Securing the Future of Fog based IoT Healthcare: A Framework Informed by Large-Scale Network Analysis for Suspicious Traffic Detection

Md. Iftekhar Hossain Turja, Khalid Redwan Sun, Sheikh Sadi Emon, Marium Malek,
Md Humaion Kabir Mehedi, Farah Binta Haque, Annajiat Alim Rasel
Dept. Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
{iftekhar.hossain.turja, khalid.redwan.sun, sheikh.sadi.emon, marium.malek,
humaion.kabir.mehedi, farah.binta.haque}@g.bracu.ac.bd
annajiat@gmail.com

***Abstract*—The extensive application of Internet of Things (IoT) in the modern healthcare system, has brought out a massive change in healthcare infrastructure. Though the escalating growth of IoT in this sector has upgraded our healthcare functionality to the next level, it is also concurrently raising the security concerns. Conventional Network Security Solutions has reached its limitation competing against the new age technology since the conventional network security approach has limited resources to operate simultaneously through distinct IoT protocols. Recent Cyber threats expose the healthcare IoT vulnerabilities which indicates the necessity of cutting age tools and approaches to ensure adequate security measures.**

Conventional Security approaches are inadequate in terms of dealing with unique problems that arise by modern IoT protocols and devices . To compete with those discrepancies, we have introduced a fruitful security architecture which is specially built for context-aware security solutions as well as customized for IoT applications. This framework interconnects the cutting edge open source technology, IoT-Flock which facilitates realistic use-case scenario generation distinguishing both malicious and normal devices. It turns collected traffic into an IoT dataset with a utility. We used machine learning to detect and stop cyberattacks on healthcare systems using an IoT healthcare dataset including normal and attacking traffic.

This research proposes machine learning procedure, also detects abnormalities and threat assaults to categorise beyond theoretical issues. Along with security measures and IoT-Flock using open-source technology, data authenticity is guaranteed.Besides, this IoT security architecture overcomes conventional security solutions' limitations, improving patient safety. Our aim is to implement proactive security solutions that will strengthen IoT healthcare over time via thorough evaluation of networks.

***Index Terms*—Internet of Things (IoT), Fog,computing Healthcare, Security, Machine Learning**

I. Introduction

The Internet of Things (IoT) seamlessly integrates with the device and is simultaneously involved with transmitting the sensitive medical data . Though this interconnectedness impressively offers faster data transmission, the data security issues can not be avoided [1, 2]. Cyber Attackers can exploit resource-constrained Internet of Things devices because traditional security solutions cannot handle them [3]. This study presents a framework to address these concerns and delivers context-aware healthcare IoT security solutions.

The usage of IoT devices will reach 75.44 billion globally by 2025 and the healthcare sector is also included to dive into this massive growth. Those devices are mostly responsible for playing a critical role to immaculate continuous remote monitoring of the patient along with the crucial data transmission of the entire health care system. No matter how seamless it is, there are always bugs inside the system application . Those bugs are the main doors for the cyber criminals and they crack down the network system by erasing or stealing the important data and their steadily attacking activities on the healthcare systems causes data breaches and interruptions, which eventually harm patients' and healthcare systems' data privacy.

Traditional means of protection like firewalls and intrusion detection systems are meant to be used in stable wireless networks and often fail to adapt to rapidly changing parameters of IoT environments. Security applications that are resource-intensive usually fail to execute where these solutions have minimal processing capacity and memory. There are also multiple communication protocols used for IoT devices which make it difficult for common security solutions. Therefore, traditional approaches often fail to shield healthcare IoT systems against advanced hacks.

It is necessary to embrace a creative and distinct approach to efficiently tackle the security threats for that particular system. Therefore, the system would help monitor network traffic patterns and identify such things as unusual data transfers or attempted intrusions which will be needed because we are interested not only in cyber criminals detection but also prevention.

The study advances a contemporary framework for fabricating conscious security measures for IoT devices within the

healthcare sector. This architecture uses IoT-Flock, an open source approach, to generate authentic datasets consisting of ordinary and malicious communication patterns. After this, the information can be used to train machine learning systems for identification of anomaly trends indicative of cyber attack.

