THINK INDIA JOURNAL
ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

Data Acquisition and Collection Modelling Using Fog Computing In Internet of Things

Sakshi Takkar[1], Mohit Arora[2], Shivali Chopra[3]

School of Computer Science and Engineering

Lovely Professional University, Phagwara, Punjab, India

[1]sakshi.22258@lpu.co.in, [2]mohit.15980@lpu.co.in, [3]shivali.19259@lpu.co.in

Abstract

In recent times, various adaptable Internet of Things (IOT) frameworks have been expanded in different fields of our daily life like in health care, wearable devices, smart city, smart grids etc. An extensive amount of real-time data, images, videos are generated every day. To handle the data generated by IOT devices, a large storage capacity and high-level computation is needed. Moreover, managing the use of gigantic information and clients' security is an imperative issue in the industries. Cloud based IOT systems are in trend to store the massive data generated by IOT devices. The comfort that cloud presents to IoT follows at the expense of conceivably newly security dangers, which have never been taken into consideration in a conventional IoT framework.Fog computing is an extension to the cloud due to which hard computations and communications are possible near to the end client. Fog computing augments the real time applications, security, portability and protection in the IOT application scenarios. In this paper, we are summarizing the methods and technologies of data collection of IOT devices by using Fog computing.

Keywords: Fog Computing, IOT, Data Acquisition, Sensors, Data Mining, Encryption, Data Privacy, Data Sharing,

1. Introduction

Internet of things, or IoT, refers to the interconnection of various physical devices embedded with sensors. IoT technology deals with smart devices to collect the data as well as to provide the useful and accurate data to the users. IoT smart devices are expanding in whole world and due to which a biggest change in world is coming. Today everything we are using has embedded sensors. These sensors enable various physical devices to monitor the things and provide the results to the users. Internet of Things process mainly comprises with the two phases- data collection and data mining. Collection of Data in IoT refers to the receiving or

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

extracting information from various IoT devices. Data mining is extracting the useful patterns from the collected data. Collection of data is one of the majortask in the entire process. This whole process resides on the communication within devices and server or repositories. Each device generates heterogeneous data which gives results to massive data. Due to massive amount of the data is being generated by each device, a novel and secure data collection method is required in IoT.

There are various methods already exist, but more enhancements are needed to fetch the data accurately and efficiently from devices and sensors. After the data collection, next phase is storing the data in an efficient manner. Cloud and fog storage can be used for storing the data. But cloud computing mainly uses the centralized mechanism which is completely lacking in the security. Anyone can access the stored data in the cloud and no authentication is required to access the cloud storage. Whereas in the fog computing high security is present because it is not using the centralized mechanism and large number of nodes or systems takes part for the processing of data which makes the system more complex and secure. Now-a-days, there are numerous attacks which are breaking the confidentiality, integrity of the data. In IoT applications, security of data is the biggest challenge. There can be many attacks that are breaching the security of data. In the regard of IoT data security, IoT developers and researchers should take some initiatives. However, everyday new security methods are developing. But still, there