International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 3s,2025
https://theaspd.com/index.php

Secure Iot Communication Protocols For Healthcare

Manish Nandy[1], Prachi Gurudiwan[2], Parveen Kaur[3]
[1]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.
ku.manishnandy@kalingauniversity.ac.in, 0009-0003-7578-3505
[2]Assistant Professor, Department of Pharmacy, Kalinga University, Raipur, India.
ku.prachigurudiwan@kalingauniversity.ac.in, 0009-0008-0150-5250
[3]Assistant Professor, New Delhi Institute of Management, New Delhi, India., E-mail: parveen.kaur@ndimdelhi.org, https://orcid.org/0000-0002-5750-7115

Abstract
The main concept of the Internet of Things is to equip the network infrastructure with software and interoperable communication protocols for improved data collecting with an appropriate connection and information sharing between nodes on several heterogeneous networks. IoT applications include smart grid, pollution monitoring, healthcare, and home automation systems for smart lighting. Inappropriately, a large number of devices connected to the Internet increase the likelihood of cybercrime. The Internet of Things device gathers patient cardiac data both before and after a heart issue occurs. When patient health indicators can be remotely tracked in real time, saved, and then communicated to a data center, such as the cloud, the effectiveness, affordability, and accessibility of healthcare systems are all greatly improved. A heart illness detection model (ICA) has been built using a modified version of the Imperialist Competitive Algorithm, a competitive algorithm from the Imperialist series. Due to inadequate network segmentation, devices that are directly exposed to the internet have created a backdoor that allows hackers to enter. To safeguard IoT networks and devices, researchers and marketers are working on a wide range of solutions. Rather, a lot of work needs to be done before the standards are set.
Keywords: *IOT, Heart Disease, Medical Images, Sensor,*

I INTRODUCTION

In the current wireless communication era, the Internet of Things (IoT) is experiencing an exceptional uptick. IoT refers to items (i.e., objects) that are connected to the Internet in order to provide and retrieve real-time data. An Internet of Things (IoT) device can be smart or any electronic device, from wearable to hardware, with a wide range of applications in industries, transportation, health care, smart homes, etc [9]. They continue to sense the information persistently and then send it to dedicated servers where the necessary processing and analysis is done as and when needed for monitoring and control purposes [2][8]. Examples of these smart appliances include smart TVs in smart homes, smart devices in patients' bodies like brain neurostimulators, smart cars and smart traffic management appliances, and smart appliances in industries to monitor the industries and environment, etc[6]. The improvement of the current Internet services is known as the Internet of Things. Associating everything is necessary to obligate every single item that is currently in the IoT network or is likely to be in the future. It's intriguing to consider connecting all of that at any time [11]. Currently, billions of devices are linked to the Internet of Things for a variety of vertical applications, such as the medical field. [3].

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 3s,2025
https://theaspd.com/index.php

