# A Context-Aware IoT based Fraught Model for COVID-19 Patient Self-Monitoring

Muhammad Jamill[1],Shafiq Hussain[2],Muhammad Farhan[1], Muhammad Rehan Naeem[2]

***Abstract***—For human healthcare, the need for comprehensive systems for healthcare data sharing is ever-expanding. Context-Aware Applications using the Internet of Things have inveigled each industry over the globe. IoT-supported healthcare systems have been developed with efficient gateways that react like a connection between cloud computing and multivarious sensors. This paper addresses the concept of monitoring Covid-19 patients with an IoT-based Context-Aware System. The storage of healthcare systems' massive data on the cloud causes latency issues and creates a lot of trouble during real-time analysis. The introduction of edge computing for real-time analysis can reduce these issues. Our research proposed a fraught model that will monitor and track the patients' health records daily for smart self-treatment. We introduced the concept of context-aware wearable sensors to minimize actuation, transmission, and processing. Our model entails a cluster of internet-enabled wireless sensors, an edge computing layer, a cloud computing layer for syncing edge computing layer data, and end-user layers. We anticipated the secure end-to-end authentication sub-layers in our proposed model for the security and privacy of patients' data .

**Keywords—**Context-Aware Applications, Covid-19, Healthcare, Internet of Things

## INTRODUCTION

Covid-19 is one of the most trending global subjects that influenced worldwide. This novel coronavirus disease created a worldwide health emergency after its extensive spread. According to WHO, there are 283,449,470 confirmed cases and 5,434,338 deaths over time due to this novel coronavirus [1]. Its different variations are spreading on a non-stop basis in all world regions. It is the family of a large group of the same viruses that infect the human body by releasing genes into the body cells. To overcome the spread of COVID-19 and treatment, the doctors suggesting to adopt self-quarantine to all patients have tested positive [2]. So, it is the need of the hour that there should be a self-monitoring system that briefs the patient health reports.

[1]Department of Computer Science COMSATS University Islamabad Sahiwal, Pakistan
[2]Department of Computer Science University of Sahiwal Sahiwal, Pakistan

Email: jamil138.amin@gmail.com

The IoT systems based on context-aware applications can help the patient's daily health. The term "Internet of things" was used for the first time by Kevin Ashton in 1999. It is defined as "Any gadget, electrical or electronics, of any size, connected directly with internet for the sake of information share". The core interest of the IoT is to communicate one device with another physically and connect everything [3]. With the IoT, we can make our daily routines more efficient and convenient while keeping up with our changing priorities and preferences. The IoT appears to be a viable option for keeping pace with the rapid evolution of healthcare systems. The devices with many sensors based on IoT for healthcare systems and projects with the help of a centralized network can keep track of patient records. These records may present in any shape like statistical format, graphical formats, grayscale format, or any other. With the effective utilization of health records, patient treatment can become more effective and faster. By examining the data produced by IoT, a patient can conduct online checkups and get online treatment from any doctor present at the other corner of the world. In this manner, the patient can get a swift recovery by sitting at his home after consulting with a doctor and by the following e-prescriptions.

On the other hand, the hospital can use IoT-based healthcare systems to manage patients' sensitive data and predict diseases. In this way, they can also manage human resources in their smart hospitals because IoT-based healthcare systems are faster than the other systems [4]. The diagnosis of the patient is carried by using these IoT-based intelligent devices. The sensors embedded in the devices can detect early diseases. Diagnosis through sensors is more efficient as compared to the other methods. The authors of [5-7] highlighted this mechanism with several case studies and graphic illustrations. They also proposed several approaches like early disease detection by detecting changes in fingerprint patterns and other mechanisms. The concept of remote monitoring of patients is also emerging these days. Since it helps doctors treat their patients remotely, they can suggest suitable medicine based on electronic prescriptions based on available patient health records. This method also allows the patient to save their travel time and other outside movement activities.
Context-aware systems (CAS) benefit application developers and end-users by collecting context data and syncing systems actions accordingly. Mainly in combination with mobile phones, these systems are of high value and increase usability enormously. In this paper, we presented a standard structure

