IoT based smart medical data security system

Lakshman Kumar Kanulla, Dr. G. Gokulkumari$^{2[0000-0002-8556-1071]}$, Dr. M. Vamsi Krishna $^{3[0000-0001-5285-9990]}$and Santhosh Kumar Rajamani 4[0000-0001-6552-5578]

[1] Software Engineer, Department of SAP SD MM, Working for Apple Inc, knvslakshmankumar@gmail.com
[2] Department of E-Commerce, College of Administration and Finance, Saudi Electronic University , Riyadh -13323, Kingdom of Saudi Arabia, g.govindasamy@seu.edu.sa
3 Department of IT, Aditya Engineering College, Surampalem, India, vkmangalampalli@gmail.com
4 Department of E.N.T, MAEER MIT Pune's MIMER Medical College and Dr. BSTR Hospital, minerva.santh@gmail.com

Abstract. Health 4.o is an approach to healthcare innovation using IoT and other sensors and devices. The result is an array of intelligent health applications that are more equipped to improve people's health and well-being in practical ways while also being more reliable, scalable, and economical. However, IoT-based healthcare systems may pose problems without proper oversight, especially regarding security concerns like exposed application interfaces. Primary challenge is to learn about the architecture and security needs of IoT-based multi-sensor systems and healthcare infrastructures. In addition, it has to propose lightweight, easily implementable, and efficient designs. This research introduces the Internet of Things (IoT) in healthcare and a thorough analysis of practical, novel health frameworks that use a wide range of resources and limited-power sensors and devices. Additionally, this paper also focuses on the safety of these vital Internet of Things components and their wireless connections. The result is introduction of a lightweight-based security system that uses the Lightweight Encryption Algorithm by IoT(LEAIoT). Essential creation with the proposed hardware-based method is 97% faster than with a software-based approach, and encryption/decryption is faster by 96.2%. Finally, it is competitive with other typical hardware-based cryptography designs, achieving reduced hardware usage of up to 77% with the lowest frequency with its lightweight, flexible implementation and configuration of high-speed keys.

Keywords: IoT, Health 4.o, Multi sensors, Security, frame work,

1 . Introduction:

Medical gadgets changed healthcare. Now we can track our health without going to the hospital. We need to examine the security of such devices not withstanding this drastic development.

These technologies compromise privacy and security. Medical device security is critical since many patients' lives rely on it. Healthcare security is crucial.

Wearable Internet of Medical Things devices diagnosis patient health. These gadgets monitor physical activity, temperature, diabetes, sleep, heart rate, and more. Smart wristbands, watches, glasses, belts, necklaces, and patches are available from head to toe.

Wearable systems include sensors, memory, solar cells, and batteries. They gather, display, and wirelessly transmit data. Gadgets may communicate patients' health data directly to doctors to reduce office visits.

Modern information technologies like the Internet of Things (IoT), big data, cloud computing, and artificial intelligence have made healthcare smarter. Care of this kind is more effective, convenient, and individualized than the alternative. Electronic healthcare systems (eHealth) based on the Internet of Things (IoT), mobile healthcare (mHealth), and ambient assisted living (AltHealth) are all part of "smart healthcare" (sHealth). Smart Healthcare Systems (SHS) are widely used presently because of their practical data storage and sharing system, fast reaction times, and reduced treatment costs. With the aid of IoT devices, patients' private medical records may be securely saved in the cloud and shared with doctors and other patients. As a result, the telecare e-medical service model may provide care recommendations based on data gathered from the patient's medical monitors. Care for patients with long-term conditions, including critical care emergency services, heart patient symptom records, and more are part of this process. These IoT-based monitoring devices may collect vital signs and transmit them to a cloud server using implanted sensors. In the future, members of the savvy community may share this information. Network assaults, such as denial of service (DoS) attacks, router attacks, replay attacks, etc., threaten the privacy of transmitted data. Additionally, at any one time, a vast quantity of patient data is being saved in the cloud platform to make diagnoses or provide recommendations, might be challenging to keep sensitive data safe in a third-party cloud [1].