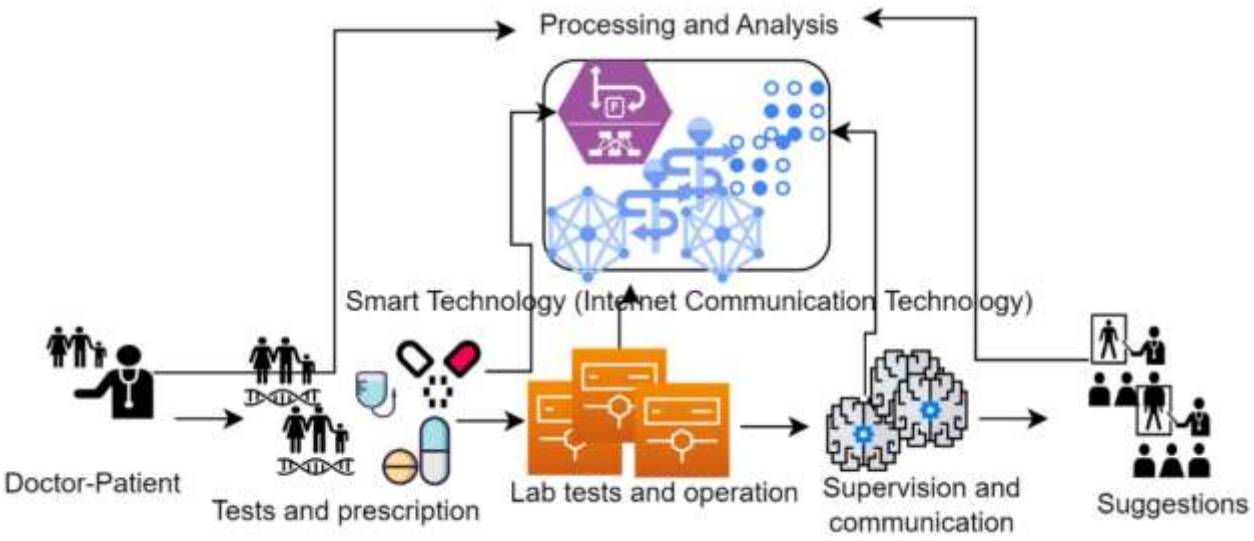

Figure 1: IoT communication

III PROPOSED METHOD

3.1 IMPERIALIST COMPETITIVE ALGORITHM (MICA) MODEL

Authentication, confidentiality, availability, integrity, and other aspects of smart healthcare devices and sensitive patient-centric data sharing via a network are among the most important security and privacy needs in the healthcare industry[10]. Non-repudiation, freshness, forward and backward secrecy, and many more criteria are examples of additional security needs. In order to safeguard the continuous communication that takes place in the IoMT communication environment, research has been conducted for years to design and build efficient and effective security procedures and protocols [13]. These security methods are resistant to a number of possible attacks because of their many features [4].

Robots, humans, and even other IoT devices can make intelligent decisions thanks to the analysis of the Internet of Things device. The Modified Imperialist Competitive Algorithm (MICA) is used to choose characteristics for the diagnosis of heart disease. The goal of this study is to identify the best characteristics to employ in order to improve the diagnosis of heart disease while taking into consideration the amount of characteristics that are anticipated to remain constant. It is expected that a similar amount of chosen features are present in various datasets for the tests that were developed. A consistent output that provides the characteristics of cardiac disease with the highest level of diagnostic accuracy will be produced from the responses that are collected. This problem has several early answers, which describe a country as follows:

$$country = [\, P_1, P_2, \ldots \ldots, P_N \; var \;] \quad (2)$$

Typically, it is shown as an array of variables to optimise in N_{var} dimensions. The cost of every nation is inversely correlated with its power. The following defines the cost function f:

$$cost = f\,(country) = f(P_1, P_2, \ldots \ldots, P_N \; var \;) \quad (3)$$

N_{country}\\ initial countries are created in initial by the technique. N_{imp} is the number of empires built by the most powerful nations. N_{col}\\ stands for the nations that were founded as colonies and stayed on the left side of the empires. The method will be completed after the maximum number of decades or a predetermined number of repetitions [5-7].

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 3s,2025
https://theaspd.com/index.php

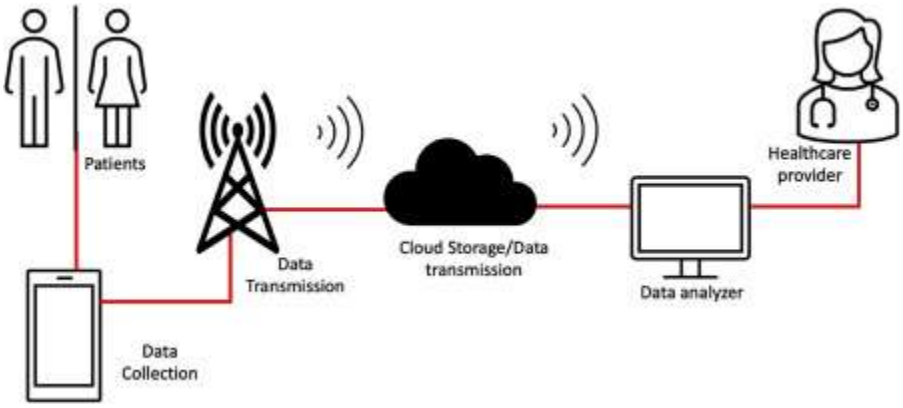

Figure 2: Proposed architecture

Initially, N_{country\ } initial nations are established. A number of empires are constructed using the most powerful nations, N imp. The designations N_{imp} and N_{col} refer to the colonies of the other empires. The procedure will completely stop after a certain number of repetitions, or the maximum number of decades. The idea behind a collection of processes known as "ISABA" is that each set of attributes being categorized is unique from each other. On the basis of relevant diagnostic information, first-order premise logical structures for the diagnosis of this cardiac ailment can be created.

IV EXPERIMENTAL RESULTS

An IOT device was used to retrieve the "Heart Disease Dataset" from the UCI Machine Learning Repository, which was used in the study [14]. This study uses data sets from a California University data source to diagnose Cleveland heart disease. Heart illness can present with a wide range of symptoms [12]. It was once known as "coronary angiography" (NUM) and has 74 distinct characteristics. NUM supplied information about a patient's cardiac health. The methods shown in Figure 2 are used to evaluate the effectiveness of the suggested smart heart disease prediction system.

