besides, data housed on a concentrated server can be compromised/pursued by developers, extending the bet of client individual data being spilled.

IV. Methodology

The goal of KYC/AML/CFT rules is to keep banks from being utilized, deliberately or accidentally, by criminal components for illegal tax avoidance or psychological militant funding exercises KYC strategies additionally empower banks to be aware/comprehend their clients and their monetary dealings better which in tum assist them with dealing with their dangers judiciously.

- To give client improved security.
- It will likely utilize web to achieve paperless personality confirmation.
- It's administration is completely computerized and accessible on the web. It can send information progressively
- Any misappropriation, unlawful way of behaving can be followed back to the individual or gatherings associated with such exchange or administration utilization.

A)Database Design

We are using SQLite Database. SQLite is an opensource SQL information base that stores information to a text document on a gadget. Android comes in with worked in SQLite data set execution.

SQLite upholds all the social information base elements. To get to this information base, you don't have to lay out any sort of associations for it like JDBC,ODBC etc.

B)Architecture Design

The customer have, the authorized access to add/edit/delete a document from computerized archive. The system will authenticate the users identity. Our app has the following modules :

• *Register*: signup page (also known as a registration page) enables users and organizations to independently register and gain access to your system. It is common to have multiple signup pages depending on the types of people and organizations you want to register.

• *Login*: user navigates to an application and is presented with a login page as a way to gain access to the application. There are two possible results: Authentication is successful and the user is directed to the dashboard landing page. Authentication fails and the user directed to on the register page.

• *KYC Authentication*: KYC means Know Your Customer and sometimes Know Your Client. KYC or KYC check is the mandatory process of identifying and verifying the client's identity when opening an account and periodically over time.

User need to upload documents: User need to approved some permission. Permission such as allow their camera for upload their passport size photo,allow their gallery to access the required documents. If permission is granted then the uploading process will start. Here user can upload documents and verify them as well, so that they will be continue with the further process

• *Biometric*:To perform automated kyc onboarding:

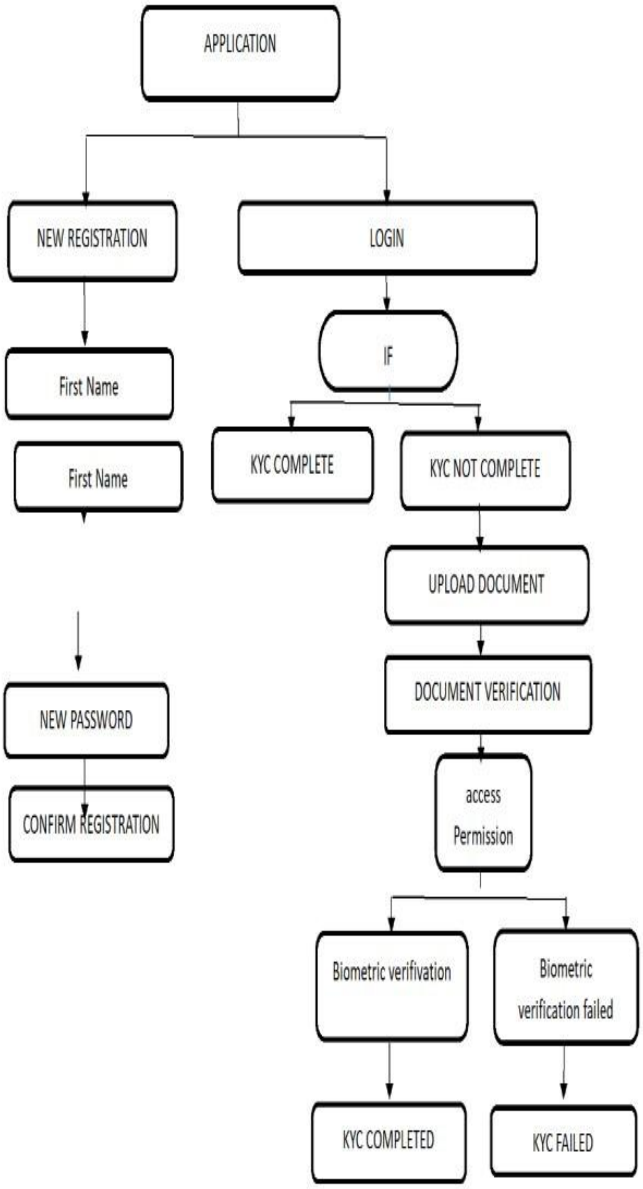
- Allow the client to take a depiction of his ID on his cellphone.
- The ID is checked for credibility/legitimacy.You request that the client take two selfies.
- The selfies are checked for liveness and contrasted with the picture on the ID.
- The ID possession is confirmed biometrically, the character sealing process is finished!

One of the critical drivers of involving Biometric ID for KYC the board is that it teaches a more significant level of safety than manual KYC cycles, for example, passwords, email locations or PINs which can be hacked utilizing numerous social designing methods and the individual data shared via web-based entertainment. Neglected, shared or lost passwords can alleviate security is they come in the possession of fraudsters. Resetting failed to remember passwords and composing long passwords and PINs likewise increments time for organizations to ready and execute with clients and emerges disappointments among them. Biometrics frameworks utilize extraordinary attributes of people like fingerprints and voice which offer vigorous security, yet additionally free clients from the weight of recalling passwords and PINs.

C)Interface Design

User Interface (UI) Design emphasizes expecting what users want to do and confirming that the interface has features that are easy to access, understand, and uses to smooth those actions. The architecture of our app is user friendly.

V. Flowchart:



VI. Experimental Results

Embracing the electronic difference in the KYC cycle licenses financial associations to lessen practical costs, be more open to clients' prerequisites and sustain their cycles. The inevitable destiny of KYC is as a particular distinction with the current work serious and dreary cycles.

· With immaterial commitment from clients, innovative financial associations will utilize various sources to support the data given by the clients and make faster, more exact decisions. The gathering of money related data network is at this point on the rising across the globe. The benefits are expansive, with brief and future moves up to consistence exercises, risk the board, client experience, and regardless, advancing.

· The data from your clients' records can be really taken a look at by a program to motorize routine endeavors, as critical level bet assessment, provoking rapid underwriting of commonly safe clients.

VII. Conclusion

We have presented the security safeguarding e-KYC approach . Our proposed plan conveys secure and decentralized approval and affirmation of the e-KYC process with the client's consent approval feature. In our arrangement, the security of the two clients' character files set aside in the data set is guaranteed key encryption Our arrangement furthermore allows the KYC data to be revived by the data owner or the client. In addition, we imagined an entry system update estimation to engage dynamic access endorsement. For the appraisal, we carried out comparable assessment between our arrangement and related functions to the extent that the estimation cost, the correspondence cost, and execution. The exploratory results showed that our arrangement beats existing plans to the extent that execution, expansive KYC consistence features, and the versatile access control part. For future works, we will test a greater illustration of data in the real data set environment and measure the throughput of the system in obliging huge number of e-KYC enrolment and affirmation requests. Moreover, we will investigate the technique to enable pack check of e-KYC trades set aside in the data set with the available encryption feature.

Acknowledgment

It has been a phenomenal opportunity to obtain lots of involvement dynamically project, followed by the data on the most capable technique to design and explore veritable task, as a matter of fact. I should offer my thanks and appreciation to all of the people who allowed me the opportunity to complete this job.

References

1. Real Time KYC using Face Recognition for Banking System , IJIRT Volume 8 Issue 9 February 2022 https://ijirt.org/master/publishedpaper/IJIRT153783 _PAPER.pdf .
2. SomchartFugkeaw, "Enabling Trust and privacy-preserving e-KYC system using blockchain",IEEE Access,vol.10,pp2169-3536,May2022. https://ieeexplore.ieee.org/document/9770032 .
3. A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan, M. S. Bhuiyan, et al., "Secure and transparent KYC for banking system using IPFS and blockchain technology", Proc. IEEE Region Symp. (TENSYMP), pp. 348-351, Jun. 2020.
4. M. Pic, G. Mahfoudi and A. Trabelsi, "Remote KYC: Attacks and counter-measures", Proc. Eur. Intell. Secure Information. Conf. (EISIC), pp. 126129, Nov. 2019.
5. Abdulla Mamu, Mohammad Yuosuf, Shamim Kaiser, Sheikh Riad Hasan, Md Salahuddin Bhuiyan,―Secure &TransparantKyc for Banking System using IPFS & Blockchain Technology,‖ 2020 IEEE Region 10Symposium (TENSYMP) At: Dhaka, Bangladesh

6. Yash Kumar, Gaurav Sharma, Komal Sakpal, Prof. A. Umbare ,—EKYC Mobile Application Using Optical Character Recognition,‖ ijert.org, vol. 9, Issue 2, February 2020
7. Nikolaos Kapsoulis, Alexandros Psychas, Georgios Palaiokrassas, Achilleas Marinakis, AntoniosLitke, Theodora Varvarigou,—KYC Implementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture, ‖ mdpi.com, February 2020
8. M. Mohamed Rafik, Dr. T. Ananth Kumar, — Blockchain technology For KYC Document Verification, ‖ ijics.com, Vol. 6, Issue 3, March 2019
9. Betty P, Mohana Geetha D,—Design and Experimentation of Face liveliness Detection using Temperature Gradient and Image Quality Assessment,‖ ijrte.org, Vol. 8, Issue 3, September 2019
10. Prince Sinha, Ayush Kaul,— Decentralized KYC System, ‖ irjet.net, Vol. 05, Aug 2018
11. Jose Parra-Moyano, Omri Ross, —KYC Optimization using Distributed Ledger Technology, ‖ doi.org, December 2017
12. Prakash c. mondal, Rupam Deb, M. N. Huda, "Know your customer (KYC) based authentication method for financial services through the internet", IEEE,Dec
13. Prakash Chandra Mondal, Rupam Deb, Mohammad Nurul Huda,—Transaction authorization from Know Your Customer (KYC) Information in Online Banking,‖ The 9th International Conference on Electrical and Computer Engineering, December 2016
14. Anurag Soni, Reena Duggal, —Reducing Risk in KYC for Large Indian Banks Using Big Data Analytics, ‖ International Journal of Computer Applications, Vol. 97, July 2014
15. Jitendra Kumar, K. K. Pattanaik, Arvind Pandey — Big Data: A Source of KYC In Reference of IndianBanking, ‖ Skoch Development Foundation, March 2013

SCRUTINIZING THE CHALLENGES TO DEVELOP SMART HEATH CARE SYSTEMS USING INTERNET OF THINGS

Akanksha D. Singh
Faculty of Engineering and Information Sciences, University of Wollongong in Dubai, Dubai, UAE
akankshasingh222@gmail.com

ABSTRACT

Internet of Things (IoT) is one of the digital technologies that has been in spotlight in recent years to push humans towards utilizing digitized healthcare services constituting Smart Healthcare systems. It focusses on remote monitoring of patients, early diagnosis of diseases, prevention of its spread, its treatment and education using digital technologies to maintain well-being and quality of life among vulnerable populations of society. Therefore, its implementation and successful facilitation within society is a major challenge to be addressed. IoT framework consists of interconnected devices at various levels of abstraction to form a complex close-knit system, which can be used in various application fields. This paper discusses about the state-of-the-art in each level of abstraction, evaluates its strengths and investigates technological and societal challenges associated with its implementation for reliable, reproducible, secure and sustainable generation of data therein for Smart healthcare systems. Accordingly, recommendations are made for future research directions.

Keywords: *Internet of Things (IoT), Smart Healthcare Systems, Sensors*

I. Introduction

Health is an essential aspect of life, be it for the elderly population or for thecurrent generation.Statistically, the elderly population aged 65 has exceeded761 million globally in 2021 [1] and number of older persons is projected to double to 1.5 billion in 2050. As the world enters a new stage of development under the pressure of an aging population, the related rise in chronic illness is placing significant strain on modern healthcare. The demand for resources from the hospital beds to doctors and nurses has also increased. Modern lifestyles, such as unhealthy diets, sedentary work, and high-stress levels, have led to an increase in chronic diseases such as obesity, diabetes, and heart disease in the current generation including them in the vulnerable population group along with the aging population. These conditions require ongoing medical management and monitoring, making healthcare an essential aspect of maintaining good health and quality of life. Healthcare is also essential to ensuring the well-being and productivity of the workforce of a nation. Moreover, access to healthcare is a basic human right and everyone should get it regardless of their socio-economic background.
A solution is apparently needed to minimize the pressure on healthcare systems whilst continuing to provide high-quality care to the vulnerable groups. To better serve the elderly and their families, the health care sector is transitioning from conventional family-based care system to the smart care system. Most developing nations are expanding their smart care sectors and modernizing their healthcare infrastructure toprovide quality health facilities available to all at affordable rates[2].Internet of Things (IoT)[3] is one such framework of interconnected technologies, that has become the apple of an eye among the researchers and has the potential to be a viablesolution to ease the load on the healthcare systems.

Simply speaking, IoT refers to a network of physical devices that are connected and integrated to transmit data between sensing devices and systems over the internet [4-6]. Theoretically, it entails streamlining data interchange and storing the data on a secure cloud server, where a network of connected computing devices can share data and communicate with one another across the server. An exponential expansion has been observed in the production of IoT connected devices from around 15 billion in 2023 and predicted to double by 2030. IoT has emerged as a crucial enabler of the deployment of heterogeneous applications because of recent advancements in MEMS technology, large scale integration, and high-speed, low-latency pervasive connectivity. IoT-based services are beneficial for almost all application areas, including transportation, smart home automation, smart health care systems, industrial automation, smart agriculture, and smart cities.

This article offers a distinctive contribution by outlining each essential element of a complete Internet of Things healthcare system. The focal point of the discussion would be sensors for monitoring various health parameters, short- and long-range communications standards, cloud technologies and challenges associated with its implementation. It also offers a thorough analysis of the cutting-edge technologies included in the suggested paradigm and also analyseschallenges associated with each element of an IoT-based healthcare system at device and system-integration level.

The remainder of this paper is structured as follows. Section IIenlists the key elements in Smart Healthcare systems, followed by Section III which demonstrates working of IoT. Section IV demonstrates the functionality of each abstraction level of IoT. Various technologies that can be a part of IoT system for healthcare applications are discussed in Section V. Section VI scrutinizes the various challenges imposed on the implementation of IoT in healthcare systems followed by conclusion in Section VII.

II. Key Elements In Smart Healthcare System

The vision to develop Smart Health care system [7-10] encompassesthe presence of certain key elements, which are highlighted as below:

- Remote patient monitoring: Using tools like wearables and sensors, remote patient monitoring enables medical professionals to keep an eye on patients' health from a distance. This can lower healthcare expenditures, prevent hospital readmissions, and enhance patient outcomes.
- Electronic health records (EHRs): EHRs are digital files that include a patient's medical background, test results, and other crucial health data. Healthcare professionals can access EHRs from many locations, which makes it simpler to coordinate care and prevent repetition of tests and procedures.
- Telehealth: The use of video conferencing and other related technology can enable patients to get medical care remotely, referred to as telehealth. Thus, patients who reside in rural places or have mobility challenges may benefit from better access to care.
- Health information exchange (HIE): HIE enables healthcare professionals to securely communicate patient data, facilitating care coordination and preventing the need for repeated tests and procedures.
- Predictive analytics: Predictive analytics identifies patients who are likely to need hospitalization or who are at risk of contracting specific medical problems using data. This enables medical professionals to act quickly and avert expensive problems.
- Patient engagement tools: Patients can access their health information, make appointments, and contact with their healthcare providers using patient engagement tools including patient portals and mobile apps.
- Cybersecurity: To safeguard patient information and fend off cyberattacks that can jeopardize the security of the healthcare, cybersecurity holds special place in Smart Healthcare systems.

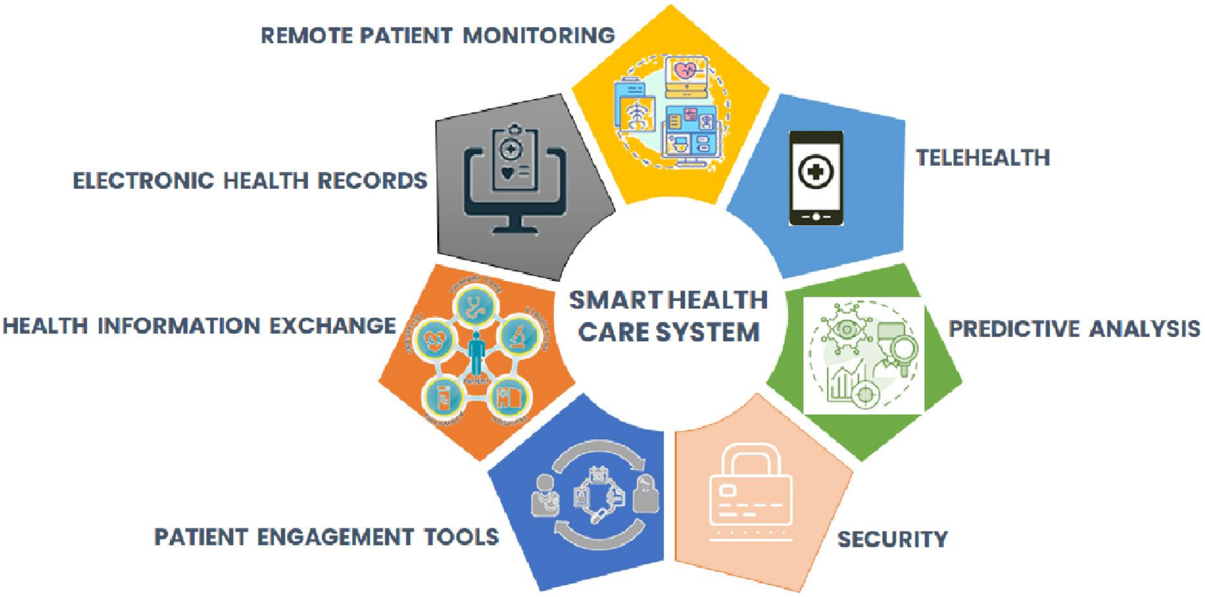


Fig. 1. Key elements of Smart Healthcare System

III. How IoT Works?

The Internet of Things (IoT) is a network of real-world physical devicesthat are embedded with sensors, processors, software, and other technologies that connect over any communication network or Internet to collect and exchange data with other devices and systems [11-13]. The role of IoT is to seamlessly integrate the physical and digital worlds so that processes may be controlled, monitored, and automated.

The operation of IoT requires the following key elements:

3.1 Devices:

Devices are the physical objects that are equipped with sensors, actuators, and network connectivity to collect and exchange data. For example, temperature or humidity sensor, wearables, cameras, drones, etc. The sensors enable the devices to interact with the physical world, sense and collect the data thereof.In order to exchange the data for analysis and use with other devices at the Central system, the network connectivity is required.

