Design of IoT Based Framework for Prediction of Information Security Issues in Health Care

Dr. Rajesh Keshavrao Deshmukh[1], Mohit Shrivastav[2]

[1]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.
[2]Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.

A collection of linked networks made up of intelligent items is known as the Internet of Things. These devices, dubbed "smart sensors," are able to sense their surroundings and easily transfer data and processes between other domains. Many applications that could convince us to live longer and improve the quality of life are made possible by the Internet of Things. The majority are now available on the market. One of the most recent technological breakthroughs in today's world is the Internet of Things (IoT). There has been a lot of promise in recent years to alleviate the burden that an ageing population and rising rates of chronic illness place on healthcare systems. This paper recommended a security issue and their prospects of Internet of Things healthcare systems since there are several obstacles and standard issues preventing growth in IoT healthcare security systems. The suggested effort focuses on assessing security concerns, model, obstacles, and the applicability of the Internet of Things healthcare system. Among the several challenges presented by IoT healthcare include smart sensor computing, smart pills, various security and privacy concerns, and low-power remote device operation.

Keywords: Internet of Things, healthcare, medical environments, sensors, Security, Privacy, Trust.

1. Introduction

Healthcare solutions utilising the Internet of Things (IoT) are a relatively new trend in the present decades. Healthcare systems built on the Internet of Things (IoT) offer a robust foundation for smart sensor technology. The current situation has a large number of IOT devices spread throughout many locations, particularly for intelligence systems [1]. the abundance of information and data available on the market covering a wide range of topics. Massive amounts of data are also released by the IoT-based healthcare system, which is gathered by various sensor networks and devices [3]. These days, there are object and cloud network topologies that facilitate the release of data from IoT-based sensors. The Internet of Things (IoT) is revolutionising healthcare and changing people's lifestyles, but security and privacy remain critical concerns that affect healthcare data [2]. Many concepts and

applications were used by the IoT healthcare security system to operate in this kind of setting. These days, the internet of things is used in every industry, including finance, railroads, healthcare, vehicle management, the auto industry, and smart transportation.

The network of connected smart sensors is known as the Internet of Things. These intelligent sensors are able to sense their surroundings and easily share data and processes across various domains. Many applications that could convince us to live longer and improve the quality of life are made possible by the Internet of Things. The majority are now available on the market. Smart IoT-based sensors are a recent development that span several domains, particularly in smart healthcare systems [12]. The IoT system architecture is responsible for technical, scientific, and industry reasons, including privacy and security, and it plays a crucial part in a logical vision for security reasons [11]. Numerous Internet of Things designs, technologies, and design techniques are designed to address and manage security concerns. Encryption and decryption algorithms are used by IoT security devices, which are monitored and managed by cloud infrastructure and visualization [9]. The internet of things architecture is divided into several layers, each of which uses a separate set of equipment and topologies to preserve sensor data standardisation, security, and privacy. In the IoT healthcare system, numerous middlewares operate in between these layers to coordinate how each person's parameters change.

The rest of the paper is organized as follows: Section 2 provides the classification scheme for the survey; Section 3 provides an overview of proposed architecture. Section 4 provides a summary and comparison of the results of the various papers discussed in this taxonomy. Finally, Section 5 concludes the paper.

2. Related Works

The Internet of Things (IoT) comprises innovative advancements in technology, particularly in the areas of healthcare equipment and patient tracking, maintenance, and sensor-based monitoring. A significant element in the COVID-19 situation and other unobservable disease scenarios is healthcare security [4]. Remote patients and their medications, hospital equipment performance and activity, and patients are all closely monitored by internet-based sensor technology. Real-time and practical solutions to healthcare issues are offered by IoT applications in the healthcare system, preserving patient-doctor relationships. Additionally, these support various healthcare applications, develop the personal healthcare information system, and establish the industrial connection between hospitals and the Internet of Things [6]. Current situation: RFID is intimately tied to hospitals, the medical industry, and its applications. IoT-based devices have numerous uses in the fields of context-based intelligence, cloud computing, fog computing, data mining, and artificial intelligence, among others [5]. In the current day, healthcare is the backbone of numerous organisations, including hospitals, synthetic pharmaceutical laboratories, smart pill design, remote healthcare facilities, biosensor medication and device management, smart treatment delivery, and cumulative decline magnifying. Numerous security and service providers uphold connections with businesses and organisations developing Internet of Things (IoT) artificial intelligence systems. The artificial pharmacy industry, in particular, is looking for a strong security and protective framework for RFID and smart pill design. IOT healthcare requires security for database administration,

payment applications, remote healthcare applications, and personal information. SQL injection, connections between hospitals and industries, and a common control gateway [14].

