Enhanced Internet of Things Security Integration Framework with an Emphasis on Virtual Health Monitoring

Dr.C.S.Anita[1], Mr. Dhruva Sreenivasa Chakravarthi[2], Dr.Aruna.M[3], Mrs. K.Balasaranya[4], Dillip Narayan Sahu 5*, Mrs.V.S.Kotwal[6]

[1]Professor, Department of Artificial Intelligence & Machine Learning, R.M.D.Engineering College, R.S.M.Nagar, Thiruvalluvar, TamilNadu, India.
[2]Research Scholar, KL Business School, Koneru Lakshmaiah Education Foundation Deemed to be University, Vaddeswaram Guntur District (A.P). India.
[3]Associate Professor, Department of Electrical and Electronics Engineering, Nitte Meenakshi Institute of Technology, Bangalore, Karnataka, India.
[4]Assistant Professor, Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, TamilNadu, India
[5*]Assistant Professor, Department of MCA, Gangadhar Meher University, Odisha, India.
[6]Lecturer, Department of Computer Engineering, Dr.D.Y.Patil Polytechnic, Kolhapur, Maharashtra, India.

*Email: dillip1seminar@gmail.com

Abstract

Humans spend a lot of money on healthcare services. The healthcare business is growing more sophisticated and technologically advanced. It also required patients to expend time, effort, and money to get care. When a patient is in a distant location (particularly for the elderly), it takes time to go to the healthcare facility, make an appointment, and wait for his/her turn to meet with the doctor. Many individuals have perished as a result of heart attacks. If there is technology that can be utilised to remotely monitor a patient's vital signs, it might save lives and offer better treatment. Such QoS is attainable with remote health monitoring using technologies such as cloud computing, sensors, and IoT. When remote health monitoring using IoT technology is realised, particularly for rural people, it will revolutionise the way healthcare services are delivered and ordinary people will survive from a variety of life-threatening illnesses. This paper investigates current IoT-based remote health monitoring systems, as well as their benefits and limits. It also contains a suggestion for a revolutionary remote patient monitoring system that merges PHC in a community with smart beds linked to IoT technology for real-time patient health monitoring. The scope also includes security upgrades to the planned remote health monitoring system, such as support for secure end-to-end connections and the preservation of healthcare data privacy.

Keywords: Health care, Remote Patient Monitoring, IoT, PHC, Security and Diseases.

1. INTRODUCTION

The old adage that "health is wealth" is truer now than it ever been before. Despite being able to launch rockets to other planets, human beings continue to face health problems on Earth. The healthcare business has become highly advanced and technologically rich, with the ability to treat a wide range of illnesses. However, it has become expensive, and people all around the world are spending a great deal of money on health care. It might seem that the average person cannot afford to get medical treatment[1]. Healthcare services for the poor and underserved should, therefore, make use of technological advances. City dwellers may visit medical clinics and hospitals if they have the financial means to do so or are covered by medical insurance[2]. What about folks in rural areas who don't have access to cities' affordable healthcare options? This is the key issue that must be addressed by technology-based setups. If technology doesn't benefit the underprivileged, it's not really useful. This line of thinking has prompted scientists and academics to look at cutting-edge developments in the computer sector. As a whole, this concept is on assisting those who reside in rural areas. Because of this concept, work has begun to implement remote health monitoring. Many years ago, the whole idea was inconceivable. But with distributed computing technologies like cloud computing and the Internet of Things (IoT), remote health monitoring systems are more likely to become a reality[3]. The Internet of Things can bridge the gap between the digital and real worlds. A human person is an example of the physical realm, whereas a mobile device is an example of the digital realm. In both cases, the Internet of Things makes the integration effortless. The Internet of Things (IoT) makes this possible via the use of technologies like Radio Frequency Identification (RFID), sensing technologies, and sensors incorporated in wearable devices, telecommunications devices, Internet-linked devices, and other connected gadgets. Cloud computing, on the other hand, has the potential to provide storage and processing capabilities on demand, along with availability, scalability, and fault tolerance. Thus, cloud computing and the Internet of Things are crucial for use in remote health monitoring programmes. Data storage and management frameworks such as Hadoop are now available on the cloud[4]. The current integration of IoT and cloud to healthcare units has little empirical benefit, as is recognised from the literature. A robust framework that may realise remote health monitoring is essential when taking into account individuals who live in villages and have access to local PHC. This thesis proposes a system in which a smart

bed equipped with IoT and cloud technology is linked to a PHC, allowing for remote patient monitoring. The data from a patient's vital signs are sent to the cloud, where they may be analysed and made available to other parties, including the doctor, through a mobile app[5]. The power of IoT technology lies in its ability to bridge the gap between the digital and the real worlds. Many other fields and industries may benefit from it, including agriculture, home automation, city planning, and transportation. Integration of IoT technologies into healthcare facilities, however, might have positive effects on patients. All demographics have an inherent need for medical care[6]. However, the high expense of these advanced medical treatments means they are out of reach for most individuals living in rural areas of nations like India. Since the Internet of Things may connect real-world objects (like people) to virtual ones (like computers), it is theoretically possible to utilise wearable devices with people to collect vital signs and conduct real-time health monitoring. Only the Internet of Things allows for such seamless connection. Cloud computing serves its purpose by offering convenient, on-demand access to data storage and processing power. Remote health monitoring cannot be realised without mobile cloud computing (MCC). In reality, cloud computing allows mobile access to healthcare data collected by distant monitoring systems. Healthcare services that enable remote health monitoring are therefore realised via the use of cloud computing, MCC, and the Internet of Things[7]. Figure.1 depicts some of the various security and privacy concerns associated with IoT applications. Authentication at the level of individual devices is also crucial for the Internet of Things. IoT applications are susceptible to assaults due to issues with authentication, among other security issues. Access control is another factor to consider. Only authorised users or organisations should be able to access protected data and systems[8]. When it comes to sharing and analysing data, privacy is essential in the IoT. All Internet of Things use cases include the transmission of confidential data. This will lead to breaches of privacy. Therefore, protecting privacy is essential for enabling smart IoT use cases.