of CAS and derived a layered design model to explain its cycle activities. CAS can play a vital source in monitoring patients remotely as they provide essential information related to patients' health. The patient data can be passed to the doctor with the help of cloud computing like Amazon Web Service (AWS). The data can be interpreted on the cloud and parsed for visualization purposes in the doctor's mobile application. In this way, a treatment connection can be established between the patient and the doctor. Many researchers worked to form such a bridge in literature, but the major challenge they faced was power consumption, as this process needed more power. The introduction of edge computing can resolve this problem by performing accurate time analysis without latency issues. We introduced this concept and developed a fraught model for Covid-19 patients for monitoring their health at their homes. Our solution is viable from both a technology and business standpoint of view because it not only addresses the desired goals but has extra features like security and privacy of the system with the help of additional authentication layers. These benefits include legitimate access to end-users and secure data sharing.

***Covid-19***

Originating from Wuhan, China, the first patient having Covid-19 was 55 years old, according to South China Morning Post, on November 17, 2019. Later in December, Chinese doctors and other medical staff understood that they were dealing with a novel disease by the end of December [8]. Initially, the spread of this virus was low, but after 2019, the virus created a worldwide health emergency. Figure 1. describes that there will be a massive increase in active cases of this novel disease in 2021.

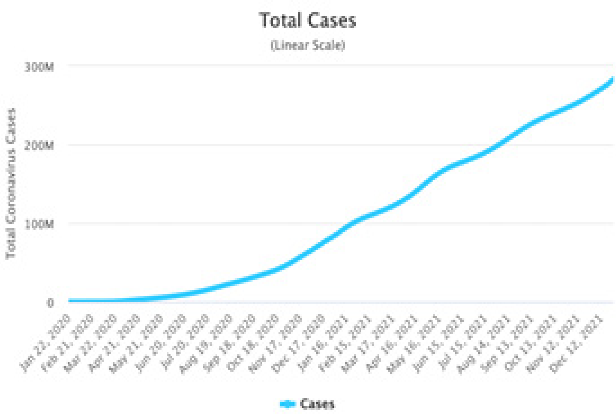


Figure 1. Coronavirus Cases [9]

Despite many conspiracy theories behind Covid-19, it is clear that it is a global health issue at present, and it will remain with us for the long term. However, many countries started the implementation of several Covid-19 vaccines. The University of Oxford/AstraZeneca, Beijing Institute of Biotechnology, and Wuhan Institute of Biological Products are the top developers of Covid Vaccine. The first two developers work on Non-Replicating Viral Vector, while the last works on RNA [10]. The United States Centers for Disease Control and Prevention (CDC) recommends if you are infected with Covid-19, "Stay in touch with your doctor" and "Be sure to get care if you have trouble breathing, or have any other emergency warning signs such as persistent pain or pressure in the chest, new confusion, inability to wake or stay awake, bluish lips or face." Moreover, the Disease Control and Prevention CDC recommends clinical guidelines for the treatment of Covid patients that alerts doctors to the high risk of progression after five days of no improvement in their health. However, these recommendations are not sufficient for proper treatment, and there is a need for hours to develop an intelligent healthcare system for self-monitoring and remote treatment of the Covid patients.

***Authors' Contribution***

This research proposed a Fraught Model to share Covid-19 patient health data using a context-aware IoT-supported intelligent healthcare system. The proposed model is composed of a cluster of internet-enabled wireless sensors. The model has several primary and intermediate layers, including a device layer, an edge computing layer, a cloud layer, and the end-users layers. Secure end-to-end intermediated authentication layers are present in our fraught model to ensure the privacy of the sensitive record of a patient's health. We carried out our research work using Restful APIs with the help of Amazon Web Services (AWS). Our projected model is based on three significant steps of CAS. 1) accomplishment of perception into context (input), 2) defining what kind of mechanisms are required to sense and adapt to context, 3) defining the directions for how the system will have to adapt in different circumstances. We solved the issues related to low latency time while accessing the record of patients, ensured privacy and security of data sharing, and minimized the energy consumption by introducing a novel edge computing layer in an intelligent health care system. Our proposed model is an idea for self-monitoring of a Covid-19 patient, and it is also beneficial for monitoring other diseases. Still, in this research, we mainly focused on Covid-19 patient data sharing and remote treatment while in the quarantine period.