The primary goal is to describe the capabilities, usability, and security aspects of medical sensors. These sensors are wireless devices that measure vital patient information. The utilisation of healthcare technology and its associated society is increased by IoT-based healthcare systems, which offer a safe, secure, and protective environment. The IOT security architecture is primarily responsible for enhancing healthcare system privacy while maintaining confidentiality. Misuse of information and data was also concentrated on this related effort. The sensitivity of the healthcare care system was impacted by the sensor that had all the data and information reading healthcare and leaking such information.

3. Methodologies

While discussing the security of data in a cloud context, there are two points of contention. First, while data is being transferred into the network from the user site via any web-based application, there may be concerns about data security. Additionally, when data is already travelling over a network and is ready to be stored on a cloud drive, there may be a security risk at the cloud end.

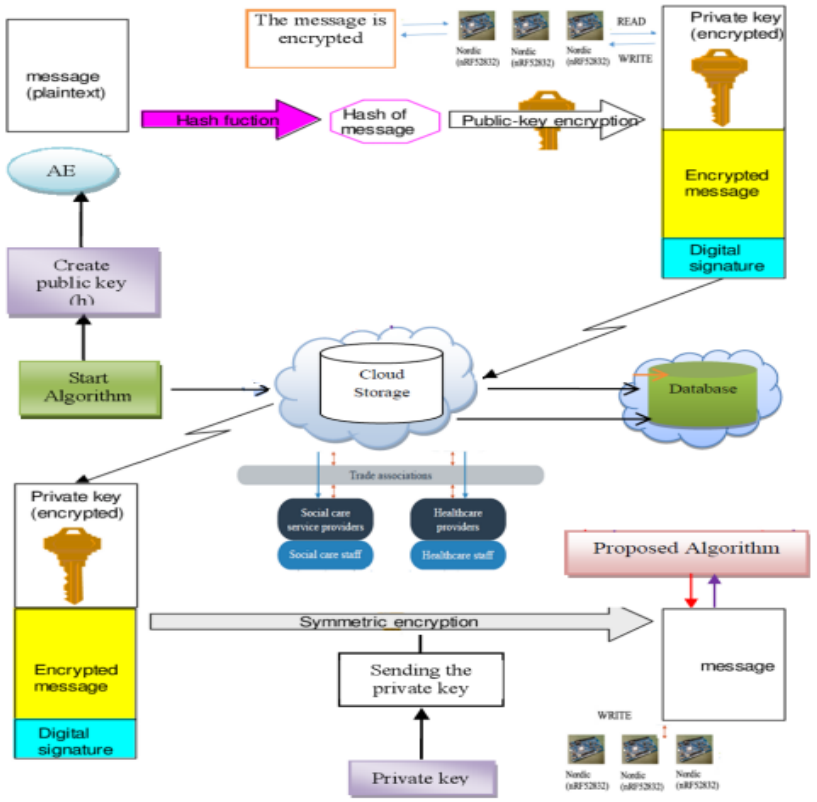

Figure 1: overall block diagram

The primary driver behind the suggested work is the second be concerned, which is the security of the data file while it is being saved on a cloud disc at the cloud end. Researchers have provided the following outline of a hybrid task that consists of three stages in order to maintain security at cloud storage [7].

First-phase ciphering techniques have been created that provide more precise key while also providing a preliminary level of security. The newly devised encryption method used in the second stage of the predicted effort arrangement is based on Last but not least, it is evident that cryptographic encryption techniques are significant when discussing data security, but it is also crucial to confirm the authentication rights of each user attempting to access the data stored on the cloud disc. User authentication or verification while accessing cloud data is crucial for improving security [8]. In order to prevent unauthorised users from accessing the IoT-based cloud environment, security measures are implemented in the third phase of the cloud environment. that raises the healthcare system's utilisation factor. As a result, this method generates a feature linked to the encrypted text, and user authentication is managed based on this characteristic. The key component of the proposed method allows the creative looks to determine the introduction as groups above GRQ. It also supplies such appearances. By doing this, it is possible to prevent more collisions with the already-collided requests that are pending in the queue [13].

The technique of obtaining the fused image in the proposed work involves inversely modifying an artificial wavelet transform array that associates information from the two input images. The proposed algorithm's primary goal is to be successful and allow the new appearance to determine the foreword from the cluster that is larger than the GRQ. By doing this, the current collided requests that are waiting in the queue are helped to avoid any more collisions. Furthermore, the approach that helps the MDs select the appropriate effective cluster and can be applied to reduce the chance of collision [10]. The access rate and access delay are mutually improved as well as resolved by this. In this case, the sender encrypts the message using the recipient's public key, and the recipient decrypts it using its private key.

4. Results and Discussion

In addition to some other conventional techniques, this section includes information on the tools utilised in the implementation of the suggested methodology. Our job is performed more quickly and reliably thanks to the usage of the Nordic nRF52832 in an Intel I3 800X4 core processor with 4GB of primary memory and the Raspberry Pi3 Model B+, SoC enabled SBC.