These days, medical computing equipment may connect to the IoT and send patient data and photos via the internet without any intervention from a person. User-level components of the echo system include the patient, doctor, pharmacist, etc., while storage-level features include a cloud data centre housing real-time and asynchronous application. Data sharing and communication are hampered by the complexity and volume of available data. The delays in responses and communications are also an issue. Most standard cloud computing solutions fall short of the service needs of real-time applications like remote medical care during emergency scenarios. An edge-based computing facility that speeds up responses while decreasing network latency may resolve this problem. Therefore, IoT solutions need an edge and fog computing to protect patient confidentiality. Mediation at the sensor network's periphery may enable data to be processed closer to its origins (the healthcare network), strengthening user privacy and data security. This mediation layer can manage enormous volumes of data, expedite computing, improve mobility, and increase privacy with low latency and bandwidth, addressing these obstacles. Edge computing may process healthcare data twice. For a timely decision, edge nodes collect and analyse sensor data. Second, distant health cloud data centres handle vast volumes of data (clinical test results, scan images/reports, etc.). Sensor data are used for essential choices like monitoring oxygen, glucose, cardiac pumps, etc.

In 2019, we saw the emergence of a new virus that causes a disease called Coronavirus. Also known as COVID-19, it was formally reported on December 31, 2019. Infections with this virus cause both SARS and MERS, which might result from problems in breathing, headaches, fever, and even respiratory collapse. It's contagious. Therefore it's not safe for otherwise healthy people to become involved. This needs a system that can track changes as they occur in real-time. Strong authentication is essential whenever sensitive patient data is accessed in such a system. Literature [2, 3], [4] provides a variety of authentication frameworks. However, the authentication process takes longer because of most three-factor-based authentication frameworks' high False Rejection Rate (FRR). However, although IoT with edge computing may help, the currently suggested solutions are not flexible enough to deal with both scenarios without compromising privacy or security.

It is widely believed that IoT will become standard in all technologies of the next generation [1]. In this context, "interconnection" refers to the linking together of innovative items and gadgets via which they may be detected solely. Invisible sensors connected to many things around us provide IoT with a wealth of tracking data [2]. Research indicates that health monitoring is the most promising field for future wearable electronics (HM). Smart HM [3] combines innovative computing, remote HM, and the Internet of Things.

HM expands clinical monitoring and care limits (i.e., house, for instance). An HM system consists of a smartphone with internet access and an HM app, a monitoring device for submitting health data to smart contracts [4]. Wearables and IoT are important for HM and intelligent cities [5]. Wearable devices capture patient health data for healthcare administration, diagnosis, and patient care. A Big Data scenario [6] arises as medical records are analysed and shared. A secure data interchange between organisations is also required [7].

Security is a significant consideration for any setup. There are several security definitions since individuals have different perspectives [8,9]. In a broad sense, security may be thought of as a concept analogous to the system's overall stability. Most modern IoT-centric HM relies on wireless connectivity, posing several potential security risks [10,11]. These security concerns might cause significant difficulties for wireless sensor equipment [12,13]. Thus, medical and health data management needs lightweight block encryption techniques for medical IoT resources [14].

Predicting abnormal health changes from the Internet of Things data [17,18] is accomplished via the use of data mining techniques, including classification and clustering [15], neural networks [16], and other machine learning approaches. The study that utilises clouds and IoT technologies forms the foundation for a secure patient HM system using BC-XORECC and a patient monitoring system utilising LSK-RNN, which together permit the safe transfer of data and offer accurate patient monitoring. As a result, doctors could keep tabs on the patient from afar and catch potentially fatal conditions in their earliest stages.

Several dangers and vulnerabilities are associated with utilising the IoT for intelligent health, and they may be categorized into two broad categories: embedded and network problems [2]. Dealing with the hardware and software of IoT-based devices might lead to embedded difficulties. The number of IoT nodes has limited resources, such as battery life or data storage space.

Robotic or remotely controlled gadgets. They are not designed to run resource- and computation-intensive security techniques. Lightweight cryptography's ability to sufficiently protect the design while making more minor hardware demands is the key to solving this issue. However, many substitute methods are less secure than the widely-known heavy cryptographic primitives [7]. Further, most digitally savvy healthcare providers must allocate more resources to ensure the three pillars of security [8].

They are only concerned with the healthcare features of the app and the savings on deployment. The outcome is a system readily exploited due to poor security measures and inadequate upgrades. The scalability creates another potential weakness.

In particular, new devices are being added to the system without any assurance that they will maintain its security. An attacker may access the more extensive system by compromising a tiny, unsecured device. Thus, even the smallest devices interacting with the centralised services need some lightweight security strategy that keeps them safe from harm.