Figure.1: Security and privacy challenges in IoT use cases

Problems with trust can arise in IoT contexts. Because trust is a nuanced concept, relying on trust-based judgements may be difficult. In particular, access control and identity management are intertwined with trust management. Therefore, techniques for determining a person's or organization's trustworthiness are crucial[9]. Another difficulty is mobile security. Because of their mobility and limited resources, smart phones present security risks when used in Internet of Things (IoT) applications. Different suppliers' implementations of middleware in IoT devices might leave them open to attack. The vulnerabilities in middleware might spread to Internet of Things programmes. As with other security features, confidentiality is often absent from IoT applications owing to the lack of standardised protocols and the absence of inter-disciplinary processes.

2. NEED FOR REMOTE HEALTH MONITORING

The most fascinating thing of our day is undoubtedly remote health monitoring. Numerous potentially fatal illnesses are associated with the contemporary lifestyles of its inhabitants. However, with the right measures in place, any of these illnesses may be avoided altogether. However, several deaths occur daily as a direct result of cardiac arrest. The delay between when symptoms first appear and when a patient is seen by a doctor is the primary cause. If patients are being monitored by a remote monitoring system, any changes in heart rate might be sent to physicians and carers in real time through a smartphone app. This type of approach was necessary to prevent needless human deaths[10]. The second rationale is that rural residents simply cannot afford high-priced medical treatment. If there is a way to check their health remotely, they can save time and energy. However, they may go to the local PHC in their hamlet to get comprehensive medical treatment. In order to store and analyse healthcare

data and deliver it back to mobile applications used by the stakeholders in real time, there is a requirement for smart beds integrated IoT system that connects to cloud. As a result, the claim that "remote health monitoring serves common man to avail healthcare services with technology driven approaches" is very significant[11]. The literature study has yielded a wealth of knowledge on the development of new technologies like cloud storage and the Internet of Things (IoT). Additionally, it highlighted ongoing initiatives in the realm of remote health monitoring and its potential realisation via IoT connection with healthcare facilities. But even rural residents with ready access to primary health care facilities need remote monitoring. Several issues from the books are taken into account. First, the issue of proposing a remote health monitoring system based on smart beds for use in village PHC, where data such as a patient's temperature and heart rate (among other parameters that could be obtained via wearable sensors) would be transmitted to a cloud and made available to all parties involved in the use case, including the doctor, via mobile app[12]. Second, the challenge of making the system a reality by capitalising on technological advances. Third, the issue of ensuring privacy in addition to providing end-to-end security for communications in the proposed remote health monitoring system. Therefore, this study considers the difficult topic of creating a new healthcare system that addresses these concerns.

3. LITERATURE SURVEY

New technologies are having an impact on individuals from all areas of life. The Internet of Things (IoT) is the result of a convergence of technologies (cross-disciplinary) that made it possible to connect the digital and physical worlds. Numerous applications will have a tangible impact on society. The healthcare sector, however, is one of the application cases where IoT integration will have the greatest effect on people[13]. It would be ideal if villages who lack the resources to access healthcare could have access to remote health monitoring systems. In this context, we looked at the research done on the subject of implementing healthcare facilities that make use of the Internet of Things in order to provide remote health monitoring services. It sheds light on the potential applications of IoT in the healthcare industry, IoT and robotics, cyber physical systems, security and privacy challenges associated with healthcare systems, and the roles of mobile computing, RFID and NFC-type technologies, machine learning for performing analytics on health data, ECG signal analysis, the cloud, and SOA-based IoT messaging[14]. People's health records must be available in real time to healthcare facilities. Therefore, in addition to identifying technologies like RFID and NCS, they need a kind of technology that enables 24x7 availability, sensing, Internet, and

communication. The Internet of Things enables connections to be made at any time, from any location, and to any object. As a result, it paves the way for healthcare apps to not only achieve availability and scalability, but also to acquire real-time, global access to patients' health records. The technology also allows for inter-object communication[15]. For instance, it works for communications between personal computers, between devices, between humans and devices, and between humans. Hassanalieragh et al. [HPS+15] investigate this hypothesis and provide it in Figure.2. Rapid advancements in IoT technology are facilitating the interconnection of smart items via the Internet in order to provide compatible services in a decentralised setting. According to Boyi Xu et al. [BLH+14], the exponential rise of data is a direct outcome of the Internet of Things' use in healthcare and other fields.