***Paper Organization***

Section I starts with the introduction and describes an abstract level of knowledge about novel coronavirus with the help of facts and figures. Section II looks at IoT-based healthcare-related work present in literature with the help of literature studies. It highlights the significant artifacts proposed by several researchers on the novel Covid-19. The section tries to present literature work that covers several research aspects. The section also discusses sharing data with graphic resources and illustrations. Section III discusses the methodology, including Restful APIs, AWS, Context-Aware System, Proposed model, patient self-monitoring, privacy preservation analysis, and patient data access control system. Section IV addresses the discussion related to our proposed model. Section VI expresses conclusionary remarks and future research work. Table 1. defines the list of abbreviations and acronyms used in this paper.

## LITERATURE REVIEW

This section deliberates a brief overview of related work on patient healthcare present in the literature. We tried to describe recent literature because this field has become more intelligent and innovative due to the evolution in IoT. Recently the authors of [11] proposed an architecture of asymmetric approach purely based upon crucial management for data sharing concept in IoT supported healthcare systems. They expressed the communication between patients and hospitals with the help of communication media and resources. Their proposed architecture is shown in figure 2.

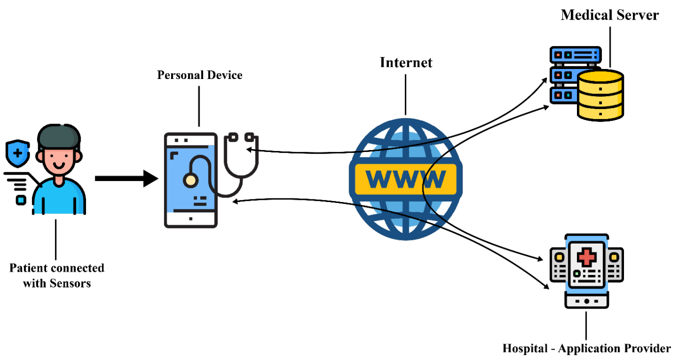


Figure. 2. Purposed architecture based upon symmetric approach key management by [11]

Three primary objects are being present in illustrated this figure. The first one is the patient connected with a personal device. The other is the Medical Body Area of Wireless Networks, and the third is the medical server. The authors proposed an ECC grounded junction containing mutual authentication by generating an end-to-end session key. They interlined the client and application provider through this approach. The authors did not discuss the privacy and energy consumption issues in their process.

Moreover, the authors only provided architectural-level information related to their research work. The authors of [12] anticipated a new concept to address three objects; Sensor, GWN, and the user. They proposed three factor-based session key generation mechanisms with the help of these entities. They compared the features with security and calculated the computational cost. In their research, they first established the connection of the application provider with a client with the help of GateWay Node through registration. They also highlighted the concept of password change in their research. For WHMS, the authors of [13] devised the most heightened and improved scheme in which they proposed the connection of the doctor and the wearable sensor. The process of authentication and key-generation consists of quadratic residues. They gave the idea of eradication mobile device attacks launched on the stolen devices. They provided a fuzzy verifier mechanism with the help of real-time timestamps. Their work comprises five significant phases: registration of new patients, registration of medical persons like a doctor, etc., login and authentication procedure, and facility of changing the password. They also delivered an overview of applying security analysis to their proposed scheme. Still, the author did not address the issue of too much energy consumption and put this issue in the challenges section. Newly, with the help of a case study, the authors of [14] anticipated several cloud models and significant security concerns. They performed a SWOT analysis on the primary and improved blockchain models. The authors discussed that with the introduction of decentralized networks, the energy consumption factor would increase at a significant rate that should be controlled with some suitable approaches. The authors also discuss other primary concerns related to distributed data storage.