A number of key points on healthcare IoT security are presented in this article. First of all, the proposed framework can be of great importance in helping researchers and developers to develop, as well as to evaluate, healthcare specialized context-sensitive security mechanisms. Secondly, the fact that IoT-Flock open source technology promotes cooperation along with contributing to robust and widely accessible security measures. Thirdly , for strengthening safety and improving cybersecurity of healthcare IoT, this paper proposes a set of preventive measures against cyber attacks and a scheme for resilience. And finally , the end result is an improvement in the quality of patient care and outcomes.

Despite the fact that previous works have considered various approaches to securing IoT devices, only few have been dedicated to the health care sector. Thus, this study is focused on proposing a customized solution that addresses specific security issues and considerations inherent within healthcare IoT scenarios. Additionally, the research differs from other available solutions in respect to IoT-Flock being an open source tool that is not a privately owned tool, can be used together with authentic data sets.

II. Literature Review

The usage of Internet of Things (IoT) devices has been rapidly increasing in the field digital healthcare monitoring systems has significantly increased data collection and processing capabilities. Many new use cases for Fog based healthcare have been discovered. According to [4], "The use of a Fuzzy-assisted Machine Learning Framework (F-AMLF) in conjunction with fog computing is a promising idea for improving the efficacy of health monitoring". When compared to conventional methods, the framework used in [4] shows notable improvements in accuracy, prediction ratio, and energy efficiency. This emphasizes the potential of advanced machine learning and fog computing for robust health-care systems. Another study done in [5] introduces an all-encompassing computing framework that combines edge, fog, and cloud computing to address the challenges posed by high response times in cloud-based e-health systems. This study emphasizes the significance of real-time smart health care domains, providing recommendations for optimal network infrastructure deployment [5]. Building upon the previous study, [6] puts emphasis on Quality of Service (QoS) in healthcare, that has led to the integration of IoT and fog computing. These new approach has displayed many positive outcomes, among which includes better data accuracy, decision-making speed, and real-time monitoring. As stated in [6], "Through the utilization of fog computing, an integrated hardware solution developed for EHS safety and utilizing IoT successfully mitigates transmission and processing delays. This method has the potential to improve the overall dependability of health-care systems."

In [7] a Hybrid-Fog-Computing (HFC) system, incorporating deep learning, GIS tools, and spatial cluster analysis, is proposed in the context of addressing Acute Encephalitis Syndrome (AES). As stated in [7], "The HFC system performs better than other similar models and excels in real-time alert generation and disease monitoring in terms of accuracy and stability." [7] highlights the potential of hybrid fog computing solutions for critical disease monitoring applications. Even other animals have also benefited from this technology as seen in another study done in [8], "It is seen that beyond human health, the Smart VetCare system for domestic pet health monitoring utilizes Internet of Medical Things (IoMT) technology and a FogBus platform." The research reported in [8] also showed excellent clarity, dependability, and the f-value for actual time animal health care analysis, indicating the practical application of fog computing across multiple health care scenarios. Fog computing also has application in reducing the time required for the data to travel between the cloud and the end device in the case of monitoring vital patient data, particularly cardiac arrhythmia [9]. According to the study [9], "Using an Arduino board, an AD8232 sensor module, and the K-Nearest Neighbor (KNN) algorithm, the system used in this study provides effective diagnosis." In summary, this study tries to demonstrate the underlying potential for further improvement in the field of Fog computing and its respnose time in healthcare scenarios. Fog based healthcare is also seen in another paper [10], "Being used for senior citizen health monitoring, a mobile health monitoring model utilizing fog computing is introduced, significantly reducing delay and power consumption." In another research, efficient disease management, particularly in the context of gliomas, is addressed through a machine learning ensemble with the added integration of edge-fog computing with it [11]. The framework proposed in [11], "It shows effectiveness in terms of power consumption, latency, accuracy, and execution time, showcasing the potential for tailored solutions in disease-specific contexts." In another study [12], a home hospitalization system is proposed, which also leverages the synergies of IoT, Fog computing, and Cloud computing. According to [12], "This system monitors patient health and environmental conditions, providing real-time healthcare services." The positive acceptance from both patients and doctors testifies to the practicality of such integrated healthcare solutions. The paper in [13] expands beyond individual healthcare systems, and shows that fog computing and IoT are also recognized for their contributions to the development of smart cities. The architecture proposed in [13] enhances urban operation efficiency through intelligent perceptions and information processing, emphasizing the broader societal impact of these technologies. Continuing the exploration of smart cities, potential applications of fog computing are examined, emphasizing caching techniques, UAVs, and AI/ML in IoT environments [14]. This comprehensive analysis considers both challenges and prospects, contributing to the understanding of the evolving landscape of smart cities. In healthcare applications, the integration of Edge, Fog, and Cloud infrastructures is deemed essential