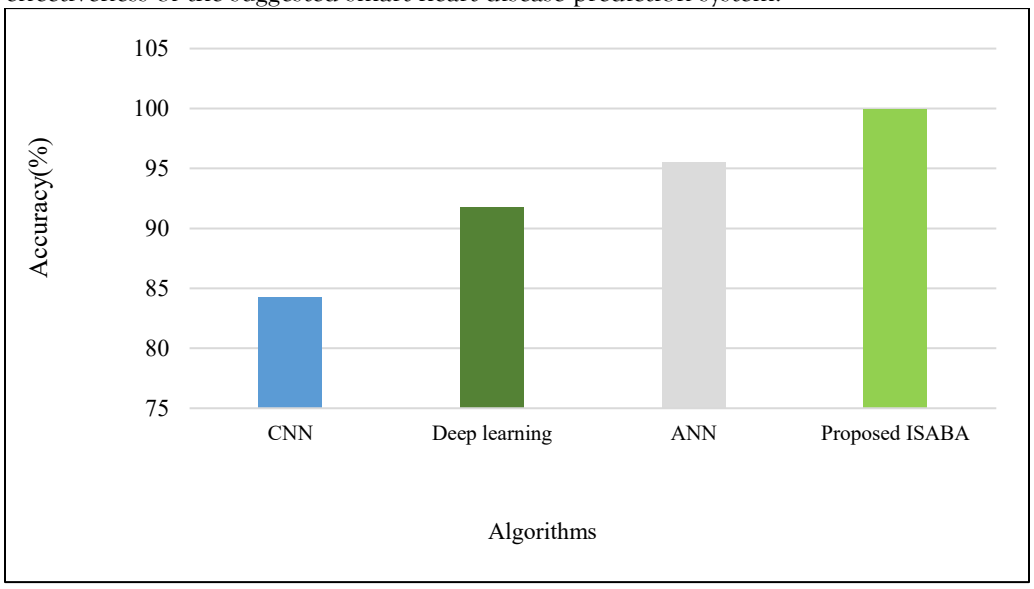

Figure 2: Accuracy

The Improved Self-Adaptive Bayesian Algorithm (ISABA) performs better than previous algorithms in terms of prediction rate and accuracy, especially in Internet of Things-based applications. It maintains its advantage throughout a variety of learning percentages.

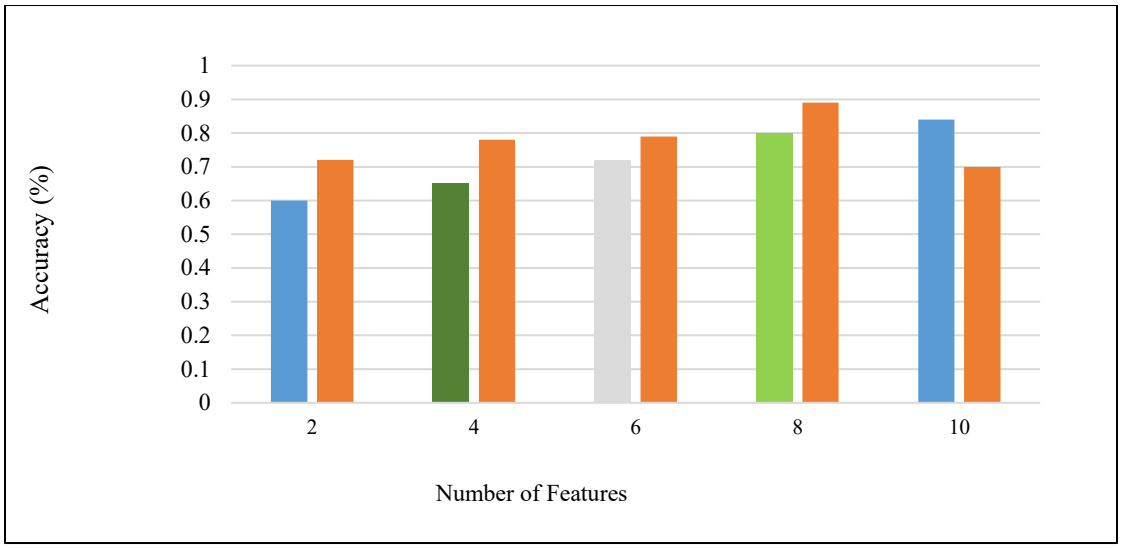

Figure 3: Comparison of the diagnostic accuracy using a variety of indicated methods' attributes

The technique's feature selection capabilities aid in the correct diagnosis and prediction of heart disease by lowering the need for invasive procedures such as coronary angiography, as well as unnecessary testing and costs (Figure 3). Laboratory testing, cardiac eco, electrocardiogram (ECG), physical examination, and demographics are the four areas into which the variables are separated..