## METHODOLOGY

### *Restful API*

Application Program Interface (API) allows software developers to connect two different applications or get one application's features in another application. It acts as a bridge between two systems and enables information flow from one application to the other. When it comes to the client-server architecture, both the client and the server become completely autonomous. The front-end component is called the client, while the back-end side acts as a server. RESTful APIs are lightweight and cacheable. It means that the client can save all responses within a cache. This feature indicates an improved performance of the API. When request transmissions are handled, no data gets protected on the server-side. The data is stateless, and the session is stored on the client-side. These APIs are usually stated as RESTful web services. It is because these APIs implement REST ethics as well as HTTP protocols. In our model, the edge layer sends data to the cloud and user layers through APIs. The data of the APIs is parsed on the destination sides and can be further interpreted to produce valuable outcomes.

### *Amazon Web Services (AWS)*

Amazon is at number three at this moment, having a market value of 916.6 billion USD launched the AWS platform 14 years ago. AWS platform, at present, provides cloud-based services to its users with subscription charges. It allows its customers to upload, store, and configure their data on its server. Like Microsoft Azure, AWS provides all IoT networking and configuration solutions. We used the Amazon Elastic Cloud tool for managing IoT healthcare systems in our research. With the utilization of AWS and APIs, we worked on a cloud-based centralized IoT healthcare system. Moreover, we traced the data flow between the healthcare systems using the Amazon Elastic Computing (EC2) tool.

***Context-Aware System (CAS)***

Context-aware systems are based on the SDA (Sense, Decide, and Actuate) operational cycle. It means that sensing takes place first, then there is a procedure of decision making while actuation comes at the end in which results are generated. The context might be present at any time, like personal identification, geolocation, surroundings of a particular person. It is also yoked with current timestamps. The CAS is conscious about their surroundings and nearer conditions, and they intelligently retort in a specific interval. Figure 3. defines the same basic operational cycle of CAS. In our model, we used CAS to measure the patient's health conditions like body temperature, blood pressure, and heartbeat from instant to instant to find the average values for better treatment.

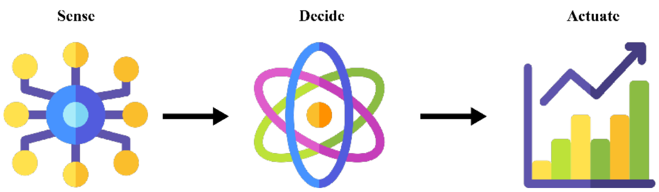


Figure 3. CAS operational cycle

***Fraught Model***

We proposed a Context-Aware system using IoT Fraught Model to manage IoT healthcare Wearable devices. In figure 4, we described a generalized architecture of the patient monitoring model with a generic look.