2 IoT based health care security system:

IoT technology can develop several smart health apps, accomplishing Health 4.o goals [4]. Figure 1 shows the integrated technology and healthcare architecture components of Health 4.o. High-quality services for persons with diverse healthcare requirements are a crucial goal that involves optimizing tools, resources, and system performance. Automation and intelligence may improve outcomes and speed up monotonous activities. Remote access and real-time answers aid medical care and monitoring. Finally, designing databases with complete and easy-to-access medical information helps improve diagnostics and tailored therapy.

Another important goal is to improve operations while reducing expenses, resource use, and energy usage. Thus, energy-constrained IoT devices may run healthcare applications. In the end, resources will balance the critical and actual requirements of the system. The best strategy maximises performance throughput with few resources. IoT may help monitor, diagnose, and forecast illness through health sensor data.

Cloud services quickly transmit, evaluate, and store this data, making diagnosis more straightforward and accurate. Cost-effective, user-friendly, and promptly responsive health assessment procedures will relieve healthcare staff and materials. Finally, information exchange and cooperation between healthcare institutions and providers will be easy and timely.

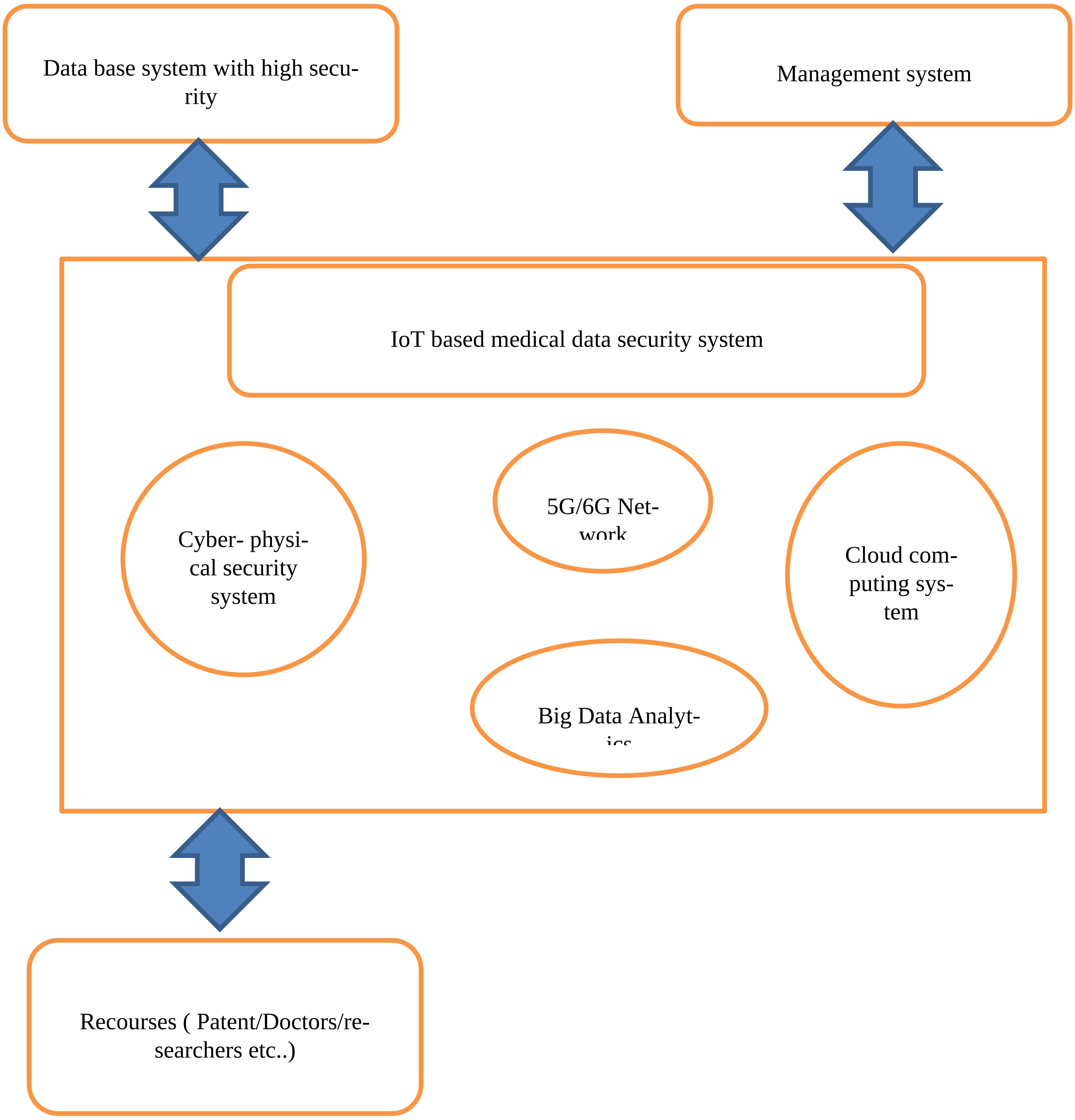
Data base system with high security
Management system
IoT based medical data security system
Cyber- physical security system
5G/6G Network
Cloud computing system
Big Data Analytics
Recourses (Patent/Doctors/researchers etc..)