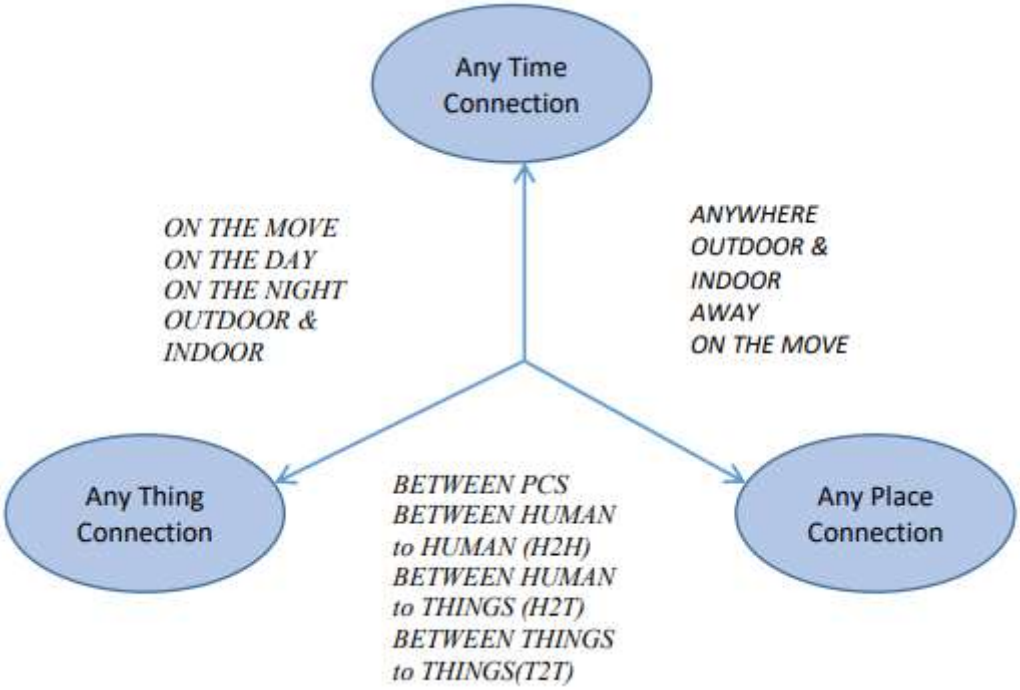

Figure.2: Internet of Things and its suitability for healthcare units

It's difficult to manage such data and implement a system where info may be accessed from anywhere. The availability of many data formats also makes it difficult to standardise on one access mechanism. In the medical field, research conducted by Boyi Xu et al. investigates a resource-based data access mechanism dubbed UDA-IoT. They looked at "the ways and means to have integrated approach in healthcare information system to use data obtained from different IoT sources." For the purpose of storing and making sense of IoT data, they suggested a semantic data model[16]. Stakeholders may have quick access to data on emergency medical services thanks to the UDA-IoT. As Boyi Xu et al. explained in their case

study, "The medical DSS is used to handle emergency medical events with the DSS," the DSS is put to use in the context of dealing with actual medical emergencies[17]. The solution includes a persistency and execution engine, as well as cloud IoT data access services, as well as real-world entities, alternative alternatives, entity-oriented models, and transition-oriented models. In order to make educated judgements, doctors and healthcare system administrators may tap into IoT data sources. "Mobile computing, cloud computing, wireless networks, network operators, mobile users, and cloud computing service" providers are just few of the numerous parts that make up mobile cloud computing. Jiafu Wan et al. investigated MCC's use in medical care [JSX13]. They said that wearable devices can collect real-time patient health data via the integration of MCC with body area networks. Devices using MCC also require less powerful memory and processing power since they can offload these tasks to the cloud. Advantages include "rich user experience and functionalities, efficient performance, patient-centric services, and reinforced" dependability when MCC is linked with a network of wearable devices. Together with mobile devices, patients' usage of body sensor nodes creates a network inside the hospital. In turn, such a system is linked to the web through a series of access points or a central hub[18]. After it is done, the healthcare network will have Internet access to cloud and mobile application servers. The data storage servers may hold the patient's vital signs and use diagnostic algorithms on them. Then, doctors may use the data they've gathered about their patients to provide immediate care. By allowing for data storage and processing to be offloaded to the cloud, as claimed by Hiremath et al., MCC lessens the load on smartphones. electronic health records and provide some insight on radio frequency identification. RFID, in their opinion, is crucial to the development of the Internet of Things and its incorporation into healthcare systems[19]. RFID is essential for identifying medical devices and any physical object that interacts with the digital world. An RFID system requires a plethora of parts. Antenna, Radio Frequency Identification Reader (RFID) Tag, Host Computer, or Host Device. Figure 3 depicts the individual parts.