Thus, the devices can be categorized as:

a) End Devices: These are the devices that are located at the end of the network, mostly in the 'Sensing Layer' and are responsible for measuring, collecting and transmitting data. For example: sensors, smart meters, and wearables.

b) Gateway Devices: These devices serve as intermediaries between the end devices and the central system and are usually the network devices. They aggregate data from multiple end devices and transmit it to the central system. For example: routers, switches.

c) Cloud Devices: These devices provide cloud-based services for IoT applications. For Example: cloud servers, storage, and processing units.

3.2 Connectivity:

Connectivity is the mechanism that enables devices to exchange data with each other and with the central system. This can be achieved through various wired and wireless technologies such as Wi-Fi, Bluetooth, Zigbee, and cellular networks and requires various communication protocols for its operation. Connectivity can be classified into three categories:

a) Personal Area Network (PAN): For connection of devices within a short range typically few meters. For example: Bluetooth and Zigbee.

b) Local Area Network (LAN): For connection of devices within a building or campus. For example: Wi-Fi and Ethernet.

c) Wide Area Network (WAN): For connection of devices over a large geographical area such as a city or country. For example: Cellular networks, satellite communications.

3.3 Platform:

The platform is the software layer whichfacilitates thedevice management, datastorage and processing (integration,analysis, and visualization)of the collected data. It has the flexibility to be deployed on-premises or on cloud. Platform can be classified into three categories:
a) Device Management Platform: For managing the devices and their connectivity and it provides services such as device configuration, firmware updates, and diagnostics.
b) Data Management Platform: For storage and processing of the data and provides services such as data storage, data analytics, and data visualization.
c) Application Enablement Platform: For enabling the development and deployment of IoT applications, and provides services such as APIs, SDKs, and development tools.

3.4 Application:

This forms the end-product of IoT, wherein the insights gained by thedata collected in the Sensing layer is provided to the end user through various services and applications. They can range from smart home, Precision agriculture, Smart healthcare to industrial automation, predictive maintenance and process optimization.
The IoT framework can be segregated into four layers based on the individualistic characteristics and connected hierarchically from the sensing devices at the bottom layer to the Application layer at the top. It is depicted in Fig. 2.The Smart Healthcare system is developed at the application layer integrating the functionalities from the layers below.

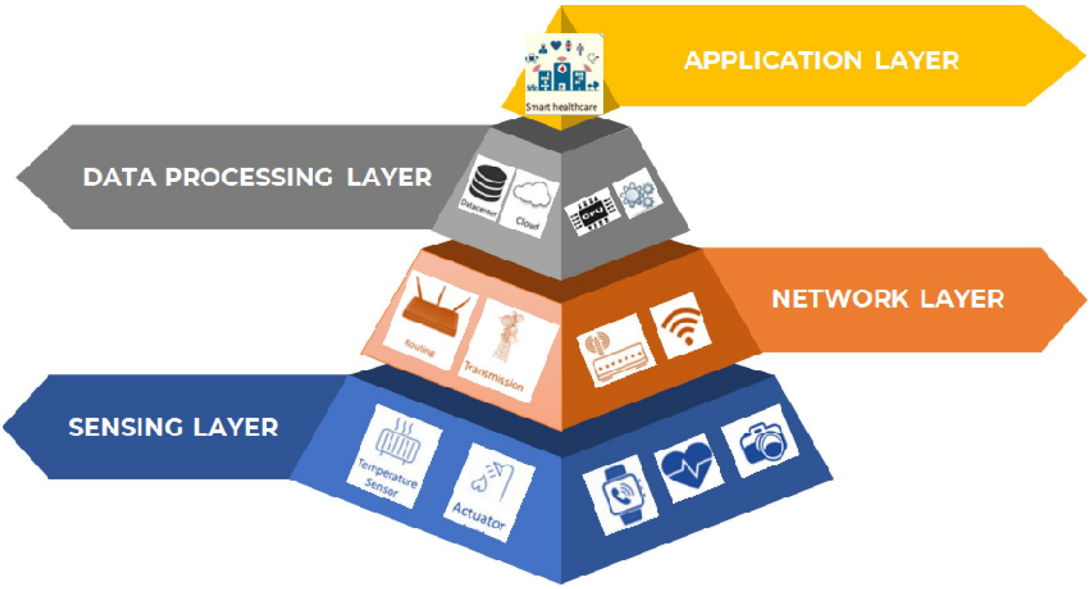


Fig. 2. IoT framework

IV. Layers In The IoT Framework:

This section discusses in detail the various layers present in the IoT framework, its functionalities and the technologies used in it.

4.1 Sensing Layer

The sensing layer of IoT is the foundational layer that enables the capture and transmission of data from the physical world to the digital world for further processes and analyses. The sensing layer consists of various types of sensors, and actuators that are used to measure physical parameters such as temperature, humidity, pressure, light, sound, and motion. The sensing layer plays a crucial role in IoT systems as it enables the real-time data acquisition of data from the physical world, which can then be further processed and analysed [14].
Based on the functionality or application, the sensors can be majorly categorized as:
Physical Sensors: They measure physical quantities such as temperature, pressure, humidity, light, position and motion. Examples include temperature sensors, pressure sensors,

light sensors, Proximity sensors, GPS sensors, accelerometers, gyroscopes, etc.

Chemical Sensors: They measure the chemical parameters such as pH, gas concentration, and pollutant levels. Examples of chemical sensors include gas sensors, pH sensors, and biosensors.

Biological Sensors: Theyusually measure biological parameters such as heart rate, blood pressure, and glucose levels. Examples include ECG sensors, blood pressure sensors, and glucose sensors.

Based on the sensing principle used, the sensors are classified as Optical, Capacitive, Piezoresistive, Piezoelectric, etc. These principles are widely used in the implementation of the sensors. Each type of the sensors mentioned above has been a subject of lot of research in the last 15 years. Miniaturization coupled with high sensitivity, reliable detection of the target analyte has been the focal point of research.Various technologies have been used for its fabrication and various sensor devices and systems have been developed [15]. One of the common technologies is Micro /Nano Electro Mechanical Systems (MEMS /NEMS), Microfluidics, etc. These technologies enable batch production of miniaturized sensors at an affordable price for ultra-sensitive detection of different quantities.

The various technologies used for data communication from the sensing layer includes Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), Near Field Communication (NFC). Each of these technologies has their advantages and must be chosen considering the application field for its deployment.

Biological sensors can be integrated with physical or chemical sensor and a biomedical sensor can be developed. This will play an important role in creating a smart city that promotes health and well-being. Here are some ways that biomedical sensors can be used in a smart healthcare system and insmart cities help to create a safer, healthier, and more sustainable urban environment [16-17]:

- Tracking disease outbreaks: Biomedical sensors can be used to monitor for the presence of pathogens that can cause disease outbreaks. This information can be used to quickly identify and contain outbreaks, preventing them from spreading to other parts of the city.
- Supporting healthcare: Biomedical sensors can be used to monitor patients remotely, allowing healthcare providers to monitor vital signs and other health metrics without requiring patients to come into the clinic. This can help to improve patient outcomes and reduce healthcare costs.
- Promoting physical activity: Biomedical sensors can be used to track physical activity levels and encourage people to be more active. For example, sensors can be placed in parks and other public spaces to track the number of people using them and the types of activities they are engaged in. This information can be used to design more effective exercise programs and promote healthy lifestyles.
- Monitoring air quality: Biomedical sensors can detect the presence of harmful pollutants in the air, such as carbon monoxide, nitrogen oxides, and particulate matter. This information can be used to develop strategies to improve air quality and protect public health.
- Monitoring water quality: Biomedical sensors can detect the presence of harmful contaminants in drinking water, such as lead and bacteria. This information can be used to ensure that water is safe to drink and to prevent outbreaks of water-borne illnesses.

4.2 Network Layer:

The network layer of IoT enables devices in the sensing layer to connect and communicate with each other over the internet. It manages the communication between devices and the exchange of data over various communication protocols [18]. We will enlist the key features of the network layer of IoT and its role in ensuring reliable and secure communication between devices.

- Communication Protocols:

Various communication protocols such as HTTP, MQTT, CoAP, and WebSocket are supported. Each protocol has its pros and cons depending on the application's requirements. For example, HTTP is suitable for transmitting small amounts of data between devices, while

MQTT is more efficient for transmitting real-time data.

- Routing and Addressing:

Routing and addressing protocols enable devices to locate and communicate with each other. One of the fundamental protocols is Internet Protocol (IP), used for addressing and routing data packets over the internet. In addition to IP, other protocols like 6LoWPAN, ZigBee, and Bluetooth Low Energy (BLE) provide additional routing and addressing features to support IoT device communication.

- Wireless Sensor Networks (WSNs):

Management of wireless sensor networks (WSNs) is a responsibility of network layer of IoT. WSNs contains large number of sensor nodes that communicate with each other to collect and transmit data to a central node [19]. The network layer manages the communication between sensor nodes and the central node to ensure efficient data transfer.

- Security and data privacy protocols:

The network layer of IoT plays a critical role in ensuring the security and privacy of data transmitted over the network. IoT devices are vulnerable to cyber-attacks due to their limited processing power and lack of built-in security features. Therefore, the network layer must include security protocols such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Datagram Transport Layer Security (DTLS) to protect data from unauthorized access.

- Quality of Service (QoS):

The network layer of IoT must also support Quality of Service (QoS) features to ensure reliable and on-time data delivery. QoS is essential for real-time applications such as video streaming, where a minimal delay can impact the user experience. Therefore, the network layer must support QoS features such as prioritization, packet queuing, and traffic shaping to ensure timely data delivery.

By understanding the key features of the network layer of IoT, we can design and implement effective IoT solutions that meet the requirements of different applications.

4.3 Data Processing Layer:

The data processing layer of IoT collects, processes, analyses, and stores the data generated by IoT devices. It plays a critical role in a way that it analyses and generates meaningful insights from the massive raw data that can be used to optimize various medical operations, improve patient experiences, and drive innovation.

The key components of the data processing layer of IoT enlisted below and we demonstrate how they work together to enable effective data processing:

- Data Collection:This first step involves collection of data from sensors, devices, and other sources and storage it in a centralized location, such as a database or data warehouse or on cloud. Data can be collected in real-time or at regular intervals, depending on the applicationrequirements.
- Data Processing and Storage: The collected raw data is processed, i.e.filtering of the irrelevant components, sampling of the redundant data,then normalising to a common structured format, which can be relatively easy to store, access,analyzeand visualize. The data can be stored in a data warehouse, a distributed file system, or a cloud-based storage service.
- Data Analysis:Once the data is processed, it can be analyzed to extract meaningful insights. Data analysis involves using statistical and machine learning algorithms to identify patterns, trends, and anomalies in the data. This can include predicting future trends, identifying anomalies and outliers, and detecting correlations between different data sources.
- Data Visualization:Finally, data visualization involves presenting the analyzed data in a visually appealing form,representing the trends in the data and the action-item to be worked on to make data-driven decisions. This can include creating dashboards, charts, and graphs that provide its visual representation.

By understanding the key components of the data processing layer of IoT, organizations can build effective IoT solutions that meet their application requirements.

4.4 Application Layer:

In the application layer of IoT, the communication between the end-users and IoT system occurs via the developed software applications. The main objective is to provide end-users with real-time insights, and alerts, based on the data generated by IoT devices and take appropriate actions for the same. The key components of the application layer of IoT are enlisted as below:

- User Interface:

The user interface includes graphical user interfaces (GUIs), voice interfaces, and chatbots. It allows end-users to view real-time data from IoT devices, set up rules and alerts, and trigger actions based on the data generated by the IoT devices.

- Automation:

Automation in the application layer enables end-users to automate processes based on the data generated by IoT devices. For example, an end-user can set up an alert to be notified when the water level in a pumping unit goes above a certain threshold.

- Integration:

Integration can include APIs, webhooks, and other protocols that enable data to be exchanged between IoT devices and other software systems [20]. Integration is used to enable data to be shared between different systems, such as ERP, CRM, and SCM systems.

- Security:

Security can include authentication, access control, encryption, and other security measures that are used to protect the data generated by IoT devices. Security is critical to ensuring the integrity of the IoT system and the trust of end-users.

By understanding the key components, organizations can develop effective IoT solutions that meet the needs of their end-users.

V. Technologies Integrated With IoT In Healthcare

The technological proliferations in the IoT focussed on healthcare has led to the development of Internet of Medical Things (IoMT). IoMT is the integration of medical devices and wearables with IoT technology to improve patient care and outcomes. This section discusses the technologies that are integrated with IoMT and its importance in healthcare:

- Cloud Computing: It enables the storage and processingof large amounts of data generated by medical devices and wearables [21]. It also enables healthcare providers to access patient data from anywhere, at any time, and on any device.
- Artificial Intelligence (AI):AI is integrated with IoMT to improve patient outcomes. It can be used to analyze patient data in real-time and provide personalized treatment recommendations [22-23].
- Blockchain: It is increasingly being integrated with IoMT to secure patient data and enable secure data sharing between healthcare providers [24-25]. It can be used to create a secure and tamper-proof ledger of patient data, enabling healthcare providers to access patient data securely and efficiently.
- Wearables:Wearables are a key component of IoMT, as they enable patients to monitor their health in real-time and provide healthcare providers with real-time data [15]. Wearables can monitor vital signs such as heart rate, blood pressure, and blood sugar levels, and send this data to healthcare providers in real-time.
- Mobile Applications: They can be used to monitor patient health, provide patients with treatment recommendations, and enable patients to communicate with healthcare providers. Also, they can be used to improve medication adherence and provide patients with personalized health advice.

All the abovementioned technologies are enabling healthcare providers to access patient data in real-time, provide personalized treatment recommendations, and improve patient engagement and adherence to treatment plans. As the healthcare industry continues to evolve, we can expect to see more technologies integrated with IoMT to improve patient care and outcomes.

VI. Challenges In Iot

The smart healthcare industry faces several challenges[26-31], including:

- Data privacy concerns: IoT sensors can collect sensitive data, such as personal health information, person identifying information or financial data. This data must be kept secure to protect the privacy of individuals and avoid disruption in healthcare services. To ensure data security, IoT sensors must be designed with secure communication protocols and encryption mechanisms.

- Device vulnerabilities and Cybersecurity threats:Smart healthcare systems often rely on connected devices, such as wearables and medical sensors, which can be hacked or compromised. Also, it uses various digital technologies, which imposes constant risk of cybersecurity attacks, impacting the operation of smart healthcare systems. Thus, the devices and technologies must be designed from a security perspective and should be regularly updated.
- Cost: The cost incurred in the implementation of smart healthcare systems is high. Additionally, the maintenance and updates in the system will add to the total cost.
- Interoperability challenges: Smart healthcare systems often involve multiple technologies and platforms that should communicate smoothly with each other. Ensuring the interoperability of these systems is a significant challenge.
- Insider threats: Security risks can be imposed by the hospital employees, contractors, and other insiders. They might have access to sensitive patient data and can misuse it.
- Ethical concerns: Ethical concerns might be raisedlike usingthe patient data for research or theirability to develop biased algorithms. Ensuring that these systems are developed and used ethically requires careful consideration of these issues.
- Data management: Smart healthcare systems generate vast amounts of data, which must be stored, processed, and analyzed effectively. Thus, data management infrastructure and tools are required along with analysts and data scientists.
- Power consumption: Many IoT sensors and actuators are battery-powered and require low-power connectivity options, which can limit the range and bandwidth of the devices. This can be a significant challenge for the sensing layer of IoT, as sensors must be able to operate for long periods without needing to be recharged or replaced. To overcome this challenge, IoT sensors are designed to be low power and energy-efficient.
- Data accuracy:IoT sensors must provide accurate data to be useful for analysis and gaining insights. However, many factors can affect data accuracy, such as environmental conditions, sensor placement, and sensor calibration. To ensure data accuracy, IoT sensors must be calibrated regularly and placed in optimal locations.
- Scalability:IoT networks can involve a large number of sensors, which can make it challenging to manage and maintain the network. To ensure scalability, IoT sensors must be designed to be easily deployable and manageable, and network management tools must be used to monitor and maintain the network.
- Training and education: For realising maximum benefits from the smart healthcare systems, healthcare providers and patients must be trained and educated. This may be time consuming and might also involve lots of resources.

The abovementioned challenges with respect to the data privacy, data accuracy, data management, sensor power management, training of the heath personnels and patients must be addressed for the smooth and successful functioning of Smart health care systems. These challenges also open up opportunities for industry stakeholders and researchers to work extensively in it to improve the processes, reduce costs, and enhance the overall user experiences. It requires a comprehensive approach that involves designing sensors and actuators in the sensing layers that are optimized for healthcare IoT, implementing robust security measures, standardizing communication protocols and data formats and developing scalable IoT platforms that can handle large amounts of data.

VII. Conclusion

In this paper, we have discussed in depth about the potential of IoT in healthcare applications. We enlisted the various componentsto be present in a Smart Healthcare system using IoT. A complete end-to-end description of the functioning of each abstraction layer of IoT is reviewed and discussed, with its focus on the smart healthcare system. The technologies that can be integrated into the Smart Healthcare system are described. Finally, we scrutinized the challenges revolving over the implementation of IoT in healthcare. It is concluded that there is need to work on coordinated approaches involving IoT, biosensing techniques, networking protocols, security aspects of the system, as an interdisciplinary research area to cover wide expertise of each field. To address these challenges, collaboration between healthcare providers, technology vendors, regulators, and other stakeholders will be required.The global effort in working on all these challenging aspects will help to leverage the benefits of smart healthcare systems while addressing the challenges that come with their implementation.These challenges can be considered an opportunity and a future research direction to work on for Smart Healthcare system development.