CONCLUSION

This paper's goal was to present a novel and ingenious approach to healthcare delivery through the Internet of Things. The risk of identity theft and data breaches increases with the number of personal data devices. Any technical issues with the system will result in significant financial and/or physical harm to both individuals and businesses if people grow overly dependent on this new automation and technology. Additionally, it heightens worries about cyberwarfare. As a result, it has drawn a lot of interest from scholars and academics worldwide. Security continues to be one of the most important problems that impede the development of IoT, despite the fact that its deployment breadth has garnered widespread attention. Ensuring the safety of devices, networks, data, operating systems, and servers that are integrated under the IoT's fabric is the focus of IoT security. It is difficult to ensure the security of the personal data gathered by Internet of Things devices, given the billions of devices connected to the network. Security breaches are nearly inevitable, therefore having an exit strategy in place to protect as much data as possible in the event of an attack is imperative.

REFERENCES

[1] Ahmad, Arshad, Ayaz Ullah, Chong Feng, Muzammil Khan, Shahzad Ashraf, Muhammad Adnan, Shah Nazir, and Habib Ullah Khan. "Towards an Improved Energy Efficient and End-to-End Secure Protocol for IoT Healthcare Applications." Security and Communication Networks 2020, no. 1 (2020): 8867792.

[2] Melgat, B. M. (2024). Fuzzy Nbhd System in Fuzzy Top-R-Module. International Academic Journal of Science and Engineering, 11(1), 15–18. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1103

[3] Elhoseny, Mohamed, Gustavo Ramírez-González, Osama M. Abu-Elnasr, Shihab A. Shawkat, N. Arunkumar, and Ahmed Farouk. "Secure medical data transmission model for IoT-based healthcare systems." Ieee Access 6 (2018): 20596-20608.

[4] Bhattacharya, R., & Kapoor, T. (2024). Advancements in Power Electronics for Sustainable Energy Systems: A Study in the Periodic Series of Multidisciplinary Engineering. In Smart Grid Integration (pp. 19-25). Periodic Series in Multidisciplinary Studies.

[5] Sharma, B.; Hashmi, A.; Gupta, C.; Khalaf, O.I.; Abdulsahib, G.M.; Itani, M.M. Hybrid Sparrow Clustered (HSC) Algorithm for Top-N Recommendation System. Symmetry 2022, 14, 793. [Google Scholar] [CrossRef]

[6] Thirunavukkarasu, T. C., Thanuskodi, S., & Suresh, N. (2024). Trends and Patterns in Collaborative Authorship: Insights into Advancing Seed Technology Research. Indian Journal of Information Sources and Services, 14(1), 71–77.

https://doi.org/10.51983/ijiss-2024.14.1.4004
[7] Raju, K.B.; Dara, S.; Vidyarthi, A.; Gupta, V.M.; Khan, B. Smart Heart Disease Prediction System with IoT and Fog Computing Sectors Enabled by Cascaded Deep Learning Model. Comput. Intell. Neurosci. 2022, 2022, 1070697. [Google Scholar] [CrossRef]
[8] Ravshanova, A., Akramova, F., Saparov, K., Yorkulov, J., Akbarova, M., & Azimov, D. (2024). Ecological-Faunistic Analysis of Helminthes of Waterbirds of the Aidar-Arnasay System of Lakes in Uzbekistan. Natural and Engineering Sciences, 9(1), 10-25. https://doi.org/10.28978/nesciences.1471270
[9] Refaee, Eshrag, Shabana Parveen, Khan Mohamed Jarina Begum, Fatima Parveen, M. Chithik Raja, Shashi Kant Gupta, and Santhosh Krishnan. "Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications." Wireless Communications and Mobile Computing 2022, no. 1 (2022): 5665408.
[10] Salem, M.B., & Stolfo, S.J. (2010). Detecting Masqueraders: A Comparison of One-Class Bag-of-Words User Behavior Modeling Techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, 1(1), 3-13.
[11] Sonawane, R.; Patil, H.D. Prediction of Heart Disease by Optimized Distance and Density-Based Clustering. In Proceedings of the 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 23–25 February 2022; pp. 1001–1008. [Google Scholar]
[12] Kao, Y. C., Liu, J. C., Wang, Y. H., Chu, Y. H., Tsai, S. C., & Lin, Y. B. (2019). Automatic Blocking Mechanism for Information Security with SDN. Journal of Internet Services and Information Security, 9(1), 60-73.
[13] Bhuiyan, Mohammad Nuruzzaman, Md Mahbubur Rahman, Md Masum Billah, and Dipanita Saha. "Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities." IEEE Internet of Things Journal 8, no. 13 (2021): 10474-10498.
[14] Kishor, A., & Chakraborty, C. (2021). Artificial Intelligence and Internet of Things Based Healthcare 4.0 Monitoring System. Wireless Personal Communications. doi:10.1007/s11277-021-08708-5