Framework for Collecting Data from specialized IoT devices - An application to enhance Healthcare Systems.

Saiful Islam*, Shahriar Sobhan†, Maria Valero*, Hossain Shahriar*, Liang Zhao*, and Sheikh I. Ahamed‡
*Information Technology Department, Kennesaw State University
†CyberSecurity Institute, Kennesaw State University
‡Computer Science Department, Marquette University
Email: {ssobhan,mislam16}@students.kennesaw.edu, {mvalero2, hshahria, lzhao10}@kennesaw.edu, sheikh.ahamed@marquette.edu

***Abstract*—The Internet of Things (IoT) is the most significant and blooming technology in the 21st century while rapidly developed by covering hundreds of applications in the civil, health, military, and agriculture areas. IoT is based on the collection of sensor data through an embedded system, and this embedded system uploads the data on the internet. Devices and sensor technologies connected over a network can monitor and measure data in real-time. The main challenge is to collect data from IoT devices, transmit them to store in the Cloud, and later retrieve them at any time for visualization and data analysis. All these phases need to be secure by following security protocol to ensure data integrity. In this paper, we present the design of a lightweight and easy-to-use data collection framework for IoT devices, that can potentially be applied to sensors that monitor healthcare. This framework consists of collecting data from sensors and sending them to Cloud storage securely and in real-time for further processing and visualization. Our main objective is to make a data-collecting platform that will be plug-and-play and secure so that any healthcare organization or research team can use it to collect data from any IoT device for further data analysis.**

***Index Terms*—Internet of Things, data collection framework, cloud storage, processing and visualization.**

I. Introduction

Currently, the Internet of Things (IoT) is a fast-moving technology that interconnects ubiquitous computing devices between them and the Cloud. Because every day more and more devices are released, there are more opportunities for users to send, receive, synchronize, and share information between them. IoT is nowadays a necessity with applications in different sectors such as m-Health [1]–[3], smart houses [4], smart commerce [5], etc. These devices are transforming who the data is processed in homes, industries, commercial automation sectors as the number of devices connected to the Internet is exponentially increased. Cisco estimates that over 50 million devices were connected to the internet by 2020 [6]. This trend also impacts the global market. IoT is expected to get a value of more than 1000 billion by 2026 with a Compound Annual Growth Rate (CAGR) of 10.53%, during the period 2021–2026 [7] as shown in Figure 1.

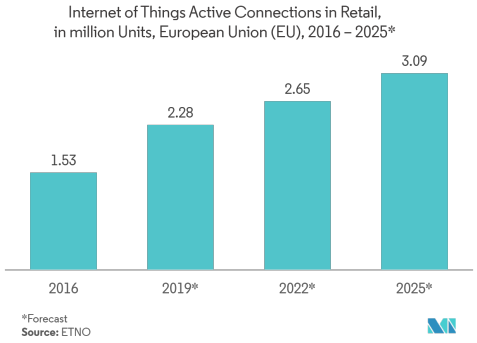

Fig. 1. Internet of Things Active Connections in Retail, in million Units, European Union(EU). 2016 -2025*

However, the data collection of data of heterogeneous devices is still a open problem in the IoT community. The data needs to be transmitted in a secure way to avoid that malicious intruders can get access or control over those devices. In this paper, we introduce a preliminary work related to a data collection framework for IoT devices, which is plug-and-pay and ensure data integrity. The system is envisioned to be used by any IoT device, especially for those that are meant to collect healthcare information.

II. Challenges in IoT Data Collection

Deal with high data volumes is not an easy task. The architectures and applications involved in the data collection task will for sure get more complex and demanding. Before designing a framework for data collection, we need to take into account multiple challenges that need to address.

Here are the main challenges with IoT data collection are facing when it comes to collecting IoT data:

- **Heterogeneity of the devices.** IoT devices in the market come in an immense variety of technologies. Creating a framework that can adjust itself to collect data from any device is a difficult task and requires planning and subsequent improvements.

978-1-6654-1685-6/21/$31.00 ©2021 IEEE
DOI 10.1109/ICDH52753.2021.00045

- **Huge volume of data.** The data needs to be prepared for transmission and storing. Due to high volume, data analysts need to design ways to optimize data storage and automatize the preparation process.
- **Security of the data.** Security concerns are present in IoT data collection, processing, and storage, especially is those devices are collecting sensitive-data. Security measures needs to be placed to avoid jeopardize the safety of the users and/or companies.
- **Real-time stream data.** Many IoT devices capture sensitive real-time data that needs to be stream for urgent analysis. The collecting frameworks need to be reliable by ensuring almost error-free communications. Also, data analysts need to find ways to process data on the fly and probably at the edge of the network.