References

1. WHO, Ageing and Health, 2021, Retrieved from https://www.who.int/news-room/fact-sheets/detail/ageing-and-health.
2. J. Li, Q. Ma, A. H. Chan, and S. S. Man, “Health monitoring through wearable technologies for older adults: smart wearables acceptance model,” Applied Ergonomics, vol. 75, pp. 162–169, 2019.
3. Ashton K. That ‘internet of things’ thing. RFID Journal. 2009; 22:97–114.
4. Pradhan B, Bhattacharyya S, Pal K. IoMT-based applications in healthcare devices. J Healthc Eng. 2021:6632599. https://doi.org/10.1155/2021/6632599.
5. Li S, Xu LD, Zhao S. 5G internet of things: a survey. J Ind Inf Integration. 2018 Jun; 10:1–9. https://doi.org/10.1016/j.jii.2018.01.005.
6. Darwish A, Hassanien AE, Elhoseny M, Sangaiah AK, Muhammad K. The impact ofthe hybrid platform of internet of things and cloud computing on healthcaresystems: opportunities, challenges, and open problems. J Ambient Intell HumanComput. 2017;10(10):4151–4166. https://doi.org/10.1007/s12652-017-0659-1.
7. Sarhaddi F, Azimi I, Labbaf S, et al. Long-term IoMT-based maternal monitoring:system design and evaluation. Sensors (Basel). 2021;21(7):2281. https://doi.org/10.3390/s21072281.
8. Islam SMR, Kwak D, Kabir MH, Hossain M, Kwak K. The internet of things forhealth care: a comprehensive survey. IEEE Access. 2015;3:678–708.
9. Muthu B, Sivaparthipan CB, Manogaran G, et al. IOMT based wearable sensor fordiseases prediction and symptom analysis in healthcare sector. Peer-to-Peer Netw.Appl. 2020;13:2123–2134. https://doi.org/10.1007/s12083-019-00823-2.
10. Bisio C, Garibotto F, Lavagetto A, Sciarrone. When eHealth meets IoMT: a smartwireless system for post-stroke home rehabilitation. IEEE Wireless Communications.2019;26(6):24–29. https://doi.org/10.1109/MWC.001.1900125 .
11. Sethi P, Sarangi S. Internet of things: architectures, protocols, and applications.J Electric Comput Eng. 2017:1–25. https://doi.org/10.1155/2017/9324035,9324035.
12. Dang LM, Piran MJ, Han D, Min K, Moon H. A survey on internet of things andcloud computing for healthcare. Electronics. 2019 Jul 9;8(7):768. https://doi.org/10.3390/electronics8070768.
13. Pham M, Mengistu Y, Do H, Sheng W. Delivering home healthcare through a cloud basedsmart home environment (CoSHE). Future GeneratComput Syst. 2018;81:129–140.
14. Landaluce, H.; Arjona, L.; Perallos, A.; Falcone, F.; Angulo, I.; Muralter, F. A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks. Sensors 2020, 20, 2495. https://doi.org/10.3390/s20092495
15. Guo J, Chen S, Tian S, et al. 5G-enabled ultra-sensitive fluorescence sensor forproactive prognosis of COVID-19. BiosensBioelectron. 2021; 181:113160. https://doi.org/10.1016/j.bios.2021.113160.
16. Wang, L.; Jones, D.; Chapman, G.J.; Siddle, H.J.; Russell, D.A.; Alazmani, A.; Culmer, P. A Review of Wearable Sensor Systems to Monitor Plantar Loading in the Assessment of Diabetic Foot Ulcers. IEEE

Trans. Biomed. Eng. (Early Access) 2019. doi:10.1109/TBME.2019.2953630

17. Aroganam, G.; Manivannan, N.; Harrison, D. Review on Wearable Technology Sensors Used in Consumer Sport Applications. Sensors 2019, 19, 1983.
18. Akpakwu GA, Silva BJ, Hancke GP, Abu-Mahfouz AM. A survey on 5G networks forthe internet of things: communication technologies and challenges. IEEE Access.2018; 6:3619–3647. https://doi.org/10.1109/ACCESS.2017.2779844
19. Manirabona A, Fourati LC. A 4-tiers architecture for mobile WBAN based healthremote monitoring system. WirelNetw 2018;24(6):2179–90.
20. Umair M, Cheema MA, Cheema O, Li H, Lu H. Impact of COVID-19 on IoMTadoption in healthcare, smart homes, smart buildings, smart cities, transportationand industrial IoMT. Sensors. 2021; 21:3838. https://doi.org/10.3390/s21113838.
21. Cui M, Baek SS, Crespo RG, Premalatha R. Internet of things-based cloud computingplatform for analyzing the physical health condition. Technol Health Care. 2021.https://doi.org/10.3233/THC-213003.
22. Gulshan V, Peng L, Coram M, et al. Development and validation of a deep learningalgorithm for detection of diabetic retinopathy in retinal fundus photographs. J AmMed Assoc. 2016;316(22):2402–2410. https://doi.org/10.1001/jama.2016.17216.
23. Javed AR, Fahad LG, Farhan AA, et al. Automated cognitive health assessment insmart homes using machine learning. Sustain. Cities Soc. 2021; 65:102572.
24. Park YR, Lee E, Na W, Park S, Lee Y, Lee J. Is blockchain technology suitable formanaging personal health records? Mixed-methods study to test feasibility. J MedInternet Res. 2019 Feb 8;21(2), e12533. https://doi.org/10.2196/12533.
25. Chen HS, Jarrell JT, Carpenter KA, Cohen DS, Huang X. Blockchain in healthcare: a patient-centered model. Biomed J Sci Tech Res. 2019;20(3):15017–15022. https://doi.org/10.26717/bjstr.2019.20.003448.
26. Qiu F. Hospital archives intelligent management system based on 5G network andinternet of things system. Microprocess Microsyst. 2021; 80:103564.
27. Wang Y, Kung L, Byrd TA. Big data analytics: understanding its capabilities andpotential benefits for healthcare organizations. Technol Forecast Soc Change. 2018;126:3–13. https://doi.org/10.1016/j.techfore.2015.12.019
28. Pradhan B, Bharti D, Chakravarty S et al. Internet of things and robotics in transforming current-day healthcare services. J Healthc Eng. 2021:9999504. doi: 10.1155/2021/9999504.
29. Bharathi KS, Venkateswari R. Security challenges and solutions for wireless body area networks. In: Computing, communication and signal processing.Springer; 2019. p. 275–83.
30. Yang, S.; Crisp, M.; Penty, R.V.; White, I.H. RFID Enabled Health Monitoring System for Aircraft Landing Gear. IEEE J. Radio Freq. Identif. 2018, 2, 159–169.
31. Altawy, R.; Youssef, A.M. Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. IEEE Access 2016, 4, 959–979.

THE DETECTION OF MALWARE USING SANDBOX TECHNIQUES

[1]Dr. Heena Farheen Ansari, [2]Kasturi Patil and [3]Sharvari Phatkar
[1]Assistant Professor, [2-3]Projecties
[1-2]Department of Information Technology, [3]Dept. of Computer Technology
Kavikulguru Institute of Technology and Science, Nagpur, India
ansariheena32@gmail.com

ABSTRACT

In the past few years along with developing technologies the number of cyber-attacks is targeting the systems be it LINUX or WINDOWS, which is getting worse day by day. Malicious software of malwares are programs that are basically created to harm, interrupt communication between client and the server or damage computers. Malwares has always been a menace to digital world but with a quick increase in the use of internet, the effects of the malwares become severe and cannot be ignored. A lot of malware detectors have been created, the effectiveness of these detectors and in this paper, a detailed review of malwares types are provided, malware analysis using sandbox and detection techniques are studied and compared.

Keywords: *Malware, Malware analysis, Analysis using Sandbox techniques*

I. Introduction

Today the internet has become an unavoidable part of our lives as it connects us to the entire world and, furthermore, provides the amenity of everything being just one click away. But along with this supremacy, the increased access to the internet has been accompanied by the great threat of "The MALWARE". Malware is simply malicious software that is used by an untrustworthy third party to attack various systems for a variety of reasons, the most common of which is the theft of sensitive data and the demand for money.

The recent incident where the leading private company Solar Industries Limited, an explosives manufacturing unit, got trapped in the ransomware attack [again, a type of cyber-attack], cost them their sensitive data leak. As per reports, around 2TB of data on solar explosives got leaked, and there might be chances it got into the dark web. These increasing attacks have now targeted the big firms. To counter this situation, both security communities and companies must put effort into developing methods to protect their assets using security products.

To protect legalised and innocent users from these threats, we have security vendors like antivirus software detection and analysis procedures. Various analysis tools can dynamically analyse the malware and detect it; the tools use cloud computing, which makes them more secure. The main idea of this study is to identify the security systems on various operating systems.

II. Literature Survey

A. Malware Analysis and Classification: A Survey

The research focuses on malware and types of malware analysis. Signature based techniques are only able to detect malware that has already caused some damage [I.e., Known Malwares].

Malware analysis: helps to detect and understand the behavior of the malicious code. Like how it will act and what pattern it can follow, etc. Types of malware analysis:

1. Static Analysis analyzing without execution]
2. Dynamic Analysis [Analyzing behavior of malicious code that is being executed in the secure virtual environment]

B. A Study on Malware and Malware Detection Techniques

This research paper discusses the types of malware aka viruses discovered so far and the techniques to detect them. Malware Types: Virus, Worm, Trojan Horse, Rootkit, Spyware, Adware, Cookies, Keyloggers. Due to the limitation of the existing malware detection techniques, the machine learning and data mining methods are combined with existing detection methods to add efficiency in the detection process. Two malware analysis techniques:

I. Static Analysis
II. Dynamic Analysis

Three major malware detection techniques:

I. Signature based detection
II. Heuristic based detection
III. Specification based detection

C. Malware Analysis

This research paper Malware Analysis ("Nirav Bhojani" 2014) states that Malware or malicious software designed to damage the system without admin's consent. VIRUS, TROJAN, WORMS, SPYWARE, ROOTKIT are all types of malwares and the process of determining the behavior and characteristics of these malware is known as malware analysis[2].

Different techniques used for static malware analysis:

I. File Finger printing
II. File Format
III. AV Scanning
IV. Packer Detection
V. Disassembly

Dynamic Malware analysis Malware is being observed and controlled from virtual enviroment.

Types of Dynamic malware analysis:

I. Filemon
II. Norman Sandbox
III. Joebox

D. Practical Malware Analysis based on Sandboxing

This paper states that behind every thousand malware attacks we have only 50 malware analyst.

Types of malware analysis:

I. Static analysis
II. Memory analysis
III. Dynamic analysis or behavioural analysis
IV. Automated analysis

[Cuckoo: popular and mostly used sandbox] The automated Cuckoo solution produces the same results in a considerable smaller time. Cuckoo allows guest machine using virtual Box ,permitting the analysis of files and applications on most OS and facilitates the analysis of URLs.

E. Automated Malware Analysis System and Its Sandbox for Revealing Malware's Internal and External Activities

This paper Automated Malware Analysis System and Its Sandbox for Revealing Malware's Internal and External Activities ("Daisuke INOUE" 2009) states that the major security threat that has been recognized on internet is Malware. In this paper basically the external (i.e. network) activities of malware are focused.

Malware Analysis Two Approaches:

I. Static analysis: White-box approach
II. Dynamic analysis: Black-box approach

MicS: Automted Malware Analysis System

Sandbox Analysis In order to extract malware's internal & external activities, they constructed analysis environment in which real machine called Victim host and internet emulator.

F. An Emerging Malware Analysis Techniques and Tools: A Comparative Analysis

This paper An Emerging Malware Analysis Techniques and Tools: A Comparative Analysis ("Arkajit Datta" 2021):

Malware analysis and detection methodology:

➢ Static
- Signature based
- Heuristic based

File based, Weight based, Rule based, Generic based

➢ Dynamic
- Behaviour based

➢ Hybrid

Malware detection tools:

Static tools: PE id, PE view, Hex Editors, Bin Text, etc.

Dynamic tools: process explorer, Olly Dbg, Burp suite, Sandboxes, etc

III. Malware And It's Types

Malicious software, or malware as it is more colloquially known, is designed to harm or exploit systems, be they the operating system, Android, or Mac. Malware can take multiple forms, from viruses, worms, and trojans to spyware and ransomware. This malware has proven to be very dangerous and harmful for the systems, so because of these malwares demonstrated high risk and damaging effects on systems, it is now crucial to defend all systems against these attacks. This can be done by using antivirus software, keeping the operating system up-to-date, and avoiding suspicious links and attachments.

Following are the malwares that are identified so far:

1. VIRUS or Vital Information Resources Under Siege: VIRUS is the malware that basically is the computer program that, when it enters the system, modifies the target system to perform the unwanted functions without the owner's concern to get access to sensitive data. A virus requires the host system and an executable file to enter the system; in other words, because the virus is an executable file, the user must execute it.
2. WORMS: Worms are the type of malware that replicates itself and spreads over a network without requiring the user to execute any infected files. Unlike viruses, worms can spread without needing a host program or file to infect. Worms can cause significant damage to target systems by consuming bandwidth and system resources, spreading to other computers, and stealing and deleting data.
3. Trojans: The Trojan, or Trojan horse, can change its appearance to look like legitimate software. Trojans, unlike viruses and worms, do not need to replicate themselves, but because they are standalone programs, they affect other systems without the need for external assistance. It can be used to steal sensitive information, keep a spy on user activities, download and install additional malware, and take control of the target computer.
4. Rootkit: This malware is designed to conceal its presence on a computer system via backdoor entries, allowing an attacker to gain unauthorized access and control of the system. Rootkits are notoriously difficult to remove because they are designed to avoid detection by antivirus and other security software.
5. Ransomware: Ransomware is a type of malicious software (malware) that encrypts the victim's files or entire computer system, rendering them inaccessible to the user. The attackers then demand payment, typically in the form of cryptocurrency, in exchange for the decryption key that can unlock the victim's data.

IV. Malware Analysis

To protect the operating systems from the ever-increasing malware, the process of malware analysis is performed. Malware analysis is the process of examining malicious software to understand its workings, patterns, and behaviors. The central goal of malware analysis is to understand the behaviors of the malware and develop methods to detect and remove it. Malware analysts often use a variety of tools and techniques, including disassemblers, debuggers, sandboxes, and other network analysis tools. It is a complex process that requires specialized knowledge and tools because it is an ongoing process as new types of malwares are constantly developed.

There are two main types of malware analysis: Static and Dynamic malware analysis.

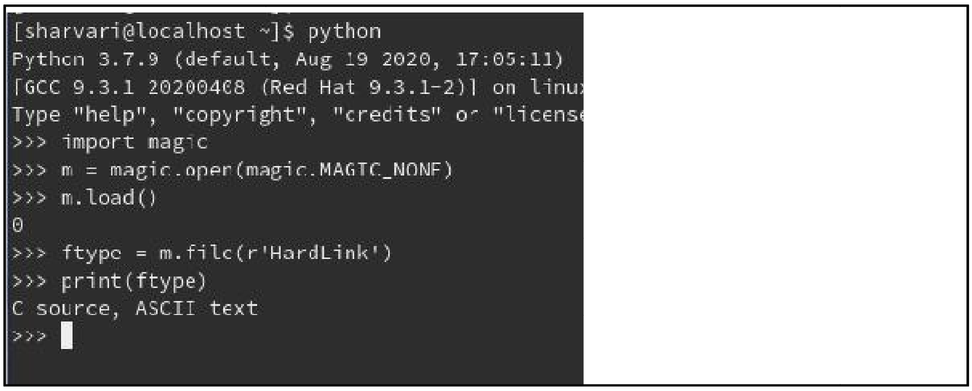
1. Static Malware Analysis

Static analysis of malware involves looking at the code rather than running the dangerous file. Without the risk of causing the malware's negative side effects, this type of investigation can be useful for understanding the threat's characteristics and behavior.

The basic steps to be followed in static analysis are as follows:

1. The first step of static analysis is to identify the file type containing the malware. This can be done by examining the file extension or by using the file identification tool. One way to determine the file type is using Python:

In Python, the python-magic module is used to determine the file type. The following figure shows the identification of a file using python-magic.



```
[sharvari@localhost ~]$ python
Python 3.7.9 (default, Aug 19 2020, 17:05:11)
[GCC 9.3.1 20200408 (Red Hat 9.3.1-2)] on linu
Type "help", "copyright", "credits" or "license
>>> import magic
>>> m = magic.open(magic.MAGIC_NONE)
>>> m.load()
0
>>> ftype = m.file(r'HardLink')
>>> print(ftype)
C source, ASCII text
>>> 
```

2. Code Analysis: Once the file type is identified and the malware is disabled (if any), the code is analyzed for potential vulnerabilities and malicious behavior. This involves looking at the code constructs such as API calls, system calls, and network connections.
3. Function Identification: Once the code analysis is done, the functions of the malware can be identified. This involves examining the code for functions such as the main function, the encryption function, etc.
4. Signature Creation: To identify malware that has the same pattern and behavior, the signature is created. This signature can be used by anti-virus software to identify and block malware.
5. Payload Analysis: Finally, the payload is analyzed, where the files created by the malware modify or delete any data that is being sent out.

2. Dynamic Malware Analysis

Dynamic malware analysis involves running the malware in a virtual, isolated environment to observe the behavior of the malware and analyze its activities. This is typically done using sandboxing techniques, which allow the malware to be executed in an isolated and controlled environment without affecting the host machine.

The process of dynamic malware analysis involves the following steps:

1. Setup the environment: Before executing the malware, the setting up of an isolated environment is required. For this paper, the isolated environment, i.e., sandbox, that is being used is the cuckoo sandbox.
2. Execute the malware: Once the environment is setup, execute the malware in the controlled environment and allow it to execute.
3. Observe behavior: While the malware is running, observe the behavior and activities of tools like network sniffers, process monitors, and system event loggers.
4. Analyze results: After the malware has finished its execution, the result is being analysed and documented about the malware's behavior and pattern. This includes identifying any command-and-control servers used by the malware, and any malicious activity performed by the malware.

Dynamic analysis is an important tool for detecting and analyzing malware, as it allows the analyst to observe the actual behavior of the malware in a controlled environment.

V. Sandbox

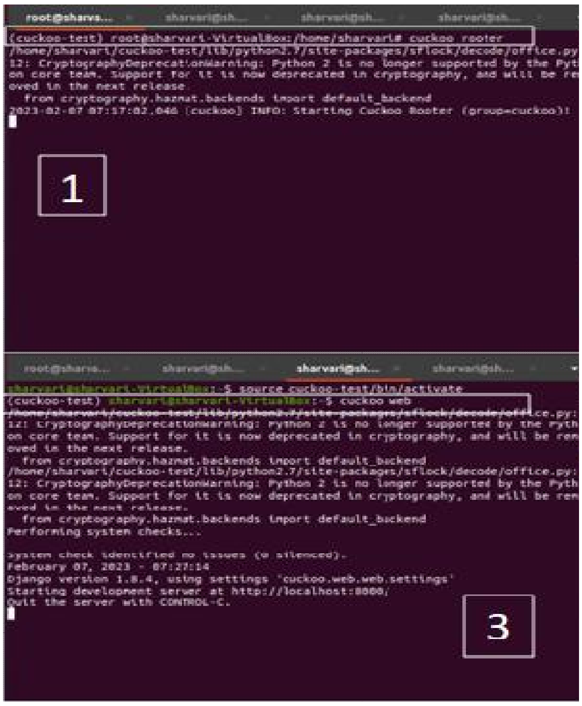
The sandbox is a safe and experimental space that allows the user to execute and evaluate software or code. The purpose of the sandbox is to isolate the code being executed from the rest of the system to protect it from any potential harm or damage.