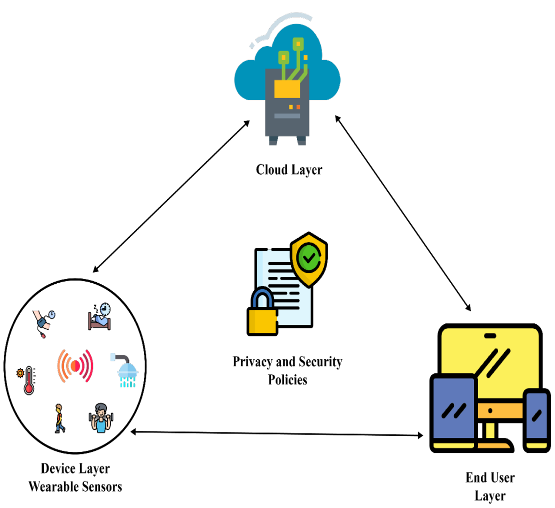


Figure. 4. Generalized IoT healthcare model's architecture

Our overall model architecture comprises four significant layers. The first layer consists of wifi-enabled wearable sensors; these sensors are connected with the mother sensor for communication. The second one is the edge computing layer that performs a local and real-time analysis to overcome the latency issues. The third entails the AWS cloud layer, and the last one is composed of user-side layers. The first layer contains many wireless sensors connected with the mother sensor, the internet, the data attainment motherboard, and several protocols related to communication to send data towards the edge computing layer. At this layer, we performed real-time and local analysis. After analysis, data will be forwarded to a centralized cloud server for different dispensation. These wireless sensors allow the users to gather real-time data at various acquiring frequencies. Data preprocessing techniques are applied at this layer, like extraction of features, data messaging, and removal of noise present in data. After data preprocessing, this data is provided to the support system for decision making. We named it the Fraught model because it performed multifaceted data examination and analysis with the help of AI algorithms. The model provides sophisticated decisions concerning the health of a particular person. Our model's fourth and last layer consists of the end-user or receiver layer. It might be in several forms, but its central portion contains intelligent devices like smartphones, tablets, or personal computers. In between all these layers, tiny modules or sub-layers are also added for the sake of heftiness and fluffiness of decision making or to support the healthcare model. These sub-layers are configured to ensure security and reliability checks as well. We present an edge computing concept for the sake of intelligent conclusions and to reduce the latency issues of the cloud. At the same time, we also introduced the CL syncing concept for the everlasting storage of data. This is our extraordinary effort because many other data management and interpretation techniques can apply to collected data in the future. In figure 5, we summarized the behavior of our proposed model with labeling and descriptions.

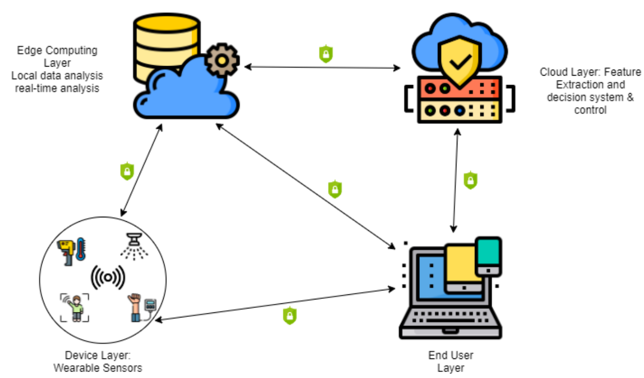


Figure 5. Proposed IoT Fraught Model for IoT patient self-monitoring

***Patient Self Monitoring***

Self-monitoring is not limited to the patient as the patient's record acquired from wearable sensors propagates in a different channel for processing. In the edge computing layer, local and real-time analysis is performed then the data can be passed on both sides, i.e., the cloud and end-users layers. On the end-user layer, the doctor can treat the patient on an urgent basis. Data can be further interpreted on the cloud layer for better results generations and future health prediction. The APIs passed data to this layer to run ML algorithms for forecasts and generate more data visualizations. The end-user layer also includes the patient mobile device for monitoring the health. Like the patient can see the improvement or deterioration based on processed data.

***Privacy Preservation Analysis***

The device layer containing several IoT-enabled wearable sensors collects data in chunks and passes data to the authenticated edge computing layer. The handshake between the edge computing layer and the device layer is only possible when the edge computing layer is fully authenticated with the device layer. The accessibility of data from the edge computing layer to the cloud and end-user layer also requires end-to-end authentication since authentication channels are mapped on all four layers. That is why there is no possibility of malicious activist intervention. The integrity of the patient data while sharing processed data from the cloud and edge computing layer can also be preserved.

***Patient Data Access Control System***

We have also devised a patient data access control system in the end-user layer. The data can be accessed by the doctor, hospital, or by the patient with the help of their mobile devices. The data consists of the gradual health record of the patient, statistics of the patient health record, and the predictive results. The data can also be transferred to other people like the patient's family members for a better cure from the end-user layer. Additional layers are only responsible for sharing data to the user layer, preventing data leakage.