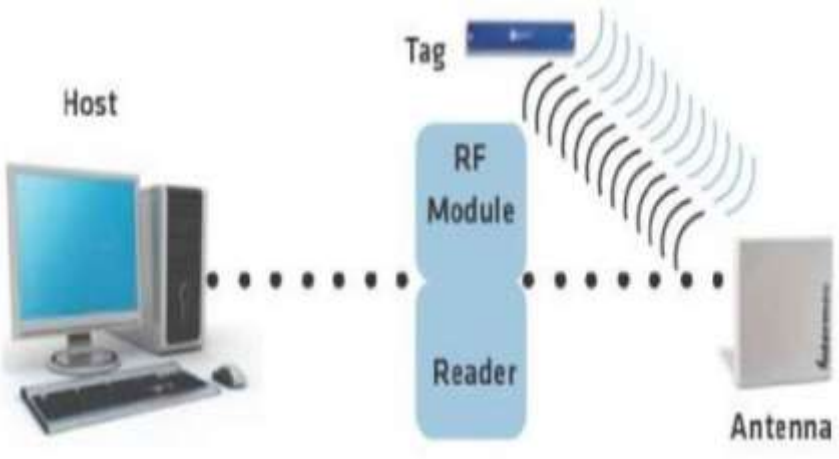

Figure.3: Components in RFID system

Objects may be labelled using tags. Tags not only transmit data to an antenna, but also offer information such as an object's position and any changes to its physical data[20]. There are three different kinds of tags: passive, active, and mixed. Passive tags don't have their own power source and have a lesser read range than their active counterparts, which are those with an inbuilt power supply.

4. RFID BASED REMOTE HEALTH MONITORING SYSTEM

In an IoT-integrated system, radio-frequency identification (RFID) is utilised to track and identify various components. Rao and Reddy [Kha17] devised the technique shown in Figure.4 for monitoring patients remotely. RFID stands for radio frequency identification and is used to create one-of-a-kind item identifiers. An RFID tag, RFID reader, and an antenna are the bare minimum for this technology to function[21]. The antenna on the reader is used to transmit an inquiry signal to the tag. The RFID tag then gives its data in response. Depending on the accessibility of a power supply, RFID tags may be either active or passive. Power-based RFID tags, known as "active" tags, with a range of up to 100 metres. Because of its extensive reach, it may be used in a wide variety of practical contexts. Active RFID tags, for instance, aid in inventory management and transportation efficiency[22]. However, passive RFID tags rely on the RFID reader's electromagnetic energy to function rather than an internal battery. Passive RFID tags may operate up to 25 metres away due to power limitations. Active RFID tags function in all three of these bands. UHF covers the range from 856 MHz to 960 MHz, HF covers the band from 13.56 MHz to 134 kHz, and LF covers the region from 125 kHz to 134 kHz. Like HF RFID, the frequency used by NFC devices is

13.56 MHz. The protocols and standards for NFC are defined in ISO/IEC 14443, which is based on RFID. Therefore, RFID proximity cards adhere to these criteria. NFC is a fine-grained variant of HF RFID that exploits the technology's limitations in terms of read range. For NFC to work, two devices must be in close proximity to one another (within a few centimetres). As a result, NFC has become the de facto standard for safe data exchange between mobile gadgets.

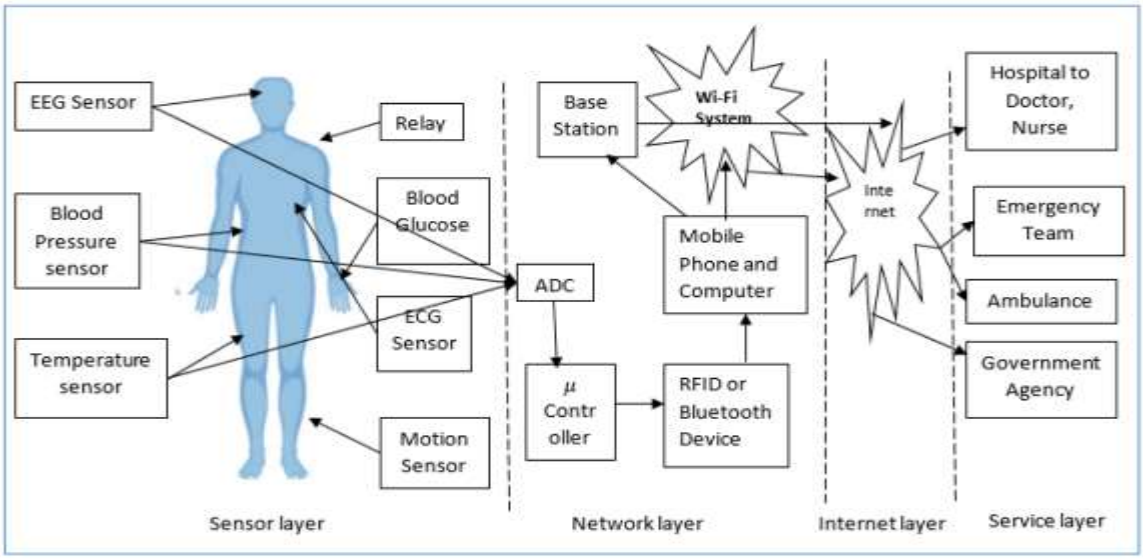

Figure.4: IoT integrated remote heath monitoring system

NFC is distinct from RFID in that it allows for peer-to-peer communication. Because of this, an NFC device may function as both a tag and a reader. As a result, NFC gained traction for use in contactless transactions. As a result, numerous companies in the mobile sector are prioritising NFC integration in their newest handsets. When two NFC-enabled cellphones are touched together, they can exchange information instantly and quickly. NFC is now being used in smart posters for use in the advertising industry. Active NFC tags can only be read by other active NFC devices. Some NFC devices may also be able to read ISO 15693-compliant passive HF RFID tags, depending on how they were built. The NFC tags may also be programmed with instructions that launch certain mobile apps. More widespread use of near-field communication (NFC) tags and high-frequency radio-frequency identification (HF RFID) tags in consumer-facing applications including posters, signage, and ads. To restate, NFC is based on high-frequency (HF) RFID, and its range restrictions become an indisputable strength in the context of near-field communication. In this work, RFID is favoured for empirical research over NFC because of the latter's range constraints. Figure.4 depicts a system with several sensors, including those for electroencephalography (EEG),