In a sandbox, the code is executed with limited privileges, access to resources, and network connectivity, which leads to minimum harm to the system. There are different types of sandboxes, including hardware sandboxes, virtual machine-based sandboxes, and container-based sandboxes. Each type has its own advantages and disadvantages and is used for different purposes depending on the requirements of the use case.

The sandbox used in this paper for the research purpose is cuckoo sandbox.

1. Cuckoo Sandbox Analysis

Cuckoo sandbox is a open-source software that allows the user to automate the analysis of potentially malicious files or URLs. It works by running the suspicious code in a controlled insolated environment, observing its behavior, and providing detailed reports on its actions[9]. Cuckoo sandbox analysis starts with the background process, in which the cuckoo sandbox scans and analyzes all the incoming files for maliciousness.



```
(cuckoo-test) root@sharvari-VirtualBox:/home/sharvari# cuckoo rooter
/home/sharvari/cuckoo-test/lib/python2.7/site-packages/sflock/decode/office.py
12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Pyt
on core team. Support for it is now deprecated in cryptography, and will be re
oved in the next release.
  from cryptography.hazmat.backends import default_backend
2023-02-07 07:17:02,046 [cuckoo] INFO: Starting Cuckoo Rooter (group=cuckoo)!
```

```
sharvari@sharvari-VirtualBox:~$ source cuckoo-test/bin/activate
(cuckoo-test) sharvari@sharvari-VirtualBox:~$ cuckoo web
/home/sharvari/cuckoo-test/lib/python2.7/site-packages/sflock/decode/office.py:
12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Pyth
on core team. Support for it is now deprecated in cryptography, and will be rem
oved in the next release.
  from cryptography.hazmat.backends import default_backend
/home/sharvari/cuckoo-test/lib/python2.7/site-packages/sflock/decode/office.py:
12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Pyth
on core team. Support for it is now deprecated in cryptography, and will be rem
oved in the next release.
  from cryptography.hazmat.backends import default_backend
Performing system checks...

System check identified no issues (0 silenced).
February 07, 2023 - 07:27:14
Django version 1.8.4, using settings 'cuckoo.web.web.settings'
Starting development server at http://localhost:8000/
Quit the server with CONTROL-C.
```

The above image is a visual representation of the cuckoo backend process. The first window with the cuckoo rooter command limits the use of commands with root privileges.
Following the limitation of the use of commands, the cuckoo sandbox is being started at the backend so that whatever file enters the system will be scanned and a report of the same can be generated in the log files. Then the third window is for starting the cuckoo web, in case any manual uploading of file is required. Once the cuckoo web is started, it starts on the 8000 port by-default[9].
Some of the log-files generated by cuckoo are:

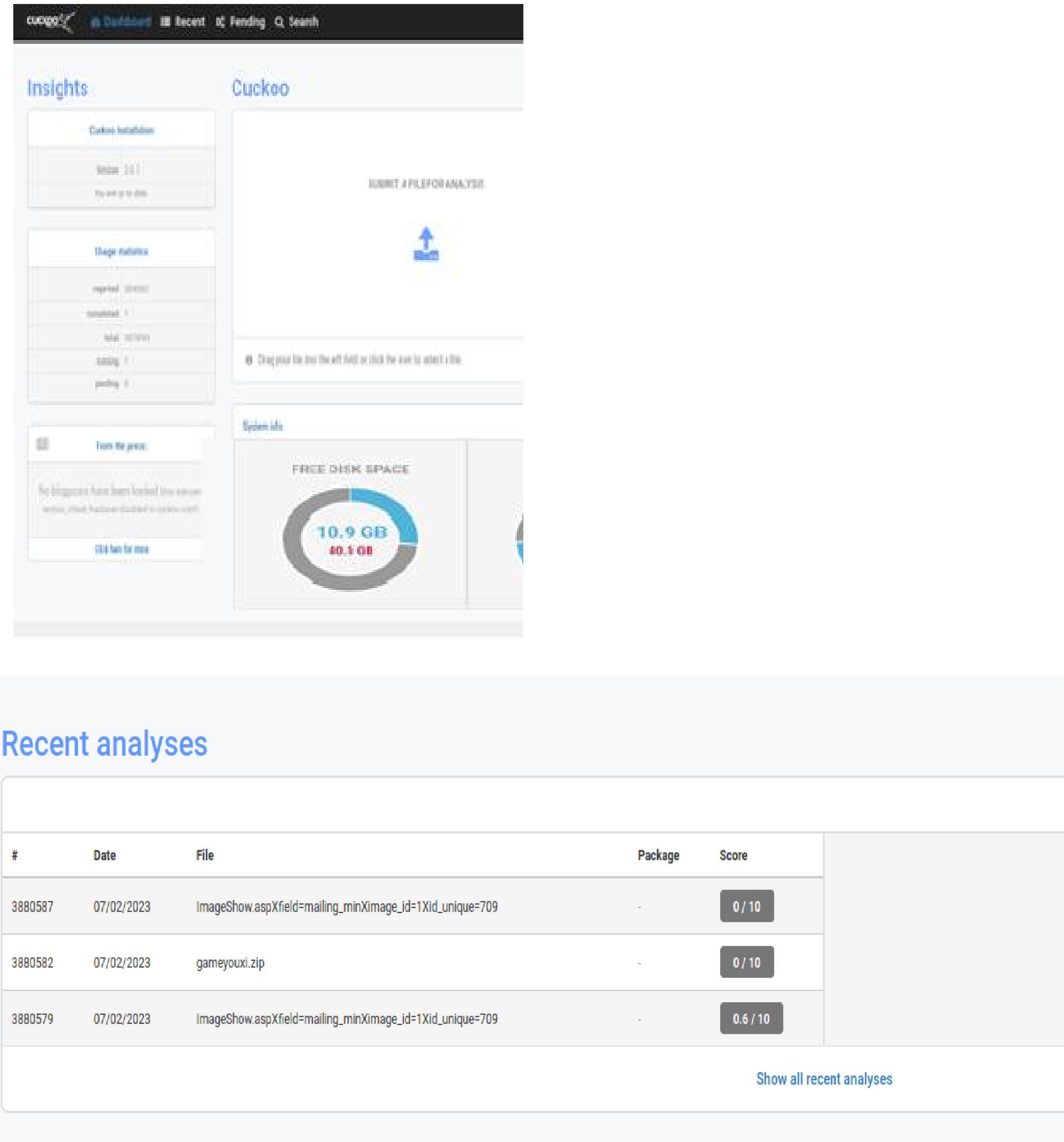
1. Cuckoo.log: this is the main log file that contains the information about the overall analysis process, including the configuration of the sandbox, the tasks submitted for the analysis and the analysis results. Whatever file is being scanned while the sandbox is active and running in the background, is reported in cuckoo.log file.
2. Api.log: this log file contains the information about the API calls made by the cuckoo sandbox web interface.
3. Debug.log: This log file contains additional debugging information that can be used for troubleshooting the issues with the cuckoo sandbox configuration.

Below are some sections of the report generated by cuckoo Sandbox after analysis.

Summary analysis: The summary runner contains details, which punctuate the train sizes, hashes, and more. The right side of the summary runner shows a score that's assigned to the train grounded on how the tool deems it vicious. The score is graded from zero, which means the document or train is benign or inoffensive, to ten, for exorbitantly vicious lines. Cuckoo Sandbox also highlights specific details of the analysis, similar as when the train was analyzed, the time taken, and the type of routing used. The summary runner also shows intriguing malware autographs in the farther details section. train autographs have blue, red, and unheroic colour canons. A blue hand shows that the train is benign; unheroic-enciphered lines have medium pitfalls; and autographs marked red mean that Sandbox has linked vicious conditioning, similar as keylogging exertion or oohing IP addresses. ditz Sandbox has screenshots from the guest device at the end of the summary runner, which had the infected malware. These screenshots are useful in analyzing ransomware since utmost rescue dispatches are displayed.

Behavioral Analysis As the name suggests, the behavioral analysis shows all the malware's conduct on the guest machine. For case, the malware may produce a series of lines or other means of discharging itself, also known as process injection.

Network Analysis The network analysis runner has multiple tabs that filter reports grounded on specific network business protocols. Malware judges can filter network analysis reports to include TCP, DNS, ICMP, IRC, UDP, and HTTP business generated by malware.



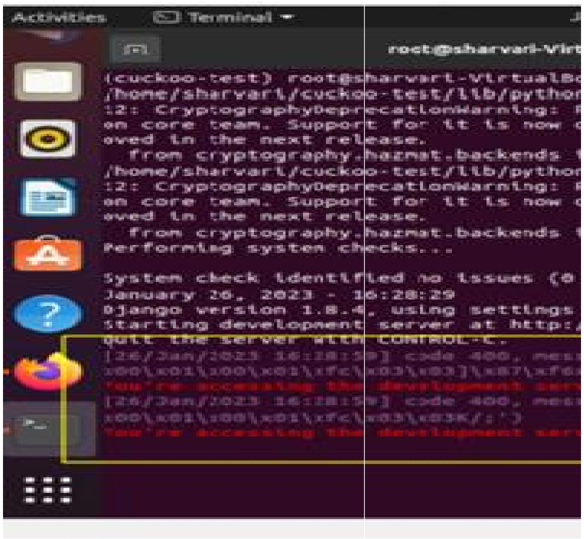
Recent analyses

#	Date	File	Package	Score
3880587	07/02/2023	ImageShow.aspXfield=mailing_minXimage_id=1Xid_unique=709	-	0 / 10
3880582	07/02/2023	gameyouxi.zip	-	0 / 10
3880579	07/02/2023	ImageShow.aspXfield=mailing_minXimage_id=1Xid_unique=709	-	0.6 / 10

Cuckoo Web

VI. Issues With The Current Cuckoo Version

The latest versions of the Cuckoo Sandbox are unmaintained, so any open issues or pull requests are most likely not to be processed. In the scenario where every system must be in its safest place, the cuckoo sandbox supports the http protocol instead of https. This makes Cuckoo Web quite vulnerable, as in the case of a third-party attack, the uploaded file may get stolen. The connectionless communication with HTTP is not encrypted, while in the case of https, the communication is end-to-end encrypted.



```
(cuckoo-test) root@sharvari-VirtualBo
/home/sharvari/cuckoo-test/lib/python
12: CryptographyDeprecationWarning: P
on core team. Support for it is now d
oved in the next release.
  from cryptography.hazmat.backends i
/home/sharvari/cuckoo-test/lib/python
12: CryptographyDeprecationWarning: P
on core team. Support for it is now d
oved in the next release.
  from cryptography.hazmat.backends i
Performing system checks...

System check identified no issues (0
January 26, 2023 - 16:28:29
Django version 1.8.4, using settings
Starting development server at http:/
Quit the server with CONTROL-C.
[26/Jan/2023 16:28:39] code 400, mess
x00\x01\x00\x01\xfc\x03\x03]\x87\xfe
You're accessing the development serv
[26/Jan/2023 16:28:39] code 400, mess
x00\x01\x00\x01\xfc\x03\x03K/:')
You're accessing the development serv
```

Another problem with the current cuckoo sandbox is the python version supported by it. Cuckoo does not support the newer versions of Python (say, from Python 3 onwards). Python2 is the only version(s) it supports. Most importantly, python developers had also decided not to support upstreaming of the python2 version. And Debian will no longer support the packages relying on Python2, so those packages will start breaking. The vmcloak tools that are required by Cuckoo Sandbox for creating and using those virtual machines for malware analysis demand the newer Python versions. This is where the conflict occurs.

VII. Conclusion

As per the reached research analysis for Dynamic malware analysis the Black-Box approach is the way for us to overcome the limitations of existing system. Sandbox briefly summarize the objectives of the analysis and the steps taken to complete it.

Along with, it also discusses the findings from tha analysis including a malware detection, network activities and other suspicious behaviour Sandbox will also evaluate the threat posed by the analyzed sample, by rating the threat on the scale of 20. Overall it provides a clear and concise summary of the analysis and provide actionable recommendations for addressing any security threats detected.

References

1. A Survey on Automated Dynamic Malware Analysis Techniques and Tools, http://www.seclab.tuwien.ac.at/papers/malware_surv ey.pdf
2. Malware Analysis & its Application to Digital Forensic, http://www.enggjournals.com/ijcse/doc/IJCSE12-04- 04-023.pdf
3. Firdausi, I., Erwin, A., & Nugroho, A. S. (2010, December). Analysis of machine learning techniques used in behavior-based malware detection. In 2010 second international conference on advances in

computing, control, and telecommunication technologies (pp. 201-203). IEEE

4. Adelstein, Frank, Matthew Stillerman, and Dexter Kozen. "Malicious code detection for open firmware." Computer Security Applications Conference, 2002. Proceedings. 18th Annual. IEEE, 2002.
5. Hashemi H, Azmoodeh A, Hamzeh A, Hashemi S (2017) Graph embedding as a new approach for unknown malware detection. J Comput Virol Hacking Tech 13:153–166. https://doi.org/10.1007/s11416-016-0278-y
6. Park JH (2017) Novel approaches for applying linguistic processing techniques based on pattern recognition and machine learning. JIPS (J Inf Process Syst) 13:643–652
7. Mobile Threat Report Q1, http://www.fsecure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_ 2014.pdf (Last Access: August 2014)
8. C. H. Malin, E. Casey, J. M. Aquilina, “Malware Forensics Field Guide for Linux Systems”, Syngress, 2014.

REVIEW PAPER: ANALYSIS OF CARBON NANOTUBE FOR LOW POWER NANO ELECTRONICS APPLICATIONS

Pradeep Singh Yadav[1], Dr. Chinmay Chandrakar[2] and Dr. Anil Kumar Sahu[3]
[1,2]Shri Shankaracharya Technical Campus, Bhilai
[3]Bharat Institute of Engineering and Technology, Hyderabad
pradeepyadav@sstc.ac.in, chinmay_sscet@yahoo.ac.in, anilsahu82@gmail.com

ABSTRACT

In the area of nanotechnology, carbon nanotubes are a notable and remarkable invention. CNT started in nanoelectronics field in 1991.Its structure is much similar to the structure of graphite. CNTs are small in size, light weight, good strength and good conductivity made them the building blocks of the futuristic new technologies. CNTs has promised to be the catalyst for the next revolution in technology. Today, a broad range of processes are available to produce various types of CNTs depending on the rolling times of graphite sheets. In this review paper different types of CNTs, its properties, ways of their synthesis – arc discharge method and chemical vapour deposition, and application has been covered.

Introduction

Iijima discovered carbon nanotubes in 1991. (CNTs). Nanoscience has arisen as a new discipline of materials science understanding since then. Millions of dollars have been poured to unravel the mysteries of the revolutionary materials. Carbon nanotube is a cylindrical tube of graphene sheet when rolled or folded. Similar to graphite, carbon nanotubes are composed of sp2 linked carbon atoms.Graphene is a carbon allotrope of single layer atoms bonded in a hexagonal pattern. It is the thinnest known material having high thermal stability, elasticity, electrical conductivity and lowest resistivity. Carbon nanotube are constructed with diameter in nanometer and length can be of any millimeters.Carbon nanotubes are incredibly light, flexible, and have 200 times the mechanical tensile strength of steel. Since they are extremely chemically stable and don't react with other chemicals unless they are subjected to high temperatures and oxygen, they have the property of being corrosion resistant.Various nanomaterials can be used to fill the hollow inner section. Graphene is one of the most compelling allotrope of carbon consist of a single layer of atom arranged in a nanostructure. Most commercial graphene has more than one layer of atoms. Graphene also varies in forms from nanoplates to powder to graphene oxides and many more. But using graphene is not as simple as “running like a wind”. Researchers are attempting to learn more about how they may enter the body and what consequences they may have. Carbon nanotubes are divided into three kinds based on the layers of a graphene sheet: single-walled carbon nanotubes (SWCNT), double- walled carbon nanotubes (DWCNT), and multiwalled carbon nanotubes (MWCNT). The armchair, zigzag, or chiral pattern in which the graphene layer rolls determines the electrical properties of the nanotube. The zigzag and arm chair SWCNT are achiral while helical SWCNT are chiral. Electrical conductivity is provided by the SWCNT, while the other two behave as semiconductors.

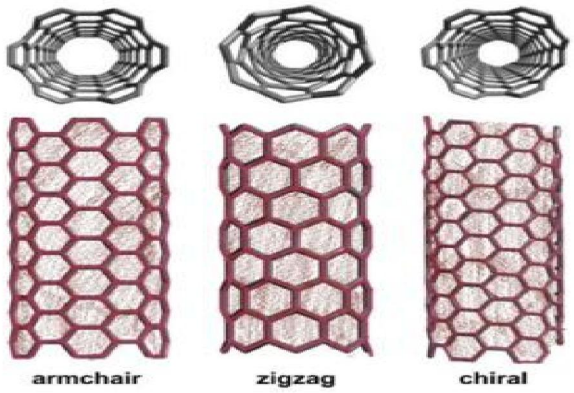


Figure 1. armchair, zigzag and chiral

Each type of a carbon nanotube has different properties and applications. True nanotechnology is demonstrated by
carbon nanotubes. They are molecules with a diameter of around a nanometer that can be chemically and physically controlled in extremely beneficial ways.They can be used in materials science, electronics, chemical processing, energy management, and a large

range of other disciplines.Its industrial uses include papermaking, printing, agriculture, steel manufacturing, and polymer chemistry, among others. CNTs are also functional in the field of biomedical. CNTs are used to destroy breast cancer tumour by antidoting the protein of cancer cell, also used in tissue regeneration, gene therapy, infection therapy and so on. Researchers looked at the toxicity of various kinds of carbon nanotubes and their subproducts, and it is strongly suggested that they be employed in clinical trials before being released to the general public.Currently, three distinct processes are used to create CNTs: chemical vapour deposition, graphite laser ablation, and arc discharge (CVD). In the first two processes, graphite is burned electrically or by a laser, and the CNTs that develop in the gaseous phase are separated. In all three processes, metal catalysts (such as iron, cobalt, and nickel) are necessary. In the CVD method, there are two different kinds of reactor tubes: horizontal tubes and vertical tubes. In ambient conditions, horizontal tubes are more frequently used in the synthesis of CNTs at temperatures varying from 450°C to 1200°C.