The main idea of the proposed framework is to provide a platform for researchers to easily and securely collect, storage and visualize data in any field, especially in the healthcare sensor where data is sensitive.

III. Innovation

The proposed research is expected to be the platform for multiple other research projects that require real-time data collection from IoT devices. With this framework, multiple researchers and students from different areas and backgrounds will be able to easily collect data from their sensors and visualize it in real-time. Furthermore, the utilization of this framework will enable data analysis decisions over the data, as the platform permits data inspection from multiple perspectives. For example, it is possible to check the temperatures over a week or month, average them, apply different metrics, to finally decide the best metrics for apply machine learning techniques for forecasting. To sum up, the benefits of this framework are broad and beneficial for multiple types of data IoT projects.

We have built the framework in a way that it can be plug and play and secure so that any industry and research group can adapt to this. We envision that this framework can be particularly useful in the following industries:

- Healthcare: Remote and in-situ monitoring of the patients is crucial these days, and IoT devices play a critical role in this monitoring. We envision that our framework can be used to collect data from personal monitoring devices, hospital tracking systems, caretakers sensor data, environmental devices, etc.
- Agriculture: Activities like crop grow monitoring, farming activities, forecast of development, temperature and climate control of greenhouses, water usage, etc., are among the activities that IoT and our framework can make a difference.
- Manufacturing: Sensor for workplace safety (e.g. measuring air conditions), worker monitoring, forecast machine lifespan, etc., are some of the activities that involve heterogeneous sensors that can be plugged in the proposed framework.

IV. Framework

Figure 2 shows the proposed framework layered architecture. The base of the architectural stack consists of a set of sensors (e.g pressure sensors, vibration sensors, temperature sensors, etc.), a computer board (e.g Raspberry Pi), a Cloud Server, a Gateway, Secure Protocol, Python Programs, and a data visualization tool. The base layer gathers information from the physical world using sensors and manipulates it while interacting with the gateway layer. The gateway layer routes and forward this data collected from the Raspberry Pi to the cloud layer for storage and processing. Lastly, the display layer retrieves all the data from the cloud and shows it in the dashboard.

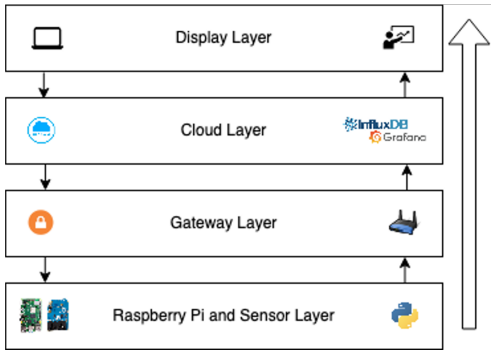

Fig. 2. Proposed framework layers.

The framework consists of a set of sensors (e.g pressure sensors, vibration sensors, temperature sensors, etc.), a computer board (e.g Raspberry Pi), a Cloud Server, a Gateway, Secure Protocol, Python Programs, and a powerful data visualization tool. The framework can extract the data from the sensor using python code. The extracted data is sent to a Cloud (High-Computing Performance - HCP Cloud) in real-time by following HTTPS (Hypertext Transfer Protocol Secure) security protocol and storing it in a powerful stream-data database (InfluxDB [8]). Then, the framework provides real-time data points monitoring using a powerful data visualization tool named Grafana [9] by showing up-to-date sensor data that is refreshed every five or fewer seconds.

Fig. 3. Prototype of the framework consist of Raspberry Pi4 connected to a sensor that transfers the data using a 12C shield digitizer.