for supporting latency-sensitive IoT applications [15]. The FogBus framework proposed in this study addresses platform independence, security, and resource management challenges, providing a comprehensive solution for end-to-end integration [16]. In [17], "Global challenges like COVID-19 are addressed through the proposal of MIC-Net, a federated deep learning approach for efficient multi-institutional COVID-19 segmentation." This approach addresses learning drift and inter-site heterogeneity, demonstrating robust performance in experimental evaluations. Moving towards enhanced security in e-Healthcare systems, [18] states that, "The solution to secure e-Healthcare is an activity monitoring and recognition framework based on multi-class cooperative categorization, leveraging blockchain architecture." The architecture used in [18] delivers more accuracy in human activity identification than prior systems, highlighting the relevance of blockchain in protecting healthcare data. The use of fog in Textile has been seen in another paper, as found in [19], "Innovative approaches in healthcare are also explored through the use of textile electrodes for ECG monitoring in fog computing healthcare." Further working on the the field of Textile and Fog computing, the study done in [19] finds that, "Cotton/nylon fiber coated silver electrodes offers more optimized comfort, signal-to-noise ratio (SNR), and thermal conductivity than traditional methods." This findings showcase the potential for improved wearable healthcare technologies. Again, returning to the field of personal health, [20] introduces a "Fog IoT Cloud-Based Health Monitoring System designed for the elderly and patients integrates physiological signals, enabling contextual monitoring of daily activities." This architecture used in [20] ensures quick access to data and continuous monitoring, even during telematic breaks, underscoring the importance of uninterrupted healthcare services. Cloud web services integration in healthcare is discussed, emphasizing enhanced data accessibility and transformative impacts on healthcare facilities and industry utilization [21]. While acknowledging challenges, [21] highlights the potential benefits of integrating cloud services into healthcare infrastructure. A patient-centric IoT eHealth ecosystem is proposed, advocating for a multi-layered architecture comprising device, fog computing, and cloud layers [22]. The research in [22] also proposes, "Applications such as mobile health, assisted living, and early warning systems are highlighted, addressing challenges in scalability and privacy." Adding to the previous work, the study in [23] also introduces, "Technological advancements in robotic telesurgery integrating 5G, Tactile Internet, and AI are presented, with a focus on a Fog-assisted interactive model to expedite the process." Furthermore, in [23], "There are many challenges in telesurgery, but there is also a huge potential of fog computing to address these complexities in the surgical procedures." Integrating blockchain into a smart healthcare business model, [24] focuses on predicting customer status and providing rewards. The model used in [24] fetches data from the Internet of Medical Things, emphasizing a customer-centric approach to modernize business practices in the healthcare sector. In the security sector, the study in [25] does a comprehensive review and deep analysis in IoT research hotspots such as healthcare, including applications, blockchain, AI, 5G, and data analytics. The study also finds important themes like authentication schemes, fog computing, and cognitive smart healthcare which is contributing to the understanding of evolving trends in healthcare IoT research [25]. To address heart failure, a hierarchical architecture for healthcare systems is proposed, improving response time and scalability [26]. The layered model in [26] facilitates early detection of heart failure, supporting timely intervention and emphasizing the critical role of architecture in life-threatening conditions. Postcloud architectures and the potential of an AI-based self-monitoring home health-care application are explored, discussing challenges, benefits, and disadvantages in the evolving landscape of edge and dew computing [27]. The study done in [27] provides insights into the transformative potential of AI-based applications in home healthcare. The study in [28] proposes a new "The IoT architecture is used for scalable sensor data processing in healthcare, it integrates Meta Fog-Redirection and Grouping and Choosing architecture." The framework demonstrates efficiency in predicting heart diseases, emphasizing key performance parameters and contributing to advancements in predictive healthcare technologies [28]. All things considered, the literature reviewed showcases the diverse applications of fog computing in securing the future of IoT healthcare.