Carbon nanotubes may not be biodegradable due to their strong physical and chemical stability.However, certain CNT degradation methods have been established. Peroxidases, neutrophils, and macrophages are examples of approaches that have shown promising outcomes.The most obvious drawback of carbon nanotubes is their inability to dissolve in water when exposed to any medium. To address this issue, carbon nanotubes are subjected to surface modification, which involves stable expertise in the field of the surface with suitable hydrophilic substituents and reaction chemistries that can enhance both aqueous solubility and biocompatibility.

Single Walled Carbon Nanotube (Swcnt) –

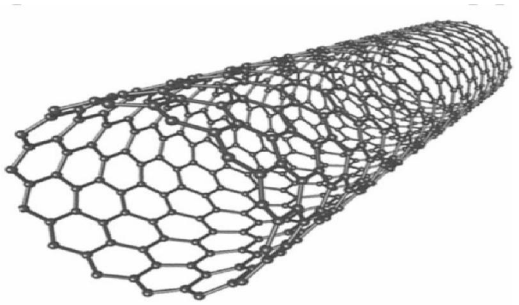


Figure 2. carbon nanotube with single wall

Single walled carbon nanotubes with single wall is nothing but a cylinder of single layer of graphene sheet. They show exceptional thermal, mechanical, and electrical characteristics, making them the most promising nanomaterials for study and application. Carbon nanotube with unity wall can be either metal or semiconductor ,it is based on its chirality vector. Carbon nanotubes have the capacity to display metallic or semiconducting electrical structures, as well as carrier mobilities. Some research has shown they have breaking strength from 13 to 52 GPa, with an average of 30 GPa.

Synthesis

The arc discharge technique, laser ablation, and chemical vapour deposition are the most frequently used processes for the synthesis of SWCNTs (CVD). While CVD is preferred at moderate temperatures, electric arc methods work at high temperatures. In an inert gas chamber, an arc discharge growth process is performed using two graphite electrodes. The two electrodes (or poles) are connected to a DC power source, allowing electric current to pass through the electrode configuration. When using graphite rods, discharge is distributed inside the chamber as soot. Single walled carbon nanotubes are created in the shape of soot when a graphite anode with an iron or cobalt-based metal catalyst is combined with a graphite cathode.

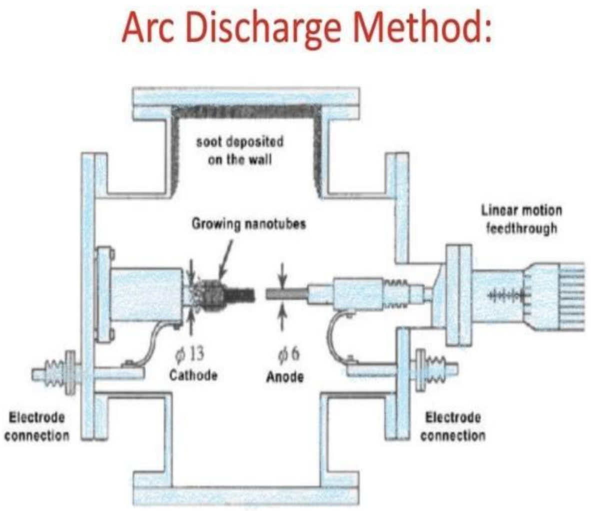


Figure 3. Arc discharge method

SWCNTs were produced using different catalysts namely Fe, Co and Ni and their mixtures along with graphite rod. The type of catalyst and combination of inert gas are considered as the utmost factor for the easy purification of SWCNTs. In some cases, thick SWCNTs finds amorphous carbon inside their tubes which are not completely formed. This may led a foundation to a formation mechanism of two wall carbon nanotube. In order to reduce the amorphous carbon created inside the tube, hydrogen gas and Fe catalyst are used and this arc method is further known as 'FH-arc' method. Inert gas was added to the hydrogen gas for the stabilization of arc method.

A cost-efficient, high-carbon-source rate, high-purity end product, and simple to control process for making chiral CNTs on a big scale is chemical vapour deposition.It has scaled up to huge areas and are used to create bulk quantities with low-cost continuous processing. The CVD procedure was divided into two stages: catalyst preparation and CNT deposition. The interior surface was oxidised for 30 minutes at 500 degrees Celsius with circulating air, then reduced for another 30 minutes with H2 at the same temperature.As a result, a nano-structured catalyst formed on the tube surface.The gaseous carbon source inside the tube thermally degraded during the deposition.As a result, active free radicals, a variety of hydrocarbon species, and elemental carbon were formed. CNT were deposited on the metal surface by the latter.

Application of Swcnts

As catalysts, polymer additives, electron field emitters for cathode ray lighting components, flat panel displays, gas- discharge tubes in telco networks, electromagnetic wave absorption and shielding, and energy conversion, carbon nanotubes have a wide range of potential applications.They are also used in composite materials as a method of improving mechanical strength. carbon nanotube yarns for ultra strong fabric, thermal management system, advanced drug delivery system could be some of the future possible uses for carbon nanotubes.Because of their characteristics and bandgap displacement, SWCNTs are more acceptable in nanoelectronics than MWCNTs. As a result, the research community's main problem in recent years has been to regulate the CNT creation process and produce SWCNTs with a single structure. Researchers are attempting to alter the chirality of SWCNTS as they are being generate.

Double Walled Carbon Nanotubes (Dwcnts)

Double walled carbon nanotubes are cylinders of two layer of graphene sheet. DWNTs exhibit greater mechanical and thermal stability, as well as intriguing electrical and optical characteristics. A double-walled carbon nanotube (DWNT) is made up of two circumferential carbon nanotubes. DWNTs are the simplest system for exploring the impact of inter-wall interaction on the physical characteristics of carbon nanotubes because of their double-wall structure.DWNTs have an unique mechanical and thermal characteristics that are preferable to other carbon nanostructures, including SWNTs, due to their double wall construction. A DWNT can be configured in one of four ways, with each wall either being semiconductor or metallic. Theoretically, DWNTs can be divided into four types depending on their electronic type (metallic or semiconducting) and the (n(inner), m(outer)) values of their inner and outer walls, namely, metallic-metallic, metallic-semiconducting, semiconducting-metallic, and semiconducting-semiconducting. DWNTs may behave like metals, according to some experiments, despite the fact that both walls are semiconducting.

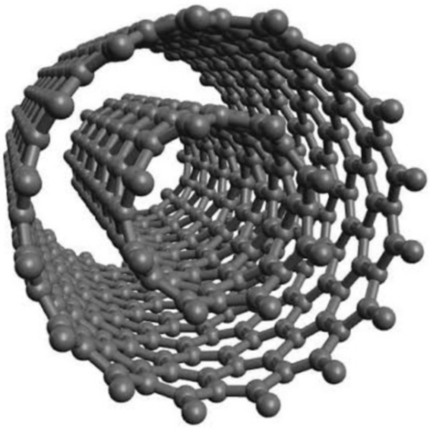


Figure 4. double walled carbon nanotube

Synthesis – CVD

The chemical vapour deposition (CVD) method was used to catalytically create the DWCNTs using an iron-based catalyst. The reactor received regular methane supplies for 10 minutes at 875°C. The best reaction occurs when using methane as the carbon feedstock and iron as the tubular catalyst. The temperature required to produce highly pure DWCNTs was 875°C. To create DWCNTs of good quality, a purifying process was used during the synthetic process. An oxidation procedure (500°C, 20 min) was used first to reduce the amount of chemically active SWCNTs. Following the removal of carbonaceous impurities by air oxidation at 500°C for 10 minutes, magnesium oxide and iron catalysts were removed using hydrochloric solution (18%, 100°C, 10 h). A thorough high resolution transmission electron microscope (HR-TEM) study supported the high yield of DWCNTs (above 95 percent) in bundles with relatively homogeneous and small inner tubes of primarily 0.9 nm diameter and outer diameters of

1.5 nm (see diameter distribution of DWCNTs). Magnetic susceptibility tests confirmed the exceptional DWCNT sample purity through their diamagnetic activity.

Double-walled carbon nanotubes (DWNTs) are produced using the arc-discharge method in a mixture of Ar and H2. In an environment of inert gas, Ni, Co, Fe, and S powders

are heated for one hour at 500 degrees Celsius. The most widely available DWNTs bundles have interior tube diameters between 1.1 and 4.2 nm and outside diameters between 1 and 2 nm. Li et al. used composite filaments made of graphite powders or MWNTs/carbon nanofibers (CNFs) as the carbon feedstock and a co-catalyst made of Fe/Co/Ni and Sulphur as a growth promoter to synthesise DWNTs on a large scale. They found that the MWNTs/CNFs-derived DWNT was purer than the DWNT made from graphite powders. The ends of the solitary DWNTs were not capped. High-quality DWNTs are produced using the high-temperature pulsed arc-discharge method with Y/Ni metal catalysts at 1250 °C. The ideal conditions for DWNT synthesis are almost similar to those for SWNTs, indicating that the two types of nanomaterials' growth mechanisms are probably connected.

Application

There are numerous potential applications for carbon nanotubes with two walls in numerous sectors. Among them are the areas of medicine, energy, electric-electronics, chemistry, and others. Just a few of the uses include biosensors, drug transport, catalysis, hydrogen storage, lithium batteries, nanoprobes, solar cells, photoluminescence, and templates. As sensitive materials for detecting gases like H2, NH3, NO2, and O2 as well as dielectrics and technically difficult uses like field-emission displays and photovoltaics, DWNTs can be used in gas sensors.

DWCNTs are superior to single-walled carbon nanotubes in that the outer nanotube can be altered without changing the properties of the interior nanotube. Double-walled systems are attractive as additives in composite materials because they can be doped at high concentrations without affecting the overall properties of the nanotube. The biggest barriers to further research and marketing of DWCNTs are synthesis and purification. The quantities produced by different synthesis techniques for arc discharge can be anywhere between 50% and 90%. Similarly, catalytic CVD outputs could be between

70 and 85 percent. The leftover nanotubes produced using these methods are a mix of single- and multi-walled nanotubes that need to be filtered to produce individual double-walled nanotubes. Purification is a much more difficult procedure. Techniques such as high-temperature oxidation and ultra- centrifugation are labor- intensive procedures, making commercialization and large-scale manufacture of high-purity DWCNTs challenging.

Multi Walled Carbon Nanotube

MWCNTs are a subtype of carbon nanotube made up of multiple single-walled carbon nanotubes nestled inside one another. MWCNTs lack the distinguishing characteristics of single- and double-walled carbon nanotubes, despite still being categorised as a one-dimensional form of carbon.The reason for this is that there is a larger chance of problems happening. The greater dispersibility of MWCNTs, as well as the lower cost of synthesis and purification, compensate for these drawbacks.

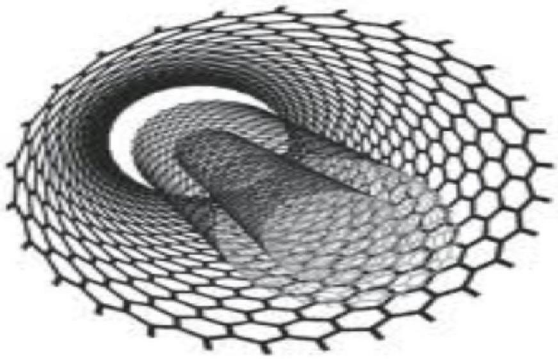


Figure 5. multi walled carbon nanotube

In compared to single-walled and double-walled nanotubes, MWCNTs may be manufactured in large numbers and therefore are easier to purify.This reduces their production costs, which is one of the factors for their widespread use in scientific research.

Synthesis –

Arc Discharge Method –

Two graphite rods with diameters of 7 and 20 mm are utilised as anode and cathode electrodes in the arc- discharge setup. A DC power source capable of providing 100–200 A current voltage range 20–30 V creates an arc between the electrodes. A large fraction of the carbon anode is converted into carbon nanotubes and graphitic nanoparticles, which are then deposited on the cathode by the improved arcing process. Graphite arc evaporation has also been done in a variety of ambient gases like He, Ar and CH4.

In a hydrogen environment, arc-produced MWNTs have less carbon nanoparticles. When both electrodes in an arc discharge are made of graphite, the principal products include MWNTs, as well as side products such as fullerenes, amorphous carbon, and graphite sheets. The anode electrode sublimates and carbon deposits on the cathode electrode in the form of carbon nanotubes and other forms of carbon under the influence of the arc. The carbon soot that has accumulated on the cathode is collected and examined. We generate carbon nanotubes with fewer layers and diameter by adjusting the current and voltage levels for arc generation between graphite rods.

CVD-

The most common and practical technique of synthesis nowadays is catalytic chemical vapour deposition (CVD).CVD synthesis of CNTs is a two-step method that begins with the creation of a catalyst and ends with the synthesis of the nanotube. The catalyst is commonly made by sputtering a suitable transition metal onto a substrate, then dissolving with chemicals like ammonia or thermal annealing to allow catalyst nanoparticles to form. The creation of metal clusters on the substrate from which CNTs grow is aided by thermal annealing. The temperature at which nanotubes are synthesised by CVD is typically between 650 and 900 degrees Celsius. 59–62 The average yield of nanotubes produced by CVD is roughly 40 %.

High yields of MWNTs are produced by burning polypropylene in the presence of a Ni catalyst and an organically modified clay. 63 The support in this technique is silica–alumina, and the combustion is carried out at 600°C. Methane breakdown over Mo/Ni/MgO catalysts produces thin wall MWNTs. Multi-walled carbon nanotubes are readily accessible in a wide variety of purities and lengths. Transistors, solar cells, flat panel displays, batteries, energy storage are some of MWCNT's main applications.

Applications have been centred on its usage as an ingredient in composites which helps in increasing the electrical and mechanical properties of a material. MWCNTs are used in a wide range of biotech and medicinal applications. They're also involved in the manufacturing of RFI shielding materials and wafer processing.

This is due mainly to carbon nanotubes' excellent biocompatibility and capacity to link particular proteins to functional group.

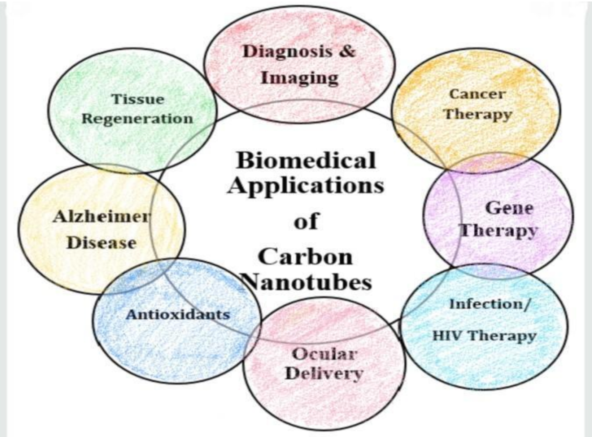


Figure 6. Applications of carbon nanotube

Properties	Single Walled Carbon Nanotube	Double Walled Carbon Nanotube	Multi Walled Carbon Nanotube
1. Based on layers	These are a product of the synthesis of carbon to form a single cylindrical layer of graphene.	These are a product of the synthesis of carbon to form a double cylindrical layer of graphene.	These are a product of the synthesis of carbon to form a multi cylindrical layer of graphene.
2. Arc discharge method	Short tubes with diameters of 0.6–1.4 nm. Large quantities of impure SWCNTs have structural defects	Short tubes with inner diameter of 1–2 nm and outer diameter 1.1-4.2 nm or more.	Short tubes with inner diameter of 1–3 nm and outer diameter ~10 nm or more.Large quantities of impure MWCNTs are generally produced.
3. Chemical vapour deposition	Long tubes bundles with individual diameters of 0.6–1 nm	Long tubes with indiviual diameters of 0.9-1.5 nm	Long tubes with external diameters of 10-240nm
4. Strength	Easy to bend and can be twisted easily.	It can also bend and twist but not as ease like SWCNTs.	Cannot be twisted easily.
5. Bulk synthesis	Bulk synthesis is difficult in SWCNTs	nominal in DWCNTs	easy in MWCNTs

Conclusion

Due to the excellent (and distinctive) characteristics of CNTs and their potential use in a variety of applications, researchers now view carbon-based nanotubes as one of the developing materials that may play significant roles in the future of nanoscale-based applications.We have concentrated on the many CNT kinds made in this review. In this review, we have differentiated popular method of types of CNTs in tabular form. In the past few years, nanotube research has advanced significantly. With the help of the engineering community, possibly nanotube technology will advance in the near future.

References

1. T. Arunkumar, R. Karthikeyan, R. Ram Subramani, K. Viswanathan & M. Anish(2018): Synthesis and Characterisation of Multi Walled Carbon Nanotubes (MWCNT), International Journal of Ambient Energy, DOI: 10.1080/01430750.2018.1472657
2. Yoong Ahm Kim, Kap-Seung Yang, Hiroyuki Muramatsu, Takuya Hayashi, Morinobu Endo, Mauricio Terrones and Mildred S. Dresselhaus (2014):Double-walled carbon nanotubes: synthesis, structural characterization, and application, OI:10.5714/CL.2014.15.2.077
3. P.A. Gowri Sankar, Dr. K. Udhayakumar (2011) A study on single walled carbon nanotubes
4. 4. Kim YA, Muramatsu H, Hayashi T, Endo M, Terrones M, Dressel-haus MS. Fabrication of high-purity, double- walled carbon nanotube buckypaper. Chem Vap Deposition,12, 327(2006). http://dx.doi.org/10.1002/cvde.200504217.
5. Kalpna Varshney, Carbon Nanotubes: A Review on Synthesis, Properties and Applications, International Journal of Engineering Research and General Science,2014
6. 6. Ossila enabling materials science https://www.ossila.com/en-in/products/multi-walled- carbon-nanotubes
7. Sebastien Nanot, Nicholas A. Thompson, Ji-Hee Kim, Xuan Wang, William D. Rice, Erik H. Hároz, Yogeeswaran Ganesan, CarL.Pint, Junichiro Kono (2013)- springer handbook of nanomaterials, DOI 10.1007/978-3-642-20595-8_4
8. Amr Mohammaden, Mohammed E. Fouda et al CNTFET-Based Ternary Multiply-and-Accumulate Unit, InternationalJournal of Electronics 2022.
9. Vikas Prasad ,Anirban Banerjee,

Debaprasad das Design of Ternary Logic Circuits using CNTFET International Symposium on Devices, Circuits and Systems (ISDCS) 2018.