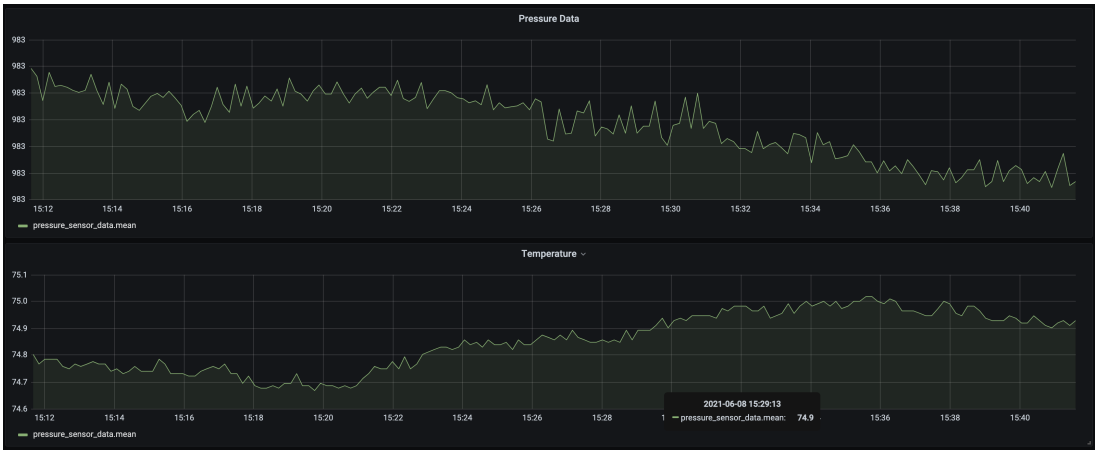

Fig. 4. Example of real-time data collected in the proposed framework

V. Results

With our initial prototype (Figure 3), we were successfully able to collect sensor data indefinitely into the cloud server using a raspberry PI. The Raspberry Pi is connected to a specialized sensor. We have conducted experiments to collect data from a pressure sensor to understand the variability of the application of pressure from hands, fingers, and objects (like pencils, markers, etc.). We also successfully collect real-time data from a temperature sensor that continuously runs for several days in order to measure the variability of the temperature over time. We applied multiple techniques to increase the temperature of the environment (like place direct light over the sensor) to evaluate the increasing and decreasing temperature. With these results, we believe that it is possible to conduct multiple research studies in the healthcare, smart homes, agriculture, and manufacturing sectors. Figure 4 shows an example of continuous and real-time data collected from two sensors; a pressure sensor (top of the image), and a temperature sensor (bottom).

VI. Conclusion and Future work

The objective of this project is to provide a robust data collecting framework for variety of IoT devices. We believe that this framework can adapt by many major areas including healthcare, smart homes, agriculture, and manufacturing sectors. In future, we want to evaluate the effectiveness of collecting real-time, synchronous, and stream data along with performance benchmarks.

VII. Acknowledgement

This work was supported in part by research computing resources and technical expertise via a partnership between Kennesaw State University's Office of the Vice President for Research and the Office of the CIO and Vice President for Information Technology [10].

References

[1] S. Deshkar, R. Thanseeh, and V. G. Menon, "A review on iot based m-health systems for diabetes," *International Journal of Computer Science and Telecommunications*, vol. 8, no. 1, pp. 13–18, 2017.

[2] A. Eldosouky and W. Saad, "On the cybersecurity of m-health iot systems with led bitslice implementation," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2018, pp. 1–6.

[3] K. N. Mishra and C. Chakraborty, "A novel approach towards using big data and iot for improving the efficiency of m-health systems," in *Advanced computational intelligence techniques for virtual reality in healthcare*. Springer, 2020, pp. 123–139.

[4] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "Sok: Security evaluation of home-based iot deployments," in *2019 IEEE symposium on security and privacy (sp)*. IEEE, 2019, pp. 1362–1380.

[5] E. Turban, J. Whiteside, D. King, and J. Outland, "Mobile commerce and the internet of things," in *Introduction to Electronic Commerce and Social Commerce*. Springer, 2017, pp. 167–199.

[6] D. Evans, "The internet of things how the next evolution of the internet is changing everything," https://tinyurl.com/theIoTCisco, April 2011, accessed: 04-01-2021.

[7] M. Intelligence, "Internet of things (iot) market - growth, trends, covid-19 impact, and forecasts (2021 - 2026)," https://tinyurl.com/IoTSmarter, accessed: 04-01-2021.

[8] Influxdata Inc, "InfluxDB," 2019. [Online]. Available: https://www.influxdata.com/

[9] Grafana Labs, "Grafana," 2018. [Online]. Available: https://grafana.com/

[10] T. Boyle and R. Aygun, "Kennesaw state university hpc facilities and resources," 2021. [Online]. Available: https://digitalcommons.kennesaw.edu/training/10