blood pressure, temperature, relay, electrocardiography (ECG), electrocardiogram (ECG), and motion. The analogue signals provided by the sensors are processed by an Analogue to Digital Converter (ADC) to produce digital data. The collected information will be sent back to the hub. Multiple entities, including law enforcement, EMS, and medical professionals, may view the data remotely from the base station over the Internet. The system consists of four distinct levels. Sensor, Network, Internet, and Service Layers are the various tiers involved. The system's benefits are extensive, including cost savings, improved efficiency, and improved patient time management. The suggested system is described theoretically. However, there has been little to no empirical research done, and no safeguards are offered.

5. IOT FOR REMOTE HEALTH MONITORING

The healthcare industry is one that affects individuals from all areas of life. Numerous tools and pieces of machinery have been developed and used with the help of ICT to improve healthcare delivery in this field. Internet of Things (IoT) is a cutting-edge technological framework for connecting and syncing devices in the real and virtual worlds. Wearable devices, RFID, NFC, WSN, WSAN (Wireless Sensor and Actuator Network), cloud computing, mobile cloud computing, web services, Service Oriented Architecture (SOA), smart homes, Web 2.0, Web 3.0, and gateway technologies to seamlessly integrate cross-domain devices to reap the benefits of innovation. Using the Internet of Things and its applications, we may achieve the synergistic impact of these technologies. Unprecedented quality in healthcare services is possible when IoT is realistically integrated with healthcare facilities. The Internet of Things allows for the remote monitoring of health thanks to its integration of many technologies. In this thesis, this is the central hypothesis that drives the investigation. To that aim, this article sheds insight on how the Internet of Things might be used to remote health monitoring. Existing technology and emerging standards are used to implement IoT. Given its role in bridging the gap between the digital and the physical, it must make use of any appropriate technology. It relies heavily on organisations' preexisting physical and digital infrastructure, including sensors, communications tools, and other forms of communication and computer networks. An organisation may gain from connecting its infrastructure to the IoT with its support. The architecture of the Internet of Things is multilayered. Figure 5 depicts the layered construction.

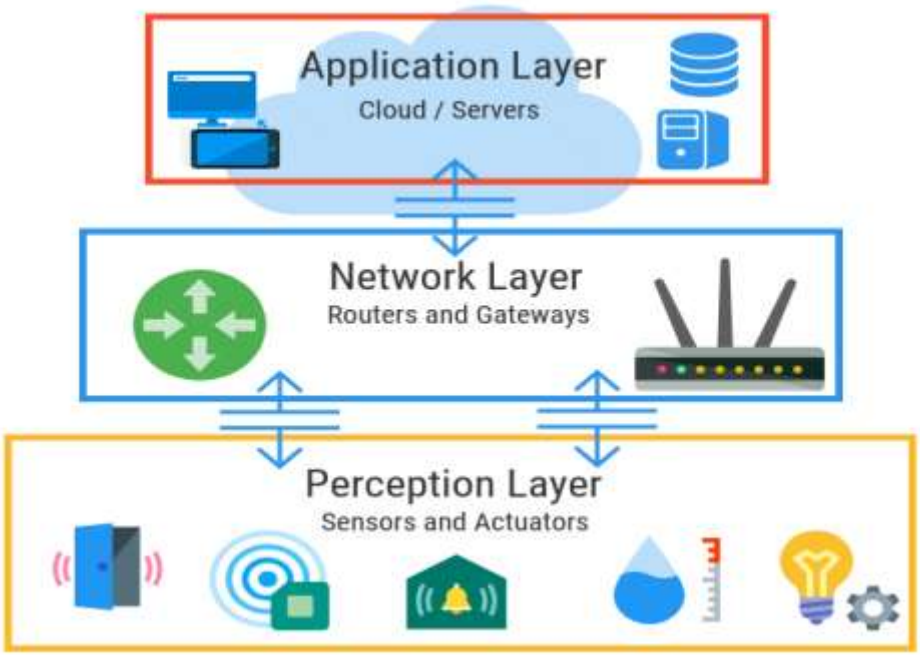

Figure.5: Architectural overview of Internet of Things technology

The IoT architecture consists of several different parts. They are the "network layer" and the "sensors connectivity" layers. Sensing technologies, sensors, actuators, RFID tags, etc., make up this layer. Detection and labelling are also handled by this system. Then, assistance at the gateway and transport layers is required. Existing gateway protocols are encapsulated here. The modelling, configuration, management, security control, and dataflow management of devices are all handled by the management service layer. Then, the application layer stands in for any and all domain-specific real-world business applications. The next section goes into more detail on the interplay between several business areas and IoT. The Internet of Things makes it possible to link objects at any given moment, in any given setting, with any given person, service, company, route, network, location, or device, anywhere on the planet. The Internet of Things relies on "smart objects" as its foundation. Connectivity is an always-on feature of smart things. One application of the Internet of Things is smart cities. Increased connection and the actualization of M2M are both possible in IoT-integrated cities. It's also useful in "smart health," where it may be used to keep tabs on a patient at all hours and guarantee a timely diagnosis and course of treatment. The potential for a more expansive Internet of Nano Things to one day materialise is exciting. Hyderabad, India's Call Health is one healthcare service provider working to implement this goal via Internet of Things integration

[BLH+14]. IoT enables context-aware computing, which may be used in a variety of commercial settings. Figure.6 depicts the whole of the IoT opportunity space.