10. NooshinAzimi, Hamidreza Hoseini, Abbas Shahsavari Designing a Novel Ternary Multiplier using CNTFET International Journal of modern education and computer science 2014:11,45-51.
11. ErfanShahrom, Seied Ali Hosseini A New Low Power Multiplexer Based Ternary Multiplier Using CNTFET International Journal of Electronics and Communications 2018.
12. Sneh Lata Murotiya, Anu Gupta and Ayan Pandit CNTFET based low power design of 4 input Ternary XOR function International Conference on Computer and Communication Technology 2014.
13. P.A.Gowri Sankar , K.Udhayakumar Investigating the effect of Chirality on coaxial carbon nanotube field effect.Transistor International Conference on Computing Electronics and Electrical Technologies 2012.
14. Chetan Vudadha ,SowmyaKatragadda,SaiPhaneendra 2:1 Multiplexer Based Design for Ternary Logic Circuits IEEEasiapaciffic Conference on Postgraduate Research in Microelectronics and Electronics (Prime asia) 2013.
15. Nilofar Charmchi,Mohammad Reza Reshadinezhad A novel high speed two operand multiplier using CNTFETtechnology ,International Journal of advanced Information science and Technology (IJAIST) 2015.
16. MorteazaDadashiGavaber, MehradadPoorhosseini novel architecture for low power CNTFET based compressors, Novel architecture for low power CNTFET based compressors, International Journal of Circuits,Systems and Computers,2019.
17. Sneh Lata Murotiya , Anu Gupta , Design and Analysis of CNTFET Based D Flip-Flop International Journal ofElectronics and Communication Engineering & Technology (IJECET),2013.
18. Farzin Mahboob Sardroudi, Mehdi Habibi, Mohammad Hossein Moaiyeri , CNFET-based design of efficient ternary halfadder and 1-trit multiplier circuits using dynamic logic Microelectronics Journal (Elsevier) 2021.
19. Ramzi A Jaber , Bilal Owaidat, Abdallah Kassem, A Novel Low-Energy CNTFET-Based Ternary Half- Adder Designusing Unary Operators International Conference on Innovation and Intelligence for Informatic Computing and Technologies (3ICT),2020.
20. P.A.Gowri Sankar, A Novel Ternary Half Adder & One Bit Multiplier Circuits based on Emerging sub- 32nm FETTechnology International Journal of Electrical and Electronics 2018.
21. Sujatha Hiremath, Dipalikoppad, Low Power circuits using modified gate diffusion Input (GDI), International Journalof VLSI and signal processing 2019.
22. Vikash Prasad, Anirban Banerjee & Debaprasad Das Design of ternary encoder and decoder using CNTFET, International Journal of Electronics 2021.

DEVELOPMENT OF AN ELECTROPHORESIS SYSTEM FOR DETERMINATION AND MEASUREMENT OF HARDNESS IN WATER SAMPLES

Dr. Sarita B.Dhoble[1], Ms.S. S. Dhanvijay[2] and Dr.J.S.Gawai[3]

[1,2]Asst. Professor, E & C Engg., PBCOE,Nagpur

[3]Asst. Professor, Electronics Engg. KDKCOE, Nagpur

[1]saraj.rinke5@gmail.com, [2]sapanadhanvijay@gmail.com, [3]jyotsna12.gawai@gmail.com

ABSTRACT

The prime intention of this research work has been to study and develop electrophoresis system using sensor to determine the hardness of water. It is needless to emphasize the great importance of water in human life.Hard water is water that has high mineral content, it may also contain salt quantity or acidic materials. The presence of salt content causes the water to become more hard and due to this hardness, water causes the further process to deteriorate. This research presents a electrophoresis model to measure the hardness parameter of sample water before sending it for further process. The tested sample if contains unwanted chemicals may be passed through various laboratory process to make it pure and then being used is not hard and detrimental, thus resulting in essential efficiency in the industrial applications of water.

Keywords- electrophoresis, hardness, salt, contamination, water

1. Introduction

It is very important task to monitor and control the quality of water for chemical industry. Generally calcium is the very first and most common parameter associated with water hardness property. It can pose careful consideration in industrial settings, where water hardness is monitored and maintained to avoid costly breakdowns in boilers, cooling towers, and other equipment. Processed water sometimes contain high amount of salt or acidic components which can further deteriorate the process in water applications. Therefore we need a simple sensor based electronic system that is used to test water, to ensure the quality of water, then water may be processed chemically to obtain adulterated water for processing. The electronics system measures the conductivity of water samples containing several types of impurities and use to determine the purity of water, which we may use at a later stage.

The main objective of this research has been to design and develop an electronics model which can be used to test and monitor the quality of water, by checking hardness parameter which can be embedded into industrial system to test the quality of water.

2. Methodology

Electrophoresis process is the migration process of a charged particle under the influence of an applied electric field. Positively charged particles always migrate towards the cathode electrode, and the negatively charged particles towards the anode electrode. Their rate of migration depends on the presence strength of the field, on the total charge, size and shape of the particles and also on the ionic strength of sample, viscosity and temperature in which the molecules are vibrated. As an analytical calculation, electrophoresis is very simple, rapid and highly sensitive method .

2.1 System Design and Experimentation

The electrophoresis system has been designed using performance detecting sensor, micro-controller circuit, voltage regulator circuit, monitoring display 16*2 LCD and testing panel. The testing panel has set of four test tubes of water sample. The power supply used has a range of 0 to 5V DC. The integrated circuit voltage regulator is designed for a wide range of applications which regulates to deliver up to 1.5 A of output current.

As the electrical conductivity of the water sample changes, the change in voltage levels at the electrode get reflected on the LCD panel in numerical values in the closed range of 0-5 V. This indicative value acts as a qualitative measurement for the test solutions electrical conductivity, thereby allowing analysis and decision making in the qualitative domain.

The overall system has the advantage of being cost effective, robust, versatile and yet tremendously powerful for analysis purpose.

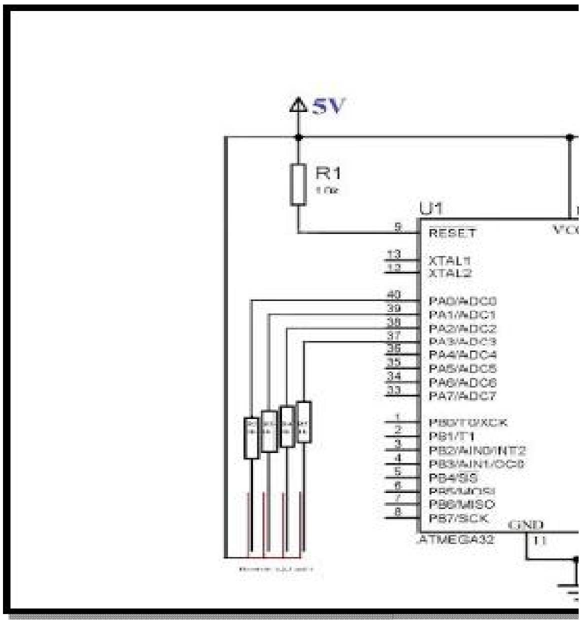


Figure 2.1.: Circuit Schematic of Electrophoresis Model

3. Result & Discussion

This Electrophoresis model is used to check the conductivity of water sample, the corresponding voltage response of water sample is converted in proportionate binary values. These values decide the type of water i.e. acidic water, hard water, regular water, distilled water. The voltage response of the water under test is also recorded.

The higher the voltage value on display panel, better is the quality of water, and lowers the value on screen; poor is the quality of test sample. Experiment was repeated for different types of water samples. Again each sample was stored at various range of temperature for number of days. With respect to type of water and contamination occurs in water, response was recorded. This response used for comparative analysis of sample with respect to other designed electronics systems.

By analyzing the various sample of water, the hardness is tested to maintain the quality of water. The testing sample having higher the value on display record, the better is the quality of water and lowers the quality on screen; poor is the quality of testing water.

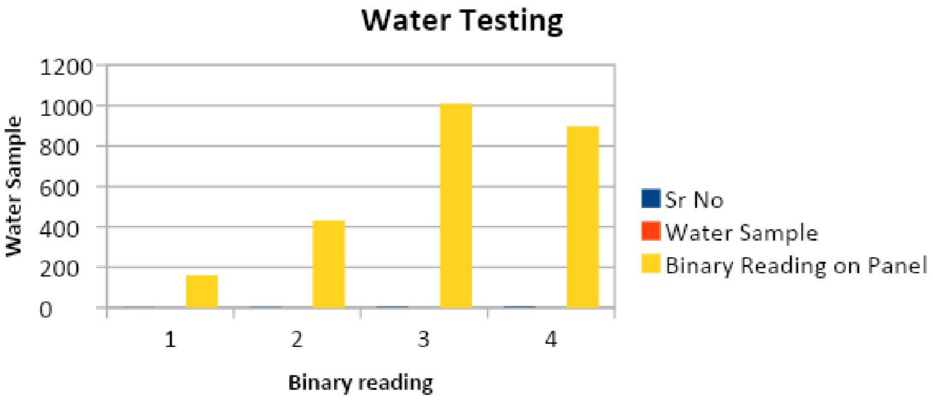


Figure 3.1:Graphical representation of response

Tabel 1:Output Response of Water sample

Sr No	Water Sample	Binary Reading on Panel
1	Acidic Water	161
2	Hard Water	432
3	Distilled Water	1010
4	Regular Water	899

Tabel 2:Output Response for Hardness of Water

Sr.No.	Water Sample	Output Response at Room Tempearature
1	Distilled water with 1%salt	5.0V
2	Distilled water with 5%salt	4.02%
3	Distilled water with 10%salt	3.15%
4	Distilled water with 20%salt	2.25%
5	Distilled water with 30%salt	1.23%

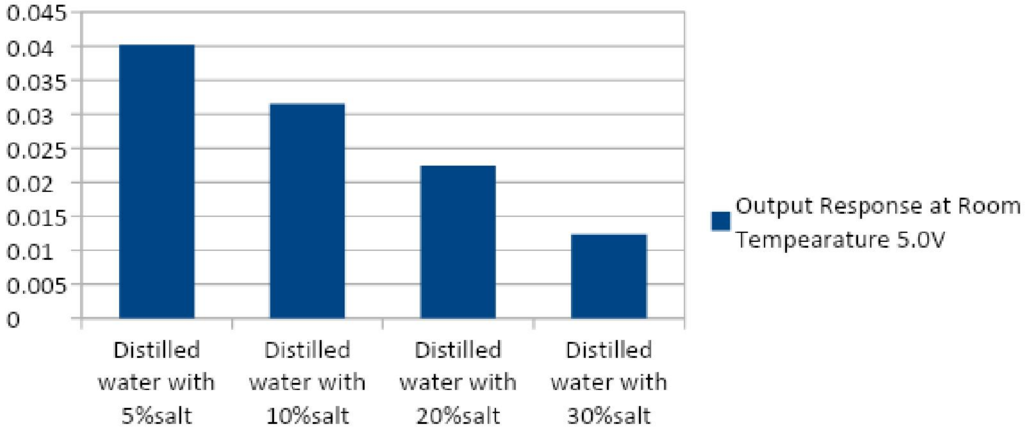


Figure 3.2:Graphical representation of output response with respect to temperature

4. Conclusion

This research work is used to design the system to study the performance parameter of water to check the quality of water.The designed system is used to test the water for various dose responses for hardness testing in a sample, at the various temperatures level. This research work is used to design the system to study the water sample. The degree of hardness becomes greater as the calcium and magnesium content increases and is related to the concentration of salt dissolved in the water.This water quality sensor model is very beneficial for the society in various application of water.

Justification of Research: Water quality management is a major issue of global health goal project and the contamination in water take a major crisis on human health and other industrial water application. So the system is required to test the quality of water. This electronics electrophoresis model is used to analyze the quality of water on the basis of performance parameters.

References

1. Dhoble S B , Dr..Choudhari N K and Dr.(Mrs.) Choudhari A R,"IR Signal Spectrum Analysis of Liquid Sample using Fast Fourier Transform", MAT Journals, Volume 3, Issue 1, Feb 2017, pp.1-5.
2. Dhoble S B , Dr..Choudhari N K and Dr.(Mrs.) Choudhari A R, "Signal Analysis of Sensor System for Infection Detection in Dairy Products",International Journal of Modern Electronics and Communication Engineering (IJMECE) Volume No.-4, Issue No.-5, September, 2016,pp.9-12.
3. Dhoble S B , Dr..Choudhari N K and Dr.(Mrs.) Choudhari A R,"Radio-Frequency pH-Sensing Model to Analyze the Quality of Food Material", International Journal of Advanced Engineering and Global Technology, Vol-2, Issue-5, May 2014,pp 680-684.
4. Dhoble S B , Dr..Choudhari N K," Neuron Model to Analyze the Infection behavior in sample food material", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 11, November – 2013,pp 421-424.
5. Dhoble S B , Dr..Choudhari N K,"Electronics system to study and analyze the performance parameters of sample food material",Photon, Vol. 118, Issue 11, November – 2013,pp 166-169.
6. Dhoble SB, Dr..Choudhari N K,"Electronics system to extract the infection information in food material", IJAMTES, Vol. 02, Issue 02(II), November – 2012,pp 19-21.

X-RAY IMAGE PROCESSING DIFFERENT STRATEGY

Gunjan J. Chimote[1], Priyanka A. Gharad[2] ,Dr. Anup Bhange[3] and Shailesh Kurzalkar[4]

[1]Department of Computer Science and Engg., KDK College of Engineering, Nagpur University, Nagpur

[1]gjchimote@gmail.com, [2]priyankagomase@gmail.com [3]anup.bhange@kdkce.edu.in, [4]shailesh.kurzalkar@kdkce.edu.in

ABSTRACT

The human body suffers from various problems it consists of various parts like legs, hands, bones, bones get cracked or discontinuity most of the day's thanks to pressure applied thereon which can flow from to the accident, sports while playing etc. Osteoporosis is one of the major problems occur thanks to extra use of bones radiologist suggests the patients take x-ray images for diagnosis purpose. This study is a review on medical imaging processing and repository techniques appeared in the literature. Many times, it is difficult and time-consuming to seek out out the situation of fracture within the a patient who is suffering from pain. Today medical imaging technique played many roles in research and diagnosis field. The X-ray imaging technique is used to diagnose and also used to represent anatomically structures such as bones, in human beings. This paper is study of X-ray imaging technique which is used to detect bone fractures than the obtained image is processed by different image processing methods like Computer- Aided Diagnosis, Edge Detection, segmentation which are beneficial for technicians.

Keywords: *X-Ray Imaging, Bones, Image Processing,Image Analysis*

I. Introduction

Bones are the solid organs in the human body that protect many important organs such as the heart, lungs, etc. The human body consists of 206 bones with various shapes, structures, and shapes [6]. Different types of bones are flat, long, short, irregular, and sesamoid. The femur bone is the largest in the body whereas the auditory ossicles are the smallest bone. fracture in bone is a common problem. Fracture is a medical condition when there is a discontinuity in the continuity of the bones. Different types of fractures such as transverse fractures, open fractures, simple fractures, spiral fractures, commuted fractures, etc [5][6]. Long bones may suffer from different types of fractures like greenstick-when one side of the bone breaks while the other gets bent, spiral bone gets twisted, commented - bone gets crushed, transverse. Fractures can be detected by X-ray [7]. Image processing is a powerful tool to modify enhance and detect any particular image details with high accuracy therefore 2d medical imaging research are increasingly dependent on computer-aided diagnosis (cad) where the missing details of visual inspection can be effectively avoided using automated segmentation of medical images and various images algorithm stomake CAD and image processing the most useful tool for the radiologist. It's the potential to draw attention to the finding of the images, highlighting changes from previous images or quantifying the size, shape, and texture of the feature's CAD has its potential to be a useful tool for the radiologist, by drawing [7]. Some CAD systems are used for image registration, virtual interaction, visualization, simulation, or training. Presently CAD is used in the identification of clustered and masses in breast tissue. This system call attention to the possible abnormalities is as good as or better than analyzing the second radiologist [9] They suggest that this type of aid can help reduce the variability in detecting abnormalities.

X-rays are a form of radiant energy, like light or radio waves. In contrast to light, x-rays can penetrate the body, which allows a radiologist to produce pictures of internal structures. Segmentation subdivides an image into its constituent regions or objects. Image segmentation algorithms are primarily based on one of the two basic properties of intensity values, i.e. discontinuity and similarity. In the former class, the approach is to partition an image based on sudden changes in intensity such as edges in an image .XRAY computed tomography imaging plays a critical role in the diagnosis, staging, treatment planning, and therapeutic assessment of cancer. CT is also indispensable in pre-clinical small animal imaging studies providing valuable anatomical information. While CT provides millimeter-resolved anatomical imaging, it lacks the ability to image multiple processes at the molecular level. It is difficult to use CT image to differentiate benign from cancerous nodules.

Furthermore, the article is arranged as follows. The related articles are briefly explained in section 2. Sections 3 various techniques are compared through complexities & accuracy then conclusion & references in the end.

II. Related work

Yuan et.al: This paper deals with the aim of present research in which technology which requires computerized image processing, image analysis, and pattern recognition. This provides the image processing

method for automatic defect detection using image data fusion that provides with several methods which include extraction of the edges of the images, wave profile analysis, image segmentation with the dynamic threshold.

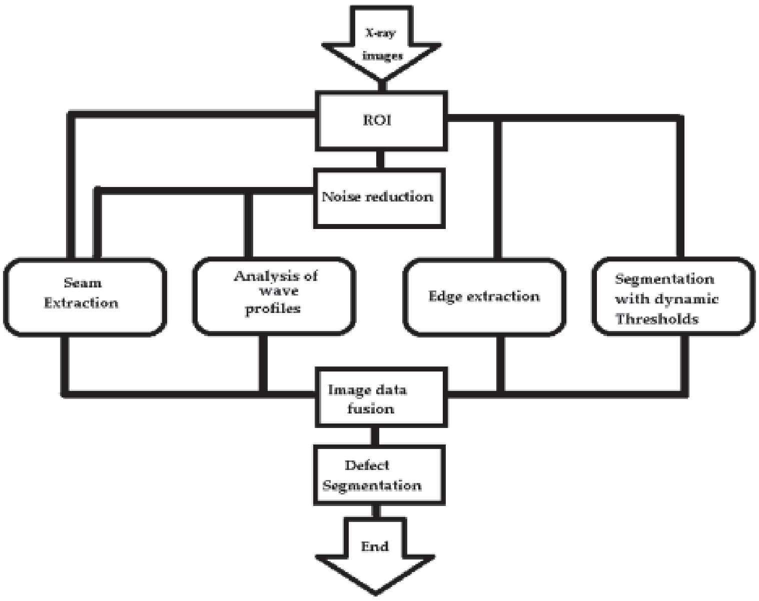


Figure 1: Proposed algorithm

Figure 1 shows the block diagram of the proposed algorithm. This paper describes the defect that induces an abrupt change over a predefined extent of the image intensity can be segmented regardless of the number, location, shape, or size. Therefore, this proposed method is better and practical[12].