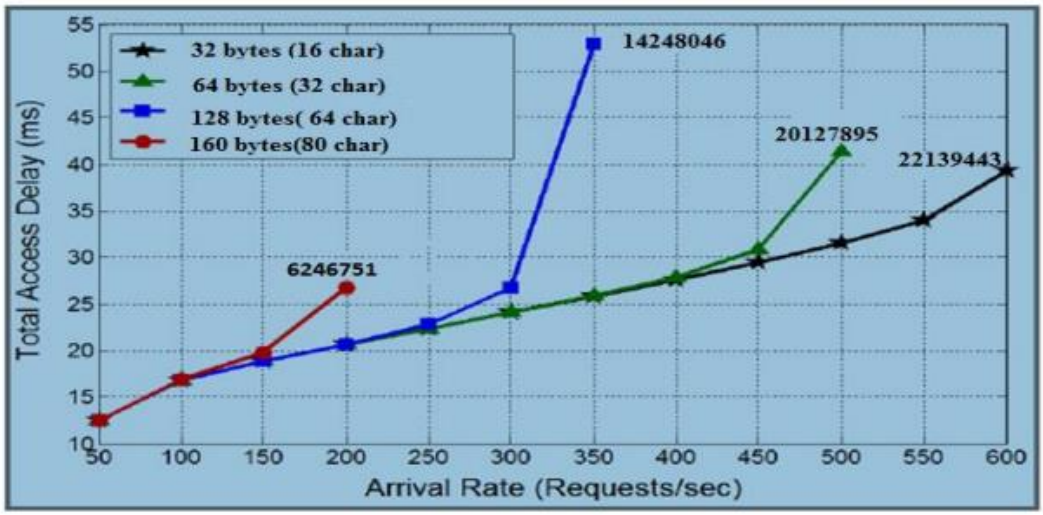

Figure 2: Security encryption comparison diagram

However, we saw that the primary goal of our models is to protect the network from the adversary, and this is given more attention than specific nodes. We presume that a node is trustworthy if it is connected to the network, confirms its legitimacy, and registers with the network.

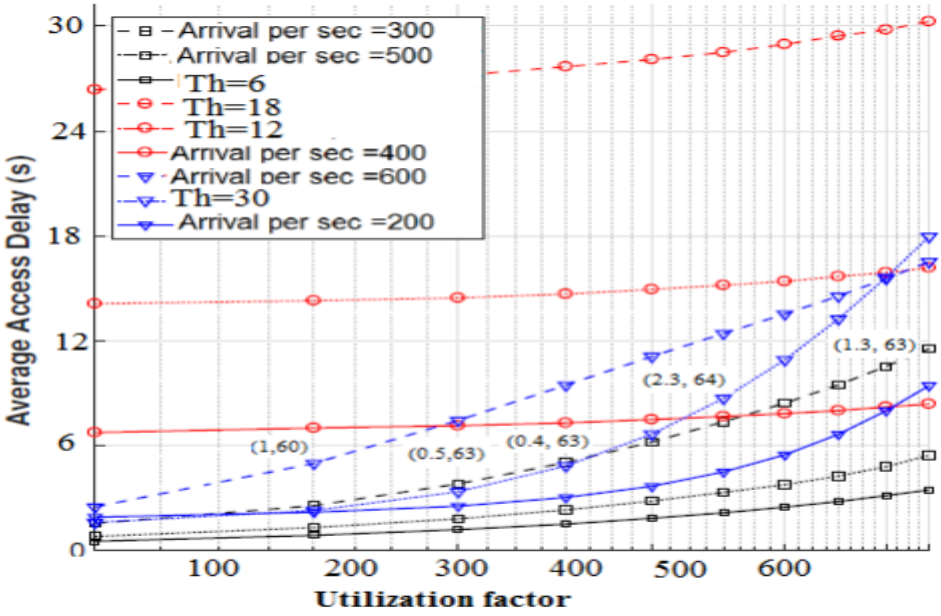

Figure 3 Frame Utilization factor and actual delay comparison diagram

The experimental development is centred on real data. Small changes can spread quickly

during algorithm rounds according to the Bytes or Char requirements of avalanche effect, meaning that before the algorithm runs out, every chunk of the output should rely on every chunk of the input. Ultimately, research may indicate that under really high load, i.e., when our procedure demonstrates a performance level that ranges from comparable to noticeably superior. Here, we want to underline that, in order to attain a performance level comparable to ours, nearly flawless coordination between all parameters must be determined in accordance with a particular load.