Figure.6: IoT utility in domain dependent/independent industries

Some important vertical markets are listed below. In truth, businesses in every sector may reap the benefits of IoT integration. Smart home, agriculture, healthcare, transportation, industry, market, and education are just some of the vertical domain specialised applications available. All of these companies need broad market services that are not exclusive to any one industry. To guarantee scalability and availability, data for all sectors or applications in vertical domains is stored on the public cloud. Actions based on analytics may be provided by application-domain specialised services like data mining. There is also interaction between intra-domain sensors and actuators. Therefore, the value of the Internet of Things is quite high, and people all over the Earth will feel its effects in the not-too-distant future.

6. RESULTS AND ANALYSIS

Here we provide the empirical study's findings in terms of security analysis, encryption performance, decryption performance, upload/download times, and temperature/heart rate

monitoring. In the context of remote health monitoring, parameters such as core temperature and heart rate are tracked and recorded. Foreign heat is used to assess temperature, whereas beats per minute is used to quantify the rate of the heart.

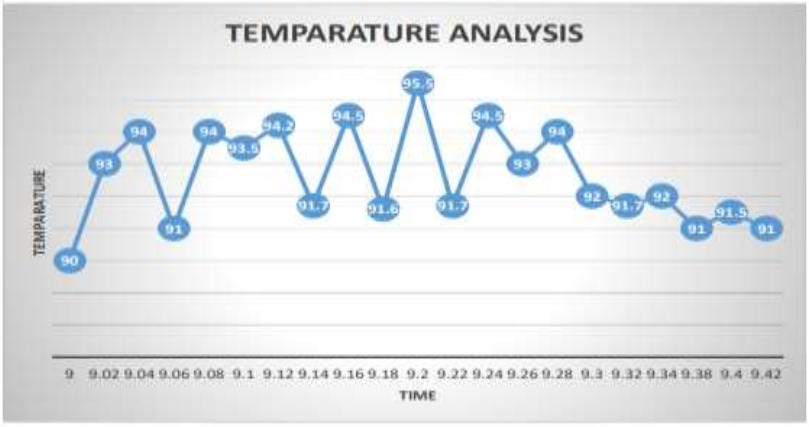

Figure .7: Temperature monitored by the remote health monitoring system (Patient1)

The horizontal axis of Figure.7 represents the time at which the patient's core temperature was measured. Temperature is shown in degrees Celsius on the vertical axis. The findings indicate that core body temperature fluctuates throughout time. By keeping an eye on the patient's core temperature, doctors can determine whether they are experiencing any of the many illnesses that might manifest themselves in this way. Given that temperature is regarded an important indication in the medical field. It's useful for doctors to get an idea of how well their therapy is working. Disease-specific triggers like fever are common. It gives the doctor crucial information for making educated choices. The body's normal temperature is adjusted to facilitate the body's natural defensive system. Taking one's temperature may be done in a variety of settings. Forehead, underarm, mouth, ear, and rectum are all examples. A typical body temperature ranges from between 97.3 to 99.5 degrees Fahrenheit. A fever or a fever induced by another ailment is diagnosed if the temperature rises over this threshold. All of these notes pertain to Patient 1. The horizontal axis of Figure.8 represents the time at which the patient's core temperature was measured. Temperature in a different heat unit is shown along the vertical axis. The findings indicate that core body temperature fluctuates throughout time. By keeping an eye on the patient's core temperature, doctors can determine whether they are experiencing any of the many illnesses that might manifest themselves in this way. Given that temperature is regarded an important indication in the medical field. It's useful for

doctors to get an idea of how well their therapy is working. These notes pertain to Patient #2.

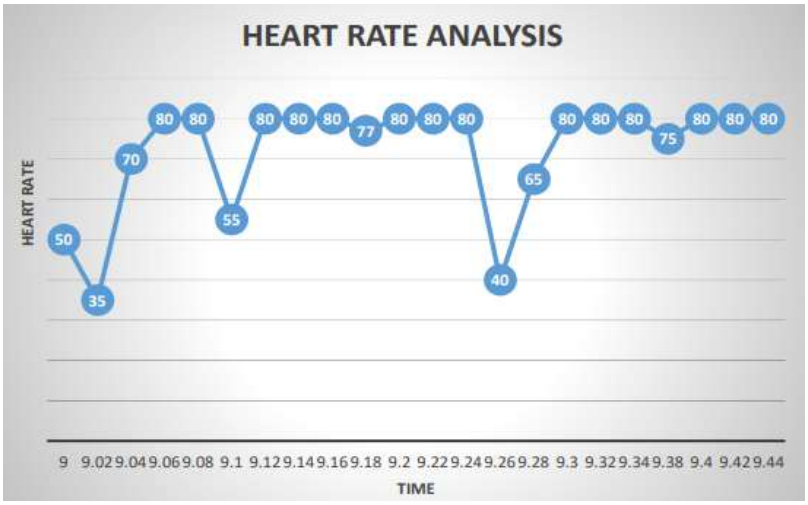

Figure.8: Heart rate analysis of patient 1 with the remote health monitoring system