Figure 1: Framework of the IoT based medical data security system

2.1 Proposed work:

- First, the utilized cryptographic primitive guarantees the maintenance of the fundamental security principles while being lightweight and able to use keys ranging in size from 64 to 520 bits. The width of the key is a generalisation of the measure of symmetric encryption's security; 520 bits is the minimum acceptable for most applications, as practical and crucial to the suggested setting.
-
- Assures efficient handling of the large amount of data sent between devices in the Internet of Things. Cryptographic primitive ran on a computer's processor (Central Processing Unit), boosting essential creation speed by up to 99.9%, and the rate of encryption and decryption is as high as 96.2%.
- Third, four distinct key sizes are included in a single architecture, Applications may achieve four different performance rates and levels of security efficiency. Instantaneously choose based on the state of the network and the required amount of processing power for the application. As a result, the system is versatile and readily adapted to situations that vary considerably.
- In the end, implement the cryptographic technique to prove its worth as resource effectiveness without sacrificing throughput. It meets the performance criteria of intelligent health and is readily accessible when used on the different nodes of the IoT network, and it protects a national and international level organization of healthcare while keeping resources in a state of optimal performance, efficiency and safety

3 Implementation process:

The IoT architecture comprises applications, networks, and physical/perception layers [11]. The application layer connects IoT devices [11]. E-health applications are included. Network layer protocols allow IoT components to communicate physical layer data. Popular networks include ZigBee, 5G, Wi-Fi, RFID, 6LoWPAN, and LoRaWAN. IoT-integrated WSN is another node network [18]. The physical/perception layer terminates architecture. It encompasses sensors, wearables, actuators, cellphones, antennas, and CPUs. This layer translates health signals to network data.

3.1 Infrastructure of IoT based medical data security system:

Figure 2 depicts an IoT-based Health infrastructure. This arrangement shows IoT-healthcare linkages. This article compares smart hospitals with near-patient/personalized systems. Individualized revolutionary health architecture comprises heterogeneous IoT devices, a wireless interface, and a cloud-based database. [2, 3]. Medical equipment gets sensors first.

They use batteries, therefore maximizing efficiency is essential. To send "sensed" data, they must connect to the system's wireless network. Multiple sensors and gadgets are used simultaneously, where their connectivity is crucial. Wearable equipment must also be lightweight and pleasant. Some implanted and wearable devices may wirelessly receive orders to modify medicine doses or gadget settings. The wireless interface must connect to the Internet to provide health data to physicians and nurses. The hospital or private clinic's main computer or near-patient IoT system may process this data. Some wearables can analyze and wirelessly communicate data to the Internet. Fixed or mobile devices may replace small, wearable, and implantable devices without processing capability. These intermediary devices evaluate sensor data from various IoT networks and transfer it to back-end systems and databases. They can also interface with sensors and process back-end data. These gadgets gain intelligence and real-time capability by making decisions and acting without back-end infrastructure. IoT devices lack storage. Thus, medical history is stored in databases.

IoT may improve hospital relationships and functionality.

Hospitals may use all implanted and wearable IoT devices. These sensors and gadgets must also be connected to wired and wireless networks and accept orders and sensitive data from authorized sources. Two things distinguish this hospital building:

With the help of the Internet of Things, hospital beds and other medical devices may now connect to the network and share confidential patient information for diagnostic purposes.

The hospital's medical records and healthcare database are to the IoT network. Thus, hospital staff may obtain real-time data and react to situations. All hospital devices can quickly retrieve the patient's medical history from the recorded data.

The hospital's Internet of Things (IoT) network communicates with other healthcare facilities and Internet-connected devices close to the patient.