5. Conclusions

Cloud computing is a current concept that explains how information specialists employ resources and functions for both controlling and utilitarian purposes. However, the revolution never ends and continually faces new challenges. Research on cloud data security or protection at the cloud end was presented. An algorithmic design is suggested and put into practice with a notion to provide data security or protection of cloud data storage at the cloud end or to improve cloud security. The experiment results that are shown demonstrate the reasonableness of the suggested concept, which improves security and execution time efficiency while maintaining cloud data confidentiality. The concept of the suggested technique, which includes several system encryption schemes based on different kinds of keys and suggested encryption algorithms, is explored in this research effort. The suggested method offers a framework for text information confidentiality in cloud storage environments, which is necessary for data storage at the cloud end and can be helpful in a variety of applications. The suggested method has the advantages of simplicity and confidentiality. According to the security study, the suggested method, which is predicated on the "proposed algorithm," is strengthened by the avalanche effect that is created. Subsequent research endeavours may showcase an improvement of the suggested algorithm, emphasising its capacity to generate keys at random throughout the key exchange procedure. Additionally, the proposed algorithm's file sharing functionalities may be improved.

References

1. Veeramakali, T., R. Siva, B. Sivakumar, P. C. Senthil Mahesh, and N. Krishnaraj. "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model." The Journal of Supercomputing 77, no. 9 (2021): 9576-9596.
2. Chakraborty, Sabyasachi, Satyabrata Aich, and Hee-Cheol Kim. "A secure healthcare system design framework using blockchain technology." In 2019 21st international conference on advanced communication technology (ICACT), pp. 260-264. IEEE, 2019.
3. Praveen Kumar Singh, Sourav Tribedi, and Manoj Kumar. 2022. FABRICATION AND EVALUATION OF CETRIZINE HYDROCHLORIDE SUPPOSITORIES. International Journal of Pharmacy Research & Technology, 12 (1), 58-66. doi:10.31838/ijprt/12.01.06
4. S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

5. Awotunde, Joseph Bamidele, Rasheed Gbenga Jimoh, Sakinat Oluwabukonla Folorunso, Emmanuel Abidemi Adeniyi, Kazeem Moses Abiodun, and Oluwatobi Oluwaseyi Banjo. "Privacy and security concerns in IoT-based healthcare systems." In The fusion of internet of things, artificial intelligence, and cloud computing in health care, pp. 105-134. Cham: Springer International Publishing, 2021.
6. Chaturvedi, Shivi. "Clinical prediction on ml based internet of things for e-health care system." International Journal of Data Informatics and Intelligent Computing 2, no. 3 (2023): 29-37.
7. Stephen, K. V. K., Mathivanan, V., Manalang, A. R., Udinookkaran, P., De Vera, R. P. N., Shaikh, M. T., & Al-Harthy, F. R. A. (2023). IOT-Based Generic Health Monitoring with Cardiac Classification Using Edge Computing. Journal of Internet Services and Information Security, 13(2), 128-145.
8. Gupta, Praveen Kumar, Bodhaswar T. Maharaj, and Reza Malekian. "A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres." Multimedia Tools and Applications 76 (2017): 18489-18512.
9. Verma, Prabal, and Sandeep K. Sood. "Cloud-centric IoT based disease diagnosis healthcare framework." Journal of Parallel and Distributed Computing 116 (2018): 27-38.
10. Mohamed, K.N.R., Nijaguna, G.S., Pushpa, Dayanand, L.N., Naga, R.M., & Zameer, AA. (2024). A Comprehensive Approach to a Hybrid Blockchain Framework for Multimedia Data Processing and Analysis in IoT-Healthcare. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 94-108. https://doi.org/10.58346/JOWUA.2024.I2.007
11. Patra, Ritwik, Manojit Bhattacharya, and Suprabhat Mukherjee. "IoT-based computational frameworks in disease prediction and healthcare management: Strategies, challenges, and potential." IoT in healthcare and ambient assisted living (2021): 17-41.
12. Verma, Prabal, Sandeep K. Sood, and Sheetal Kalra. "Cloud-centric IoT based student healthcare monitoring framework." Journal of Ambient Intelligence and Humanized Computing 9, no. 5 (2018): 1293-1309.
13. Bobir, A.O., Askariy, M., Otabek, Y.Y., Nodir, R.K., Rakhima, A., Zukhra, Z.Y., Sherzod, A.A. (2024). Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity. Natural and Engineering Sciences, 9(1), 72-83.
14. Gupta, Pradeep Kumar, Vipin Tyagi, and Sanjay Kumar Singh. Predictive computing and information security. Singapore: Springer Singapore, 2017.
15. Balakrishnan, Lalithadevi. "An Internet of Things (IoT) based intelligent framework for healthcare–a survey." In 2021 3rd International Conference on Signal Processing and Communication (ICPSC), pp. 243-251. IEEE, 2021.