Luqman et.al:This paper uses the Ultrasound imaging that is used to make changes in the images which are unclear for fast interpretation. To enhance the ultrasound images of long bone fractures. This contains image contrast enhancement and reduction using these filter techniques such as Wiener, Average and Median Filters. This paper gives a huge improvement obtained from these filter techniques that can be seen through visual inspection and histogram analysis the Wiener Filtering is the best technique among all three in this technique reducing the speckle without eliminating the image edges[13].

Jacob et.al: This paper uses the techniques which are used for detection of bone fracture the been applied to obtained images from different variation like X-ray, CT, MRI and ultrasound

field of medical imaging has been modifying not only in the acquisition of medical images but also in the technique of interpretation. This research is used to interpret and to diagnose ailment from medical images with less aid from experts. This technique uses the methods involved in designing CAD systems for bone fracture detection[14].

Mahmoud et.al:Computer-aided diagnosis is getting popular among medical practitioners and researchers. It provides very accurately, time& efforts saving, and less expensive diagnosis which used in the medical imaging profession. The main advantage of computer-aided diagnos is that it reduces errors.Long bones fracture scan be detected using the X-ray imaging technique. In this paper with the addition to the detection of long bone fractures, the author also determines the fracture type. Author extracted the different characteristics after pre- processing of the image and then the extracted characteristics are used, and the algorithm is designed for the detection of fracture. The final output of this research work is correct and efficient[15].

Anu et.al: This paper deals with the study of Detection of Bone Fracture using Image Processing Methods, used images of the fractured bone was obtained and various processing techniques like segmentation, edge detection etc methods were adopted. Here we detect the bone fracture by using image processing technique such as image

Segmentation method, the edge detection method, etc .are adopted by the author.The images are converted to greyscale images and then the images are filtered to remove the noise for a better quality of the image. The variations in images result is based upon colour, intensity, pixels,etc. Which for image processing for the selection and extraction of image characteristics. These characteristics are used to classify between fractured bone and non-fractured bone. The system proposed is accurate, sensitive and is very specific in terms of performance [16].

Kaur et.al:This paper tells that Fracture occurs in any type of bone in our body like wrist, ankle, hip, rib, leg, chest. Fractures of bones at different body parts such as ribs, legs, ankle, hip etc.

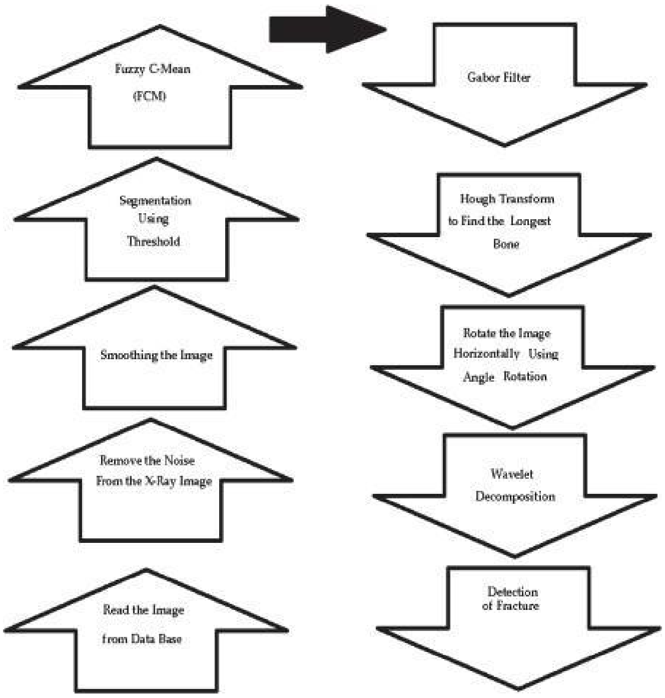


Figure 2. Block diagram of algorithm.

Figure 2 depicts the block diagram of the proposed algorithm. Are detected with the help of x-ray imaging technique by using image segmentation and an algorithm is proposed for the detection of bone fractures. Then the fracture location is selected by the technician manually so that the results are with fewer drawbacks[17].

III Strategy

Image fusion methods can be broadly classified into two groups - spatial domain fusion and transform domain fusion. The fusion methods such as averaging, Brovey method, principal component analysis (PCA) and IHS based methods fall under spatial domain approaches.

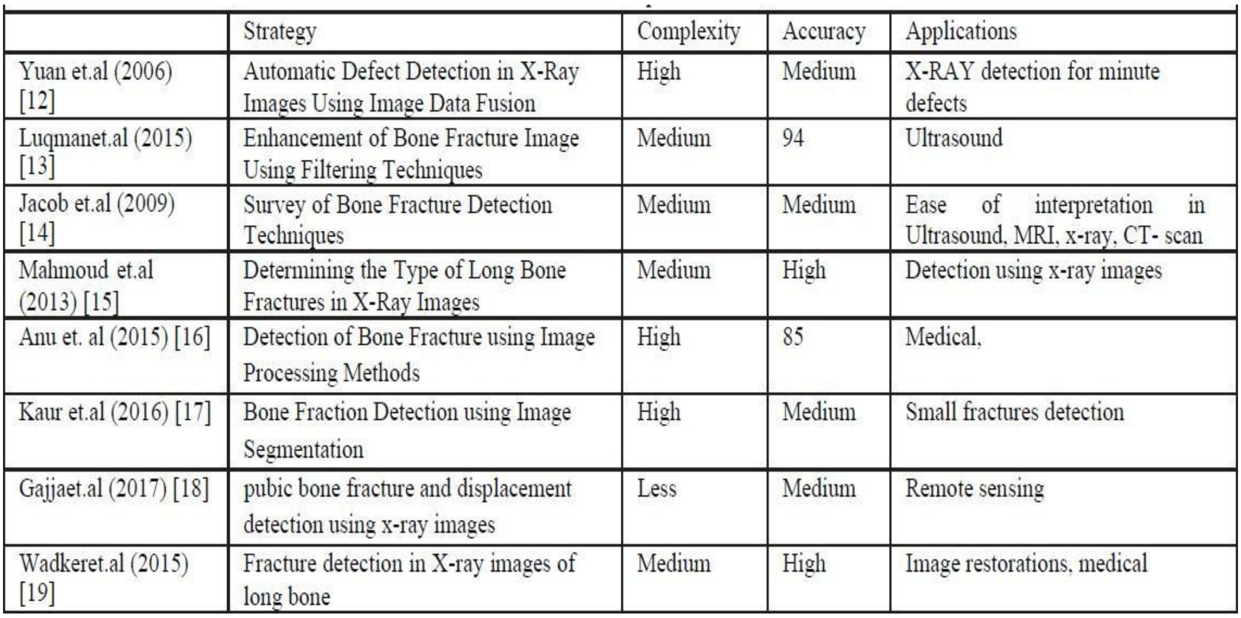
A novel multi-scale fusion framework for low-illumination image enhancement is introduced, which can effectively enhance images taken under various low-light conditions. (2) A new remapping function is employed to generate an artificial multi-exposure image set without the need for additional images.

Newer filtering methods like block-matching and 3D filtering (BM3D), non-linear means (NLM) filtering, and Shearlet transform prove more effective than previous methods used to remove noise. Spatial filtering techniques modify the spatial features of an image. A precise fracture detection approach relies on accurate segmentation of bone areas from the fleshy regions in X-ray image and the quality of fracture detection depends on the sharpness and clarity of the bone contour .

Image segmentation is a method in which a digital image is broken down into various subgroups called Image segments which helps in reducing the complexity of the image to make further processing or analysis of the image simpler. Segmentation in easy words is assigning labels to pixels. Segmentation aims to divide an image into regions that can be more representative and easier to analyze. Color image segmentation that is based on the color feature of image pixels assumes that homogeneous colors in the image correspond to separate clusters and hence meaningful objects in the image. Segmenting allows you to more precisely reach a customer or prospect based on their specific needs and wants. Segmentation will allow you to: Better identify your most valuable customer segments. Improve your return on marketing investment by only targeting those likely to be your best customers. The five basic forms of segmentation are demographic (population statistics), geographic (location), psychographic (personality or lifestyle), benefit (product features), and volume (amount purchased). Business markets may segment based on geography, volume, and benefits. Typically the effect is that the image is split up into segments, also called regions or areas. In medical imaging it is essential for quantification of outlined structures and for 3D visualization of relevant image data

IV Comparison

Table 1 details the brief comparison of the X-ray techniques that are employed X-ray image processing systems. The complexity of the design system is judged based on no of stages involved.



	Strategy	Complexity	Accuracy	Applications
Yuan et.al (2006) [12]	Automatic Defect Detection in X-Ray Images Using Image Data Fusion	High	Medium	X-RAY detection for minute defects
Luqmanet.al (2015) [13]	Enhancement of Bone Fracture Image Using Filtering Techniques	Medium	94	Ultrasound
Jacob et.al (2009) [14]	Survey of Bone Fracture Detection Techniques	Medium	Medium	Ease of interpretation in Ultrasound, MRI, x-ray, CT- scan
Mahmoud et.al (2013) [15]	Determining the Type of Long Bone Fractures in X-Ray Images	Medium	High	Detection using x-ray images
Anu et. al (2015) [16]	Detection of Bone Fracture using Image Processing Methods	High	85	Medical,
Kaur et.al (2016) [17]	Bone Fraction Detection using Image Segmentation	High	Medium	Small fractures detection
Gajjaet.al (2017) [18]	pubic bone fracture and displacement detection using x-ray images	Less	Medium	Remote sensing
Wadkeret.al (2015) [19]	Fracture detection in X-ray images of long bone	Medium	High	Image restorations, medical

Table 1.Comparision

Conclusion

x-ray imaging technique has many applications like detection of fracture, metal, etc. Extensive and effectivere search has been already done and also there a lot of space for further study in this field of the medical industry.Many imaging techniques have been studied in this article such as Computed Aided Diagnosis, Image segmentation, Edge Detection, etc. Such parameters ultimately define the applicability of the techniques in image processing.The main objective behind this study is to give more accurate, effective and less time-consuming technique for recognizing bone fractures in the body .Further enhancing this study, we give more ease to the practitioners and make the technique more efficient and productive.

References

1. Y.Kuang,G. Pratx, M. Bazalova, B. Meng, J. Qian,L.Xing, "First Demonstration of Multiplexed X-Ray Fluorescence Computed Tomography(XFCT)Imaging", Medical Imaging IEEETransactionson,vol.32,no.2,pp.262-267,2013.
2. M. Ahmad, G. Pratx, M. Bazalova and L.Xing, "X-Ray Luminescence and X-Ray Fluorescence Computed Tomography: New Molecular Imaging Modalities," in IEEE Access, vol. 2, pp. 1051-1061, 2014. doi: 10.1109/ACCESS.2014.2353041
3. P. J. LaRiviere and P. A.Vargas,"Monotonic penalized- likelihood image reconstruction for X-ray fluorescence computed tomography," in IEEE Transactions on Medical Imaging, vol. 25, no. 9, pp. 1117-1129,Sept.2006. doi:10.1109/TMI.2006.877441
4. L.Wang, H. Cheng, H. Lan, Y. Zheng, K. Li, "Automatic recognition of pertrochanteric bone fractures in femur using level sets", Engineering in Medicine and Biology Society (EMBC)2016IEEE38thAnnualInternational Conferenceof the, pp. 3851-3854,2016.
5. Y. Song, D. Brie, E. Djermoune, S. Henrot, "Regularization Parameter Estimation for Non-Negative Hyperspectral Image Deconvolution",Image Processing IEEE Transactionson, vol. 25, no. 11, pp. 5316-5330,2016.
6. R. Ebsim, J. Naqvi,T.Cootes, Clinical Image-Based Procedures. Translational Research in Medical Imaging, vol. 9958, pp. 1,2016.
7. Nahid, T. M. Khan, Y.Kong,"Hardware Implementation of Bone Fracture Detector Using Fuzzy Method Along with Local Normalization Technique", Annals of Data Science, 2017.
8. Anju, A.Khatak, "Analysis of the Various Eyes Images using Colour Segmentation techniques and their Noise effects," Journal of Image Processing & Pattern Recognition Progress, Volume 4, Issue 1,2017.
9. Ajay, A. Khatak,A.Gupta,"Gesture Recognition Techniques: A comparison on the Accuracy & Complexities," IEEE International Conference on Intelligent Computing and Sustainable System. ICICSS2018.
10. Yadav, A. Khatak, S. Sindhu, "A Comparative Analysis of Different Image Restoration techniques," IEEE International Conference on Intelligent Computing and Sustainable Sys- tem.ICICSS.2018.
11. T.Syeda-Mahmood,"Role of Big Data and Machine Learning in Diagnostic Decision Support in Radiology", Journal of theAmericanCollegeofRadiology,vol.15,pp. 569,2018.
12. Y.Tian,D.Du,G.Cai,W.Li,andH.Zhang, "Automatic Defect Detectionin X-RayImagesUsingImageDataFusion,"TsinghuaSci.Technol.,vol.11,no.6,pp.720–724,2006.
13. M.L.B. M. Zain,I. Elamvazuthi, and M. Begam,"Enhancement of Bone Fracture Image Using Filtering Techniques," Int. J. Video Image Process. Netw. Secur. IJVIPNS, vol. 9, no. 10, pp. 49–54,2010.
14. N. E. Jacob, "Survey of Bone Fracture Detection Techniques," Int. J. Comput. Appl., vol. 71, no. 17, pp. 31–34, 2013
15. M.Al-Ayyoub and D. Al-Zghool, "Determining the type of long bone fractures in x-Ray images,"WSEAS Trans. Inf. Sci. Appl., vol. 10, no. 8, pp. 261–270,2013.
16. T. CandR. Raman, "Detection of Bone Fracture using Image Processing Methods," Int. J. Comput. Appl., no. Ncpsia,pp.975–8887,2015.
17. T.Kaur andA.Garg,"Bone
18. Gajjar,S.Patel,andA.Vaghela,"Fracture detection in X-ray images of long bone,"Int. J. Comput. Sci. Eng. Open Access Res. Pap., no. 56, pp. 129–133,2017.
19. N. P. Wadker and P. A. Dessai, "PubicBone Fracture and Displacement Detection Using X-Ray Images," pp. 1580– 1586,2017.

A MODIFIED E-LEACH ROUTING PROTOCOL FOR IMPROVING THE LIFE SPAN IN WIRELESS SENSOR NETWORK

Sneha Awathre[1]Nikitha Walthare[2], Tanushree Mumandwar[3], Shrikant Doppala[4] and Dr.J.S.Gawai[5]

[12345]Department of Electronics Engineering, K.D.K College of Engineering
snehaawathre24@gmail.com

ABSTRACT

Micro-sensors and other sensors form a decentralized network known as a wireless sensor network (WSN). It can pick up environmental cues including temperature, wetness, humidity, and more. WSN may be used for a wide variety of purposes, including but not limited to engineering, medicine, environmental monitoring, industrial automation, and military surveillance. In a wireless sensor network, the sensing node, the processing node (the base station), and the power node are the three most important parts (Battery). Data transmission is an integral part of the wireless sensor network's (WSN) communication and data processing with the base station. Since batteries in WSN deplete quickly, maximizing energy efficiency is always a priority. Data transmission uses energy in wireless sensor networks, which limits the lifespan of the network. This means that we have to find a way to lessen our reliance on power plants. Therefore, a routing protocol is required. Over the last several years, more and more work has gone into finding ways to reduce energy usage using algorithms and other strategies at the hardware, network, and application layers. The Low Energy Adaptive Clustering Hierarchy (LEACH) technique is one such example. Here, we propose the LEACH protocol. LEACH is a hierarchical routing technique that minimizes energy consumption. Our main interest is in analysing and improving LEACH's application. MATLAB simulations are run to investigate and assess a number of factors.

Keywords: *LEACH, Wireless Sensor Network, WSN, Cluster Head*

I. Introduction

An increasingly popular method of remote monitoring, the wireless sensor network (WSN) has several potential applications. Since the dawn of the information age, it has been more relevant in all spheres of activity. If you want to collect and send data using a WSN, you'll likely need to set up a large number of nodes in the region you're trying to keep tabs on. The unique conditions of a monitoring setup make it challenging to keep nodes powered by swapping out batteries. Accordingly, the node's lifetime has been used as the primary benchmark for designing data collection strategies in sensor networks [1]. When trying to increase the lifespan of a wireless sensor network (WSN), a suitable routing protocol is essential for dealing with the issue of few node resources. At the moment, we can classify routing protocols primarily into planar and hierarchical types [2]. A hierarchical routing protocol can not only improve these issues, but also reduce network energy consumption and extend network life cycle [3], whereas planar routing protocols are not suitable for large-scale networks due to the need to maintain large routing tables and the limited transmission distance between sensor nodes. This study opts for a hierarchical routing technique known as the LEACH protocol.

The LEACH protocol, developed by Cui et al. [4], is the first clustering routing technology that uses a hierarchical network topology. Each node votes for a new cluster head at the beginning of each "round" in the network, which reorganises the network and reduces the likelihood of the cluster head failing owing to high energy consumption.

Many later researchers did optimization experiments based on the LEACH procedure, proposing approaches such as DEEC [5], CRBED [6], and others. The GA-LEACH routing protocol, described in [7], combines the microgenetic algorithm with the LEACH protocol in order to improve cluster head (CH) selection while decreasing the network's energy consumption. In order to minimise the amount of energy that is wasted during the clustering process, the leach-F method was suggested in [8] to choose cluster heads after each cycle of reconstruction. The EEUC method for nonuniform clustering was proposed in [9]. Distance from the gateway node determines the size of the clusters, which in turn shields the hot nodes and ensures that all nodes use the same amount of energy. In [10], an algorithm was developed using the principles of distributed learning automata. Each node in the network attained self-protection, extending its life cycle, and the network as a whole was able to fulfil its global aim with the help of the selected subset of nodes. In article [11], a method for replacing cluster heads using a modified threshold was described. To more closely align with the assumptions made in the LEACH protocol, a new chance of becoming a cluster leader, for any node in any round, was suggested. To account for avoiding data and postponing the death of the initial node, a new threshold energy

expression is provided. To address the issue of energy cost during cluster head elections, H-LEACH technology was presented in the literature [12]. Channel heads were chosen using a threshold condition that also took into account the maximal energy of nodes and the energy that had been left over after pruning. An improved coverage rate and connectivity between nodes were achieved with the greedy partial coverage (GPC) algorithm proposed in article [13], which made use of neighbour nodes to maintain the connectivity of chosen nodes and made use of the overlap between nodes to achieve the required coverage rate, all while effectively decreasing the network's energy consumption. A novel LEACH protocol based on affinity propagation (AP) was introduced in [14], which allows for completely distributed control and overcomes the practical limits of previous LEACH-based protocols by streamlining network capabilities and decreasing the price of sensor gear. To enhance the energy efficiency of particle swarm optimization, a new particle coding and fitness function scheme was presented in [15], and a new particle swarm optimization-based cluster head selection method, pSO-ECHS, was developed. The focus of [16] was on modern hierarchical routing techniques that used the LEACH protocol to improve their own performance and extend the lifespan of wireless sensor networks. Each cluster's leader is chosen via a node rank algorithm that takes into account both the route cost and the number of connections between nodes. In [17], a learning automaton based PCP method called pDCDs was suggested. Full network coverage was accomplished, and the network's lifetime was greatly increased, all because it located nodes to monitor p-percent coverage in the installed network. Based on the energy of the remaining nodes and the average energy of the network, a better energy-saving (IEE-LEACH) protocol was developed in [18]. To limit the wireless sensor network's power consumption, the nodes closest to the base station are prevented from entering the cluster in order to achieve the ideal number of cluster heads.