More tailored and sophisticated health services will help healthcare professionals reduce hospital resource strain.

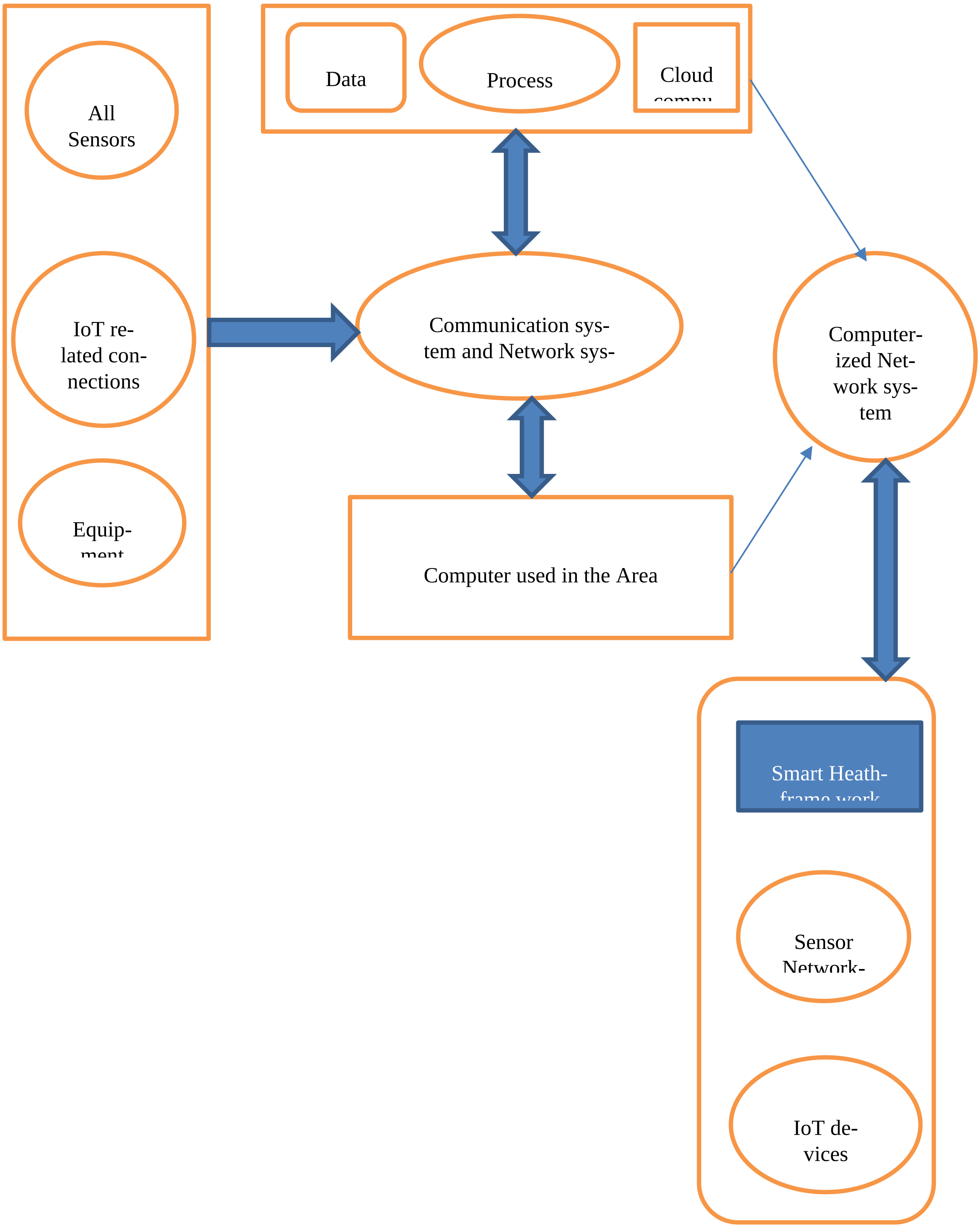
All Sensors
IoT related connections
Equip-
ment
Data
Process
Cloud
compu
Communication system and Network sys-
Computer used in the Area
Computerized Network system
Smart Heath-
frame work
Sensor
Network-
IoT devices

Figure 2: IoT-based Health architecture

3.2 Security system and scheme:

High security is essential for IoT-based healthcare applications. When it comes to attacks on the intelligent health infrastructure, the Internet of Things (IoT) network (Figure 2) is the weakest link [2]. IoT network attackers may readily access devices' personal data. Eavesdropping and data transmission/traffic tracking are major data privacy breaches [11]. Data protection also affects user authentication. Unauthorized devices may access and manipulate this data. They may potentially send false health data to the IoT network. This causes misdiagnosis and inconsistent health-provider communication.