III. Methodology

This study adopts a technique where we use a balance of literature review and also propose our own novel framework. Furthermore, our approach is informed by current research on IoT healthcare security and network analysis. The proposed framework has been designed to adapt to the particular problems of securing IoT health care systems, based on identified gaps and insights from the literature. The software used in our testing collects data from several sources, including simulated and real-world hospital IoT traffic. Large-scale network analysis techniques, such as graph-based models and machine learning algorithms, are then used to detect and classify malicious traffic patterns and separate them from the normal traffic. To give further credibility to our framework, various evaluation metrics like precision and recall are used for a quantitative assessment, comparing our framework against exiting methods. To make the framework even more reliable, an iterative refinement method has also been added where validation and expert feedback data are used to ensure its adaptability and effectiveness in real-world healthcare IoT environments. Utilizing both these approaches, our methodology provides a systematic and evidence-based solution to address the critical issue of securing the future of IoT healthcare.

References

[1] C. Patel and N. Doshi, "Security challenges in IoT cyber world," in *Security in Smart Cities: Models, Applications, and Challenges*, pp. 171–191, Cham: Springer International Publishing, 2019.

[2] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali, "Towards a universal features set for IoT botnet attacks detection," in *2020 IEEE 23rd International Multitopic Conference (INMIC)*, IEEE, 2020.

[3] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020.

[4] M. M. Kamruzzaman, S. Alanazi, M. Alruwaili, I. Alrashdi, Y. Alhwaiti, and N. Alshammari, "Fuzzy-assisted machine learning framework for the fog-computing system in remote healthcare monitoring," *Measurement (Lond.)*, vol. 195, no. 111085, p. 111085, 2022.

[5] Q. Vu Khanh, N. Vi Hoai, A. Dang Van, and Q. Nguyen Minh, "An integrating computing framework based on edge-fog-cloud for internet of healthcare things applications," *Internet of Things*, vol. 23, no. 100907, p. 100907, 2023.

[6] D. Gowda, V, A. Sharma, B. K. Rao, R. Shankar, P. Sarma, A. Chaturvedi, and N. Hussain, "Industrial quality healthcare services using internet of things and fog computing approach," *Measur. Sens.*, vol. 24, no. 100517, p. 100517, 2022.

[7] S. Kumari, M. Bhatia, and G. Stea, "Fog-computing based healthcare framework for predicting encephalitis outbreak," *Big Data Res.*, vol. 29, no. 100330, p. 100330, 2022.

[8] M. Bhatia, "Fog computing-inspired smart home framework for predictive veterinary healthcare," *Microprocess. Microsyst.*, vol. 78, no. 103227, p. 103227, 2020.

[9] E. Moghadas, J. Rezazadeh, and R. Farahbakhsh, "An IoT patient monitoring based on fog computing and data mining: Cardiac arrhythmia usecase," *Internet of Things*, vol. 11, no. 100251, p. 100251, 2020.

[10] P. Deb, A. Mukherjee, and D. De, "Mobile health monitoring for senior citizens using femtolet-based fog network," in *Contemporary Medical Biotechnology Research for Human Health*, pp. 197–204, Elsevier, 2022.