## DISCUSSIONS

Our proposed IoT Fraught Model for IoT healthcare Wearable devices covers many valuable points. The first benefit of our model is that it provides quick real-time analysis using an edge computing layer and syncing with the cloud for long-term storage. In this way, data can be analyzed in the future for further processing. Since the edge computing layer performs the real-time analysis and sends preprocessed data to the cloud, multiple operations and techniques can also be applied to the cloud layer. Like accuracy of the healthcare model can be checked by using many AI and ML algorithms. The other significant yield of our system is that it is based on a CAS concept that reduces the actuation, transmission, and processing during communication. In this way, we can save power which is the central issue of IoT described in Literature as in our model, and data is synced with the cloud after the edge computing layer real-time analysis. That is why there is zero chance of data loss in case of sensor damage or any other disaster as the cloud takes frequent backups of the data. Moreover, we also discussed data privacy and integrity concerns by introducing intermediate end-to-end authentication sub-layers. These layers can preserve the confidentiality of the data while sharing data among different primary layers.

## CONCLUSION

Starting from the brief history and introduction of Covid-19 and IoT, we presented an overview of the patient self-monitoring. We discussed several data-sharing methods in IoT healthcare systems from the past research. We proposed an elegant IoT Fraught Model for IoT healthcare Wearable devices for data sharing. We expressed how our proposed model works in an emergency where the distance between the patient and other people is mandatory. We also discussed the positives of our system as it saves energy consumption and ensures the privacy of patients' data. Since privacy and security are IoT healthcare systems' primary concerns, as discussed in the challenges section. So, there is an enormous scope of this research in the future. The concept of decentralized servers or Blockchain can also be applied to our proposed model. There is a need for an additional protection model for protecting these wireless sensors to ensure the unsurpassed security of the healthcare systems in the upcoming years.

## REFERENCES

[1] WHO Coronavirus Disease (COVID-19) Dashboard. 2021 5 March 2021]; Available from: https://covid19.who.int/?gclid=CjwKCAjwltH3BRB6EiwAhj0IUCGHN8b-difm5xexvOWaL0KVtJHI-sI1ngtj-9pMGtsE_HojaQpw6hoCuTwQAvD_BwE.

[2] Parmet, W.E. and M.S.J.N.E.J.o.M. Sinha, Covid-19—the law and limits of quarantine. 2020. 382(15): p. e28.

[3] Ansari, S., et al., Internet of Things-Based Healthcare Applications, in IoT Architectures, Models, and Platforms for Smart City Applications. 2020, IGI Global. p. 1-28.

[4] Fischer, G.S., et al., ElHealth: Using Internet of Things and data prediction for elastic management of human resources in smart hospitals. Engineering Applications of Artificial Intelligence, 2020. 87: p. 103285.

[5] Al-khafajiy, M., et al., Remote health monitoring of elderly through wearable sensors. Multimedia Tools and Applications, 2019. 78(17): p. 24681-24706.

[6] Christodoulides, N., et al., Sensors that learn: The

evolution from taste fingerprints to patterns of early disease detection. Micromachines, 2019. 10(4): p. 251.

[7] Hasan, M., et al., Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 2019. 7: p. 100059.

[8] Ma, J. Coronavirus: China's first confirmed Covid-19 case traced back to November 17. 2020, March 13; Available from: https://www.scmp.com/news/china/society/article/3074991/coronavirus-chinas-first-confirmed-covid-19-case-traced-back.

[9] Worldometer. Coronavirus Cases. 2021 [cited 2021 March 08]; Available from: https://www.worldometers.info/coronavirus/.

[10] WHO, Draft landscape of COVID-19 candidate vaccines. 2020, June 24.

[11] Sowjanya, K. and M. Dasgupta. Survey of Symmetric and Asymmetric Key Management Schemes in the context of IoT based Healthcare System. in 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T). 2020. IEEE.

[12] Li, X., et al., A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. Journal of Network and Computer Applications, 2018. 103: p. 194-204.

[13] Jiang, Q., et al., Efficient end-to-end authentication protocol for wearable health monitoring systems. Computers & Electrical Engineering, 2017. 63: p. 182-195.

[14] Luo, E., et al., Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. 2018. 56(2): p. 163-168.