Researchers prioritise safe communication network development. Cryptography protects data, authenticates users, and uses cyphers to encrypt and decode messages. Due to resource limits, the IoT system cannot employ cryptographic primitives. The cypher must not divert resources from other vital healthcare functions. Thus, IoT hardware restrictions need a lighter version. In crucial situations, low-speed algorithm implementation might delay real-time applications, which can be disastrous. Therefore, must consider quickness and responsiveness. Finally, each capability must have numerous alternatives to meet the application's network and security demands. The system needs flexibility and scalability.

A lightweight cryptographic primitive and security method is needed to secure smart health application health data. Before IoT devices communicate data, the encryption method must encrypt it. Thus, patient data is safe from hackers. For healthcare applications, the decryption algorithm must decode this received data. The outcome is complete data content security in communication networks, particularly IoT networks and cloud-connected Internet.

4 Implementation process of Security system and scheme:

The current system's lightweight-based security method leverages the LEAIoT cryptographic primitive to encrypt and decode data while offering variable key size and implementation speed. This approach is embedded into every Internet of Things (IoT) device in a healthcare system, securing sensitive patient information over public networks like the Internet and within private ones like smart hospitals and near-patient infrastructures. LEAIoT beats traditional encryption primitives in key generation and encryption/decryption speed. The IoT-based healthcare system's complicated connection demands benefit from a lightweight design, and It enables fast end-to-end communication with little hardware. LEAIoT mixes symmetric and asymmetric encryption methods. Symmetric cryptography improves performance with fewer resources; Asymmetric primitives increase key distribution, scalability, secrecy, and authentication.

LEAIoT encrypts a made-up plaintext with an n-bit private key; the sender and recipient are well-informed. NLBC employs ciphertext with two legends: n1 and k. They are protecting encrypted content. Decryption uses the modular inverse of the three encryption keys, SSK, n1 (1), and k0. Delivered ciphertext and keys n1 (1) and k (0) are needed for asymmetric NLBC decryption. These keys are made using n1 and k's modular inverse modulo 27. Using symmetric decryption, you can acquire the plaintext if you know the modular inverse of the n SSK key. This technique continuously calculates the modular inverse modulo 27. The following material analyses ciphering and decoding.

1. The key n multiplies the synthetic plaintext values. Modulo 27 follows;
2. The secret code k is a 3x3 matrix that keeps secret. Aside from that, the length of the key n is computed and used as the key n1;
3. In the first stage, the created text is split into sections using the critical k to identify each section. You are multiplying by k and n1 for each block bi. Here comes Module 27.;
4. The secure ciphertext is the original plaintext;

Decryption sequence:

1. Use the modular inverse of the keys n1 and k modulo 27;
2. Divide the received ciphertext into blocks bi, as in step 3 of the encryption process.
3. Multiply each block with the two keys k 0 and n1 (−1). Modulo 27 follows;
4. The text is multiplied with SSK and modulo 37 again;
5. The result displayed in plaintext.

The suggested lightweight-based security system. The Lightweight Encryption and Decryption for the Internet of Things (LEAIoT) use Symmetric and staged asymmetric encryption and decryption. Users may customize the playback duration of the key pairs with a symmetric key length of 64, 128, 256, or 520 bits.

5 Results:

Simulate symmetric and asymmetric key insertion and modular inverse computation. Figures 3 demonstrate the two processes for different key sizes.