Many studies have been conducted by others who came before us in order to address the issues with the LEACH procedure. However, they often only optimise the LEACH procedure from a single viewpoint. However, the literature studies [7] and [13] optimised LEACH protocol using different methods and concentrated on energy research, while disregarding other issues of LEACH protocol (such as data volume). The optimization goal was met in the aforementioned research [8, 10, 14], although this was accomplished at the expense of attention to other features of the LEACH protocol, such as network coverage. The LEACH methodology was improved in the published literature [12] by cutting down on the need for extra hardware in WSNs. Based on

what has been covered thus far, it is clear that previous studies focused on maximising LEACH agreement and extending network life cycle through different algorithms, hence wasting less energy on travelling between nodes or covering longer distances. However, it did not do a thorough optimization of energy, distance, angle, and other contributing elements, and it did not take into account the effect of cluster size on the network life cycle. Therefore, there is just one main focus of the study.

"The Internet" refers to an internetwork, which is a collection of interconnected networks. It's the biggest online community in the world. Global Area Networks (WANs) are all linked together via the internet, while local area networks (LANs) and home networks (HNs) may also connect to the internet. The Internet is addressed using IP, which is part of the TCP/IP protocol family. IPv4 now serves as the backbone for the majority of live Internet connections. IPv6 is replacing IPv4 as a result of a lack of available addresses. As a communications platform, (WSN) has the potential to have an effect on the development of a number of ICT capabilities. WSN has been garnering serious research attention as of late due to its applicability in a number of important human endeavours. To function, WSNs rely on a network of very inexpensive and disposable nodes called sensor hubs. In a WSN, nodes may each do their own climate detection, measurement, and remote transmission to a central unit for processing. Military applications for WSN are gradually giving way to civilian, terrestrial, and even extraterrestrial ones. The development of tiny electromechanical systems (MEMS) and advancements in distant communications fueled the expansion of WSN. Recent years have seen a surge in interest in wireless sensor networks (WSNs), which are made up of a sensor field, a sink, and a number of sensor hubs (located at various distances from one another). The major problems with the WSN are the excessive number of hubs, their weak force rating, and their inability to communicate over long distances. These nodes work together to detect, track, and transmit data, making remote sensors a viable option for monitoring everyday occurrences and environmental shifts, as well as gauging traffic patterns, keeping tabs on intruders, and keeping an eye on military recruitment. The sensor networks used in these applications must be very reliable, thus researchers are now focusing on figuring out how to make heterogeneous wireless sensor networks (WSNs) better.

For the sake of organisational flexibility, specialists have traditionally clustered sensor nodes into groups along a given axis, with each cluster having a cluster head (CH) chosen by its members or appointed by the cluster's designer. You may also use a more expensive sensor as the CH if you like. The biggest benefit of bunching is the improved association technique that is implemented, which not only increases the life of the sensor batteries but also enhances the activity life of the organisation as a whole.

Huge, power-hungry sensor nodes (SNs) are the norm in wireless sensor networks (WSNs). For monitoring and detecting purposes, WSNs are distributed at random over a given area to collect data on a wide range of environmental characteristics and relay that data to a central base station (BS).

We propose a new improved energy-efficient LEACH (IEE-LEACH) routing protocol to address the shortcomings of existing approaches and significantly extend the WSNs' lifespan. Initial node energy, residual node energy, total network energy, and average network energy are the four parameters introduced by the threshold setting in the proposed protocol. According to the proposed IEE-LEACH protocol, a node that is closer to the BS than the CH is excluded from the cluster formation. As a result, the technique may equalise the energy load and cut down on consumption. In addition, the IEE-LEACH protocol provides a comparison of the energy requirements of single-hop and multi-hop communication modalities during the data transmission phase. The most efficient means of communication will be used. As a result, the suggested method reduces total communication costs and considerably lengthens the lifespan of the network.

II. Literature Review

Rama Shankar Yadav et al 2020 Many applications in smart cities depend on sensing technologies for event detection and monitoring, and Wireless Sensor Networks (WSNs) have changed how this data is gathered, processed, and utilised. Despite the many advantages of this technology, a key problem is the rapid drain on sensor batteries caused by the intensive computing work and communication operations conducted by each sensor. The price of new batteries may quickly become unaffordable, particularly if sensors are placed in inconvenient locations, such as those seen in densely populated cities. This study presents a novel version of the LEACH protocol, called LEACH improved with probabilistic cluster head selection, to increase the sensors' lifespan (LEACH-PRO). For example, LEACH-PRO adds a probabilistic function based on maximum residual energy and lowest distance to the sink for selecting cluster head nodes, which helps to increase the lifespan of nodes in WSNs. Results from simulations show that LEACH-PRO outperforms LEACH and the direct transmission protocol in terms of network lifespan and traffic overhead. LEACH-primary PRO's contribution is an increase in sensor lifespan that might make widespread use of such systems in smart city contexts a reality.

G. Vishnupriya et al 2022 Many applications in smart cities depend on sensing technologies for event detection and monitoring. Wireless Sensor Networks (WSNs) are a prominent sensing technology that has transformed the way information is gathered, processed, and utilised. Despite the many advantages of this technology, one key drawback is the rapid drain of sensor batteries caused by their intensive processing activities and communication operations. As a matter of fact, changing batteries may be quite costly, particularly if sensors are placed in inaccessible locations, such as in densely populated cities. This study presents a novel version of the LEACH protocol, called LEACH improved with probabilistic cluster head selection, to increase the sensors' lifespan (LEACH-PRO). By introducing a probabilistic function based on maximum residual energy and lowest distance to the sink, LEACH-PRO proposes many approaches to increase the lifespan of nodes in WSNs. In terms of network lifespan and traffic overhead, LEACH-PRO has been shown to be superior than LEACH and the direct transmission protocol via simulation. LEACH-primary PRO's contribution is a large increase in sensor lifespan, which improves the practicality of such deployment in smart city contexts.

Jiazu Xie et al 2022 First, a mathematical model of these issues is built in this research. We suppose that HWSN has dead zones where no sensor nodes can be deployed, which complicates the deployment of relay nodes. This is converted to a measure of the length of the route used in wireless communication so that energy may be conserved during routing. Since this is an NP-hard issue, a heuristic known as the whale optimizer is used to help solve it. Three different adaptive methods are used to examine the results of the whale optimizer approach. The suggested approach for HWSN is tested by numerical simulations. Discussion and analysis of the results demonstrate the effectiveness of the suggested approach in solving the NP-hard node placement and energy-saving challenges in HWSN.

Seham Nasr er al 2019 One of the most popular methods, wireless sensor networks (WSN) are used in several fields and industries, from agriculture and manufacturing to healthcare and fire detection. The various benefits of WSN include its inexpensive price, compact size, multifunctionality, autonomous operation, and routable nature through WSN protocols. WSN, however, has a few drawbacks that prevent it from being used in some applications. These include a lack of power, a limited lifespan, a large deployment area, and high energy consumption from the sensors themselves.

In this research, we suggest a novel method for increasing the reliability and longevity of WSNs via the optimization of packet delivery times. Then, we evaluate the suggested method by comparing its simulated performance to that of the standard, fixed-parameter LEACH approach. In terms of network lifetime, the suggested technique is 128.80 percent more efficient than standard LEACH.

III. Energy Analysis of Routing Protocol

In the context of wireless sensor networks, a number of routing methods for wireless networks have been developed. With the help of our sensor network and radio models, we analyse two such protocols: direct communication with the base station and minimum-energy multi-hop routing. Further, we talk about a when all of the nodes are energy-constrained, the flaws in the usual clustering technique to routing become apparent.

IV. Improvements to the LEACH Protocol

The LEACH routing protocol features an effective self-organizing election mechanism. It can send data to GN more quickly and effectively than the standard routing protocol. Its election method, however, is not without flaws. As a result, the node's residual energy is ignored, and the random number it generates with T (n) is much too arbitrary to be a viable candidate for the cluster leader. When sending data, the cluster head that is farther from the GN uses more energy than the node that is closer to the GN, and therefore is more likely to run out of juice throughout the lengthy transmission process, which has an impact on the network's lifetime. The cluster head is chosen at random during transmission. In order to reach the cluster master, the public nodes only need to make one connection. Energy transmission costs will rise if the cluster head is off-center. In addition, the LEACH methodology may be tweaked on the fly, and there is no hard and fast limit on how many cluster leaders will participate in any given iteration. When there are too many cluster leaders, multihop traffic rises because more steps must be taken to reach the GN from each cluster leader. If there aren't enough nodes, the cluster's leader will be underutilised and eventually perish from the extra strain on its limited power supply. This process will generate both maximum clusters (with an excessive number of nodes) and minimum clusters (with an inadequate number of nodes) (too few nodes in the cluster or even only one). Many redundant nodes will be produced by large clusters, leading to wasted energy utilisation. If you have too few nodes in your cluster, the first one will crash and burn under the strain. As a result, the issue of excessively large or very small clusters may be addressed by regulating cluster sizes.

The function of a WSN is often the defining characteristic of its existence. The first node death assessment technique is one of the three currently accepted ways of evaluation [22]. If we can,

we should put off the introduction of the first node in a WSN since its failure will have a domino effect on the network's overall efficiency. Second, we must consider the possibility of losing half of the nodes. Using this evaluative strategy in a highly node-density region. If a single node or a small number of nodes were to die, the network's performance wouldn't be affected, and the average time of death would still be known. Third, we must consider the passage of time while assessing the demise of each and every node. This study employs all three types of analysis at once.

In this study, we distinguish between three distinct kinds of nodes: cluster heads, regular nodes, and centralised nodes. Nodes in the cluster provide data to the cluster head node, which then combines the data. The data packet is then sent to GN through the various cluster heads. Information in the surrounding area is gathered by shared nodes and sent to the cluster's central processor. When describing a cluster, the node closest to the cluster's centre of gravity is referred to as the "centre of gravity node" (selected during each round calculation). The node in the cluster's geographic centre acts as both a standard node and an additional cluster head, but does not vote in the election of cluster leaders.

V. Methodology

The proposed work provides the relevant prior art in relation to our strategy. There are several cluster based routing protocol implementations suggested for WSNs. You may classify them as either Static Nodes or Mobile Nodes, depending on their location. When it comes to WSNs, LEACH is the clustering procedure of choice. As part of LEACH, nodes self-organize into small groups. The starting energy level of each node is the same in homogenous networks. The procedure is broken up into rounds. If a random number generated by CH between 0 and 1 is smaller than the threshold value, then CH is selected from the arranged clusters.

During the steady-state phase, the CH at each node collects the data and transmits it to the BS. However, the cluster formation that is launched in each cycle wastes energy and hinders movement. The LEACH-Mobile protocol enhances the original LEACH protocol with a feature called membership declaration, which allows for mobile sensor nodes to be used in WSN.

In a packet-loss comparison between LEACH and LEACH Mobile, LEACH Mobile comes out on top. In any case, a statement of membership is required. The proposed LEACH-Mobile Enhanced (LEACH-ME) modifies the LEACH-Mobile cluster head election algorithm such that

the sensor node with the lowest mobility factor is chosen as the cluster leader. The CBR-Mobile protocol helps mobile sensor nodes by redistributing time slots dynamically in response to changes in network load.

In order for CBR-Mobile to be flexible enough to adapt to the varying mobility and traffic patterns of sensor nodes, it creates two owners for each node at all times: the original owner and the backup owner. Compared to LEACH Mobile, it dramatically improves the packet delivery ratio. Using this method, the mobility of the sensor node may be calculated without using up any additional time period. In order to expedite the transmission of data to BS. Cluster-based Energy- efficient Scheme (CES) is a cluster-head election method for Mobile Wireless Sensor Networks (MWSNs) that takes into account k density, residual energy, and mobility characteristics. After each cycle under the CES plan, a new cluster leader is elected. In addition, CES allows for the generation of well-balanced 2-hopclusters with sizes between two thresholds, or bounds..

VII. Block diagram

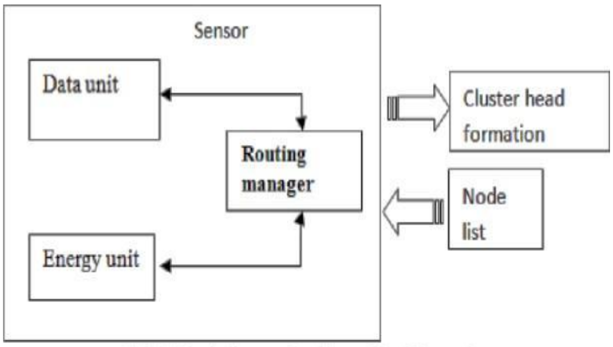


Fig 1 Block diagram FOR Clustering system

With WSNs, it's impossible to recharge sensor nodes' batteries. Accordingly, WSNs place a premium on the longevity of their networks. There are a number of different routing protocols that may be used to extend the life of a network, and these methods can be divided into two categories: flat routing techniques and hierarchical routing strategies. Large-scale WSNs cannot use flat routing protocols because they cannot aggregate the sensed data and need constant maintenance of routing table data.

But hierarchical routing schemes may alleviate the problem to some degree. When sending data from a source node to a destination node, the simplest hierarchical routing system is called Direct Transmission (DT).

This means that when the BS is further away from the sensing field, DT uses more energy to relay data to it.This will drastically shorten the lifespan of the network and the battery life of individual nodes.

Conclusions

The main objective of this study is to create a set of guidelines that can provide superior and reliable remote sensor organisation services using a stable system with hubs.

an extended lifetime. In the past, method The cluster heads determine which nodes in the cluster have lower energies in each round, and those nodes must be put into sleep mode once they have been identified. Therefore, they won't use up a lot of energy and can work for a long time. Every time the round changes in this situation, the same procedure is repeated, causing a large number of messages to be sent and increasing energy usage. This work may be expanded in the future utilising a round-robin schedule, where the cluster heads for each round are chosen initially, or during the first phase. The protocol's primary goal should be to reduce energy consumption within the WSN and lengthen the life of the network. Additionally, it is anticipated that the WSN's throughput will rise as a result of a decline in network energy usage. As a result, the network is more stable and has a longer lifespan.

References

1. Z. Aliouat an M. Aliouat. “Improving wireless sensor networks robustness through multi- level fault tolerant routing protocol”, In the proceeding of the fourth International Conference on Modeling Approaches and Algorithms for Advanced Computer Applications (CIIA’2013), pp.115-124, Saida, Algeria, 2013.
2. El korbi et al. “Coverage-Connectivity based faulttolerance procedure in wireless sensor networks”. In the Proceeding of the9th International Conference on Wireless Communications and Mobile Computing Conference (IWCMC’2013), pp.1540-1545, Sardinia, Italy, 2013.
3. M. Lehsaini and H. Guyyenet. “Improvement of LEACH for fault-tolerance in sensor networks. In the proceeding of the fourth International Conference on Modeling Approaches and Algorithms for Advanced Computer Applications (CIIA’2013), pp.175-183,

Saida, Algeria, 2013.

4. V.Katiyar et al.. "Improvement in LEACH protocol for large-scale wireless sensor networks", International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT),pp.1070-1075, Tamil Nadu, 2011.
5. W. Heinzelman, A. Chandrakasan and H. Balakrishnan."Energy-efficient communication protocols for wireless microsensor networks", Proceedings of the 33rd Hawaii International Conference onSystems Sciences, pp.1-10, Hawaii, 2000.
6. Razieh Sheikhpour, Sam Jabbehdari and Ahmad Khadem-Zadeh"Comparison of Energy Efficient Clustering Protocols inHeterogeneous Wireless Sensor Network,zs," International Journal of AdvancedScience and Technology Vol. 36, November, 2011.
7. Rabia Noor Enam , Mumtazul Imam and Rehan Inam Qureshi "Energy Consumption in Random Cluster Head selection Phase of WSN," 2012 IACSIT Hong Kong Conferences IPCSIT vol. 30 (2012) © (2012)IACSIT Press, Singapore.
8. Wendi,B.Heinzelman, Anantha P.Chandrakasan andHari Balakrishnan"An Application specific protocol architecture for wireless Micro-sensornetworks,"IEEE Transactions on wireless communications vol.1 NO.4 2002.
9. Do-Seong Kim and Yeong-ee Chung, "Self - Organization RoutingProtocol Supporting Mobile Nodes for Wireless Sensor Network Proceedings of the First International Multi Symposiums on Computerand Computational Sciences (IMSCCS'06), 2006.
10. G. S. Kumar, M. V. Vinu Paul, G.Athithan and K. P. Jacod, "Routing Protocol enhancement for handling node mobility in wireless sensor network", TENCON 2008 – 2008 IEEE Region 10 Conf, 2008,pp. 1-6.
11. S. A. B. Awwad, C.K. Ng, N. K. Noordin and M. F. A. Raisd, "Cluster Based routing protocol for mobile node in wireless sensor network,"in collaborative technologies and system, 2009. CTS '09. International Symposium on, 2009, pp. 233-241.
12. Lutful Karim and Nidal Nasser "Energy efficient and Fault TolerantRoutingprotocol for mobile Sensor Network,"IEEEICC2011processdings.
13. Lehsaini M., Guyennet H. and Feham, M. "Wireless Sensor and ActorNetworks II," 2008, in IFIP International Federation for InformationProcessing, Volume 264; (Boston: Springer),
14. Hla Yin Min, and Win Zaw "Energy Efficient, Fault Tolerant Routing LEACH (EF- LEACH) Protocol for Wireless Sensor Networks" International Conference on Advances in Engineering and Technology (ICAET'2014) March 29-30, 2014 Singapore