Figure.9 displays the heart rate of patient 1 along the vertical axis and the time at which the measurements were recorded along the horizontal axis. One's pulse rate is the number of times their heart beats in one minute. In other terms, it represents the rate at which one's heart beats in one minute. Rate of heartbeat is another name for it. Individuals have different resting heart rates. However, doctors may use the information gleaned from monitoring this to better diagnose cardiac problems. Size, drugs, nicotine/caffeine intake, mood, physical exertion, and environmental factors all have an impact on heart rate. Adults have a resting heart rate of 60-100. The remote health monitoring system's ability to provide the patient's heart rate is a crucial indicator for doctors. When a patient's heart rate is irregular, it's critical to take immediate action to restore normal function.

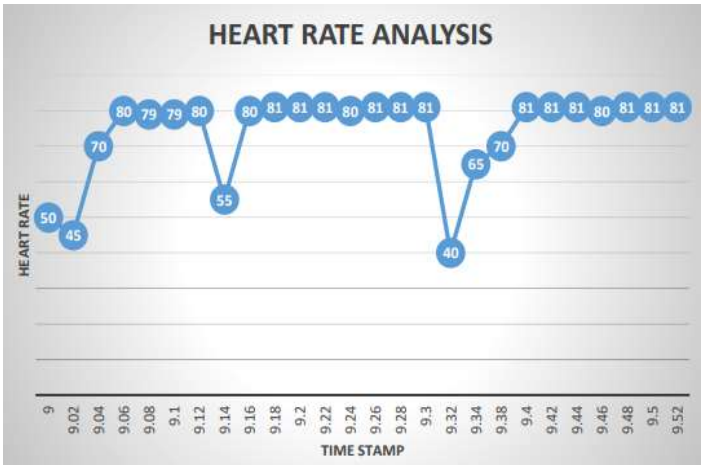

Figure.9: Heart rate analysis of patient 2 with the remote health monitoring system

Figure.9 displays the heart rate of patient 1 along the vertical axis and the time at which the measurements were recorded along the horizontal axis. One's pulse rate is the number of times their heart beats in one minute. In other terms, it represents the rate at which one's heart beats in one minute. Rate of heartbeat is another name for it. Individuals have different resting heart rates. However, doctors may use the information gleaned from monitoring this to better diagnose cardiac problems. If the patient has a cardiac condition, this may be determined by monitoring their heart rate. The reason for monitoring this indicator is because cardiovascular disease is among the leading causes of mortality worldwide.

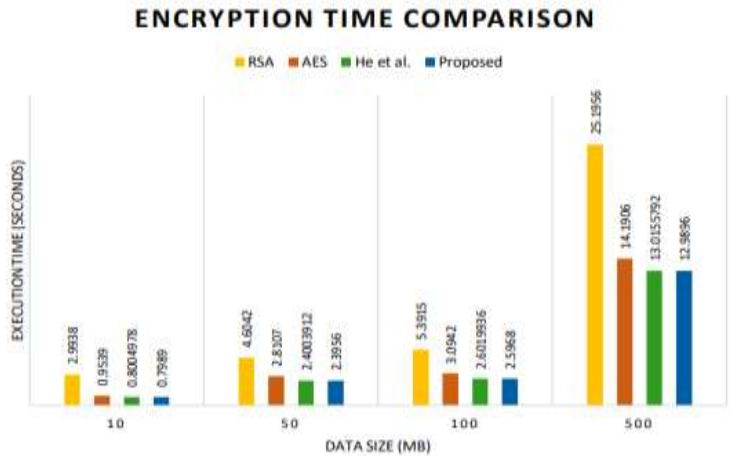

Figure.10: Encryption performance analysis

Figure.10 shows the results of a study into the encryption algorithm's performance in terms of runtime. The horizontal axis lists the security primitives that were employed in the empirical investigation, while the vertical axis lists how long it takes to execute each of those primitives. In seconds, the code will be run. Experiments are conducted with varying amounts of data, from 10 MB to 50 MB to 100 MB to 500 MB, among others. The encryption time required by the security methods grew linearly as the magnitude of the workload did. RSA's execution time was longest across the board. The suggested method outperforms the current gold standard. Comparing the proposed system against those of He et al., AES, and RSA, it was shown to have the quickest runtime. This is justified by the fact that the suggested security method is quite lightweight.

7. CONCLUSION

This study lays the groundwork for an IoT-integrated remote health monitoring system. It elucidates not only the architecture of the Internet of Things, but also its significance across sectors, the function of RFID, and the role of RFID and microcontrollers in realising the IoT.In terms of evaluating vital indicators like temperature and heart rate, it shows the findings. In addition, it sheds information on the proposed system's security analysis by comparing it to well-known security techniques like RSA and AES. After that, the system's execution time for encryption, decryption, uploading, and downloading data is analysed, and the findings are shown. We evaluate the suggested system against the findings of AES and RSA. It is well acknowledged that conventional cryptographic methods are inadequate for many Internet of Things (IoT) deployments.