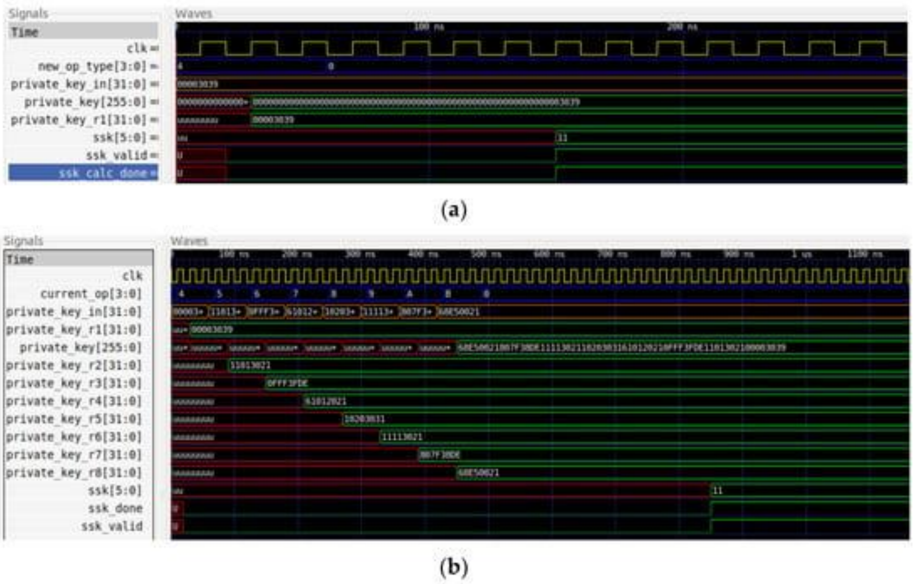

Figure 3: the two processes for different key sizes

Each encryption/decryption cycle processes three 7-bit characters. Each function takes nine clock cycles. The first cycle starts with the encryption or decryption procedure, which complete in eight cycles. Table 1 represents the cycles needed in symmetric and asymmetric to generate both keys. These clock cycles provide the start signal.

Table 1: cycles needed in symmetric and asymmetric to generate both key.

Symmetric key size of the bit	**Insertion of symmetric key**	**Inverse of the modular symmetric key**	**Insertion of asymmetric key**	**Inverse of the modular asymmetric key**	**Total**
64	4	7	7	66	74
128	12	10	7	66	81
256	18	14	7	66	97
520	36	21	7	66	116

Finally, the security and performance criteria will assess the design. Simulation validated the cryptographic primitive's security. It has four different vital sizes, so users may adjust it to meet their needs regarding network speed and security. A minor key size might speed up the encryption process when traffic is heavy on the network. A more considerable key length may be a good option when protecting sensitive information. Transmission rates and system availability have both seen boosts thanks to faster key generation and encryption/decryption. So, it's fast enough for the Internet of

Things. Finally, the synthesis results and comparisons with other hardware-based research demonstrated that the recommended design for IoT-based healthcare systems is lightweight and efficient. New approaches to security are being developed to strike a good balance between availability, efficiency, and safety in an IoT-based healthcare architecture.

6 Conclusion:

This article presents an overview of IoT-based multi-sensor architecture, the Health 4.o design framework, and cutting-edge health infrastructure. This detailed environment overview guides IoT use in healthcare, whether for intelligent hospitals or tailored innovative health systems. The representative study helped me understand the domain's current situation.

General smart health infrastructure's top priority is data protection, and user authentication suggests a new hardware-based IoT security approach. The LEAIoT encryption/decryption algorithm gives the lightweight-based security strategy additional key selection options than existing systems. Thus, it may boost speed under network congestion. Compared to a CPU-based version, the hardware-based LEAIoT implementation is 99.9 per cent quicker at key generation and 96.2 per cent faster at encryption/decryption for 1000 kilobits. Compared to the lightweight cyphers AES, SNOW 3G, and ZUC, it utilises 89.2%, 64.2%, and 13.4% less hardware in identical hardware devices. Even the tiniest devices can implement this architecture and be protected, making it useful in an IoT-based multi-sensor ecosystem. Finally, its limited throughput and frequency reflect IoT devices' resource constraints. It is suitable for resource-efficient and fast critical generation applications. It also meets the IoT-based innovative health framework's primary security and performance criteria, yielding novel outcomes and improvements.

7 References:

1. Aivaliotis V, Tsantikidou K, Sklavos N. IoT-Based Multi-Sensor Healthcare Architectures and a Lightweight-Based Privacy Scheme. Sensors (Basel). 2022 Jun 3;22(11):4269. doi: 10.3390/s22114269. PMID: 35684890; PMCID: PMC9185436.
2. Nasiri S, Sadoughi F, Tadayon MH, Dehnad A. Security Requirements of Internet of Things-Based Healthcare System: a Survey Study. Acta Inform Med. 2019 Dec;27(4):253-258. doi: 10.5455/aim.2019.27.253-258. PMID: 32055092; PMCID: PMC7004290.
3. Adil O. Khadidos, S. Shitharth, Alaa O. Khadidos, K. Sangeetha, Khaled H. Alyoubi, "Healthcare Data Security Using IoT Sensors Based on Random Hashing Mechanism", *Journal of Sensors*, vol. 2022, Article ID 8457116, 17 pages, 2022. https://doi.org/10.1155/2022/8457116
4. A. Srilakshmi, P. Mohanapriya, D. Harini and K. Geetha, "IoT based Smart Health Care System to Prevent Security Attacks in SDN," *2019 Fifth International Conference on Electrical Energy Systems (ICEES)*, 2019, pp. 1-7, doi: 10.1109/ICEES.2019.8719236