[11] X. Zhu, Y. Zhu, L. Li, S. Pan, M. U. Tariq, and M. A. Jan, "IoHT-enabled gliomas disease management using fog computing computing for sustainable societies," *Sustain. Cities Soc.*, vol. 74, no. 103215, p. 103215, 2021.

[12] H. Ben Hassen, N. Ayari, and B. Hamdi, "A home hospitalization system based on the internet of things, fog computing and cloud computing," *Inform. Med. Unlocked*, vol. 20, no. 100368, p. 100368, 2020.

[13] C. Zhang, "Design and application of fog computing and internet of things service platform for smart city," *Future Gener. Comput. Syst.*, vol. 112, pp. 630–640, 2020.

[14] H. Zahmatkesh and F. Al-Turjman, "Fog computing for sustainable smart cities in the IoT era: Caching techniques and enabling technologies - an overview," *Sustain. Cities Soc.*, vol. 59, no. 102139, p. 102139, 2020.

[15] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "FogBus: A blockchain-based lightweight framework for edge and fog computing," *J. Syst. Softw.*, vol. 154, pp. 22–36, 2019.

[16] T. Aladwani, "Scheduling IoT healthcare tasks in fog computing based on their importance," *Procedia Comput. Sci.*, vol. 163, pp. 560–569, 2019.

[17] W. Ding, M. Abdel-Basset, H. Hawash, and W. Pedrycz, "MIC-Net: A deep network for cross-site segmentation of COVID-19 infection in the fog-assisted IoMT," *Inf. Sci. (Ny)*, vol. 623, pp. 20–39, 2023.

[18] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, "A blockchain-based fog computing framework for activity recognition as an application to e-healthcare services," *Future Gener. Comput. Syst.*, vol. 100, pp. 569–578, 2019.

[19] W. Wu, S. Pirbhulal, A. K. Sangaiah, S. C. Mukhopadhyay, and G. Li, "Optimization of signal quality over comfortability of textile electrodes for ECG monitoring in fog computing based medical applications," *Future Gener. Comput. Syst.*, vol. 86, pp. 515–526, 2018.

[20] O. Debauche, S. Mahmoudi, P. Manneback, and A. Assila, "Fog IoT for health: A new architecture for patients and elderly monitoring," *Procedia Comput. Sci.*, vol. 160, pp. 289–297, 2019.

[21] F. Faridi, H. Sarwar, M. Ahtisham, S. Kumar, and K. Jamal, "Cloud computing approaches in health care," *Mater. Today*, vol. 51, pp. 1217–1223, 2022.

[22] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT ehealth: Promises and challenges of IoT in medicine and healthcare," *Future Gener. Comput. Syst.*, vol. 78, pp. 659–676, 2018.

[23] K. Tiwari, S. Kumar, and R. K. Tiwari, "FOG assisted healthcare architecture for pre-operative support to reduce latency," *Procedia Comput. Sci.*, vol. 167, pp. 1312–1324, 2020.

[24] M. J. Gul, B. Subramanian, A. Paul, and J. Kim, "Blockchain for public health care in smart society," *Microprocess. Microsyst.*, vol. 80, no. 103524, p. 103524, 2021.

[25] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, and M. Iranmanesh, "The internet of things (IoT) in healthcare: Taking stock and moving forward," *Internet of Things*, vol. 22, no. 100721, p. 100721, 2023.

[26] A. Malekian Borujeni, M. Fathy, and N. Mozayani, "A hierarchical, scalable architecture for a real-time monitoring system for an electrocardiography, using context-aware computing," *J. Biomed. Inform.*, vol. 96, no. 103251, p. 103251, 2019.

[27] M. Gusev, "AI cardiologist at the edge," in *Artificial Intelligence and Machine Learning for EDGE Computing*, pp. 469–477, Elsevier, 2022.

[28] G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, R. Sundarasekar, and C. Thota, "A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting system," *Future Gener. Comput. Syst.*, vol. 82, pp. 375–387, 2018.