REFERENCES

1. World Health Organization. (2018). Towards a Global Action Plan for Healthy Lives and Well-Being for All: Uniting to Accelerate Progress Towards the Health-Related SDGs World Health Organization. [Online]. Available: https://apps.who.int/iris/handle/10665/311667
2. WHO/ITU National eHealth Strategy Toolkit, World Health Org., Geneva, Switzerland, 2012.
3. G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, “Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain,” J. Commun., vol. 12, no. 4, pp. 240–247, Apr. 2017.
4. A. A. Toor, M. Usman, F. Younas, A. C. M. Fong, S. A. Khan, and S. Fong, “Mining massive E-health data streams for IoMT enabled healthcare systems,” Sensors, vol. 20, no. 7, p. 2131, 2020.
5. H. Mshali, T. Lemlouma, M. Moloney, and D. Magoni, “A survey on health monitoring systems for health smart homes,” Int. J. Ind. Ergonom., vol. 66, pp. 26–56, 2018, doi: 10.1016/j.ergon.2018.02.002.
6. G. Cai, Y. Fang, P. Chen, G. Han, G. Cai, and Y. Song, “Design of an MISO-SWIPT-aided code-index modulated multi-carrier M-DCSK system for e-Health IoT,” 2020, arXiv:2003.07107. [Online]. Available: https://arxiv.org/abs/2003.07107
7. X. Zhang, L. Yang, Z. Ding, J. Song, Y. Zhai, and D. Zhang, “Sparse vector coding-based multi-carrier NOMA for in-home health networks,” IEEE J. Sel. Areas Commun., early access, Aug. 31, 2020, doi: 10.1109/JSAC.2020.3020679.
8. S. Misra, A. Roy, C. Roy, and A. Mukherjee, “DROPS: Dynamic radio protocol selection for energy-constrained wearable IoT healthcare,” IEEE J. Sel. Areas Commun., early access, Aug. 31, 2020, doi: 10.1109/JSAC.2020.3020679.
9. B. D. Deebak and F. Al-Turjman, “Smart mutual authentication protocol for cloud based medical healthcare systems using Internet of medical things,” IEEE J. Sel. Areas Commun., early access, Sep. 7, 2020, doi: 10.1109/JSAC.2020.3020599.
10. S. S. Gopalan, A. Raza and W. Almobaideen, "IoT Security in Healthcare using AI: A Survey," *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, Sharjah, United Arab Emirates, 2021, pp. 1-6, doi: 10.1109/ICCSPA49915.2021.9385711.
11. T T Chhowa, M A Rahman, A K Paul and R Ahmmed, "A Narrative Analysis on Deep Learning in IoT based Medical Big Data Analysis with Future Perspectives", *2nd Int. Conf. Electr. Comput. Commun. Eng. ECCE 2019*, pp. 1-6, 2019.
12. C Ieracitano, A Adeel, M Gogate, K Dashtipour, F C Morabito, H Larijani, et al., "Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection", *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10989 LNAI, pp. 759-69, 2018.

13. A K Alharam and W El-Madany, "Complexity of cyber security architecture for IoT healthcare industry: A comparative study", *Proc. - 2017 5th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2017*, vol. 2017-Janua, pp. 246-50, 2017.
14. P Ghosal, D Das and I Das, "Extensive survey on cloud-based IoT-healthcare and security using machine learning", *Proc. - 2018 4th IEEE Int. Conf. Res. Comput. Intell. Commun. Networks ICRCICN 2018*, pp. 1-5, 2018.
15. D He and S Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography", *IEEE Internet Things J*, vol. 2, pp. 72-83, 2015.
16. A M Elmisery, S Rho and D Botvich, "A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things", *IEEE Access*, vol. 4, pp. 8418-41, 2016.
17. S. M. Karunarathne, N. Saxena and M. K. Khan, "Security and Privacy in IoT Smart Healthcare," in *IEEE Internet Computing*, vol. 25, no. 4, pp. 37-48, 1 July-Aug. 2021, doi: 10.1109/MIC.2021.3051675.
18. M. Wazid, A. K. Das, N. Kumar, M. Conti and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment", *IEEE J. Biomed. Heal. Inf.*, vol. 22, no. 4, pp. 1299-1300, Jul. 2018.
19. Y. Yang, X. Liu, R. H. Deng and Y. Li, "Lightweight sharable and traceable secure mobile health system", *IEEE Trans. Dependable Secur. Comput.*, vol. 17, no. 1, pp. 78-91, Jan./Feb. 2020.
20. S. R. Moosavi, E. Nigussie, M. Levorato, S. Virtanen and J. Isoaho, "Performance analysis of end-to-end security schemes in healthcare IoT", *Proc. Comput. Sci.*, vol. 130, pp. 432-439, 2018.
21. F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges", *IEEE Commun. Surv. Tuts*, vol. 22, no. 3, pp. 1686-1721, Jul.–Sep. 2020.
22. Y Leandro et al., "Exploiting IOT technologies for enhancing Health Smart Homes through patient identification and emotion recognition", *Computer Communications.*, vol. 89, pp. 178-190, 2016.