5. Oks, S.J., Jalowski, M., Lechner, M. *et al.* Cyber-Physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook. *Inf Syst Front* (2022). https://doi.org/10.1007/s10796-022-10252-x
6. Dewangan, Kiran & Mishra, Mina. (2018). A Review: Security of IOT Based Healthcare System. 3.
7. Bhardwaj, V., Joshi, R. & Gaur, A.M. IoT-Based Smart Health Monitoring System for COVID-19. *SN COMPUT. SCI.* **3**, 137 (2022). https://doi.org/10.1007/s42979-022-01015-1
8. K. Yadav, A. Alharbi, A. Jain and R. A. Ramadan, "An iot based secure patient health monitoring system," *Computers, Materials & Continua,* vol. 70, no.2, pp. 3637–3652, 2022.
9. Hymavathi, J., Kumar, T. R., Kavitha, S., Deepa, D., Lalar, S., & Karunakaran, P. (2022). Machine Learning: Supervised Algorithms to Determine the Defect in High-Precision Foundry Operation. *Journal of Nanomaterials*, *2022*.
10. *Ambarkar, Smita Sanjay and Narendra M. Shekokar. "Toward Smart and Secure IoT Based Healthcare System." (2020).*
11. Junho Choi, Chang Choi, SungHwan Kim, and Hoon Ko. 2019. Medical Information Protection Frameworks for Smart Healthcare based on IoT. In Proceedings of the 9th International Conference on Web Intelligence, Mining and Semantics (WIMS2019). Association for Computing Machinery, New York, NY, USA, Article 29, 1–5. https://doi.org/10.1145/3326467.3326496
12. M N Mohammed et al 2020 J. Phys.: Conf. Ser. 1450 012079
13. P. Bayari, A. Lakshman, G. Bhatnagar and C. Chattopadhyay, "A Novel Security Framework for Medical Data in IoT Ecosystems" in IEEE MultiMedia, vol. 29, no. 02, pp. 34-44, 2022.
    doi: 10.1109/MMUL.2022.3157770
14. J.-J. Wang and R. Payne, "A survey of Internet of Things in Healthcare", *EAI Endorsed Trans IoT*, vol. 7, no. 27, pp. 1–11, Mar. 2022.
15. Mamo, Kedir & Subah, Zareen & Ali, Mohammed. (2020). IoT Sensor Initiated Healthcare Data Security. IEEE Sensors Journal. PP. 1-1. 10.1109/JSEN.2020.3013634.
16. Saha, Goutam & Kumar, Sandeep. (2017). Security Issues in IoT-Based Healthcare. International Journal of Applied Research on Information Technology and Computing. 8. 385. 10.5958/0975-8089.2017.00036.7.
17. Yang Yang, Xianghan Zheng, Wenzhong Guo, Ximeng Liu, Victor Chang,Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system, Information Sciences, Volume 479,2019, Pages 567-592, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2018.02.005.
18. R. Nidhya; Manish Kumar; R. Maheswar; D. Pavithra, "Security and Privacy Issues in Smart Healthcare System Using Internet of Things," in *IoT-enabled Smart Healthcare Systems, Services and Applications* , Wiley, 2022, pp.63-85, doi: 10.1002/9781119816829.ch4
19. *Ambarkar, Smita Sanjay and Narendra M. Shekokar. "Toward Smart and Secure IoT Based Healthcare System." (2020).*
20. Santos, B. J., Tabacow, R. P., Barboza, M., Leão, T. F., & Bock, E. G. (2022). Cyber Security in Health: Standard Protocols for IoT and Supervisory Control Systems. In I. Management Association (Ed.), *Research Anthology on Securing Medical Systems and Records* (pp. 238-254). IGI Global. https://doi.org/10.4018/978-1-6684-6311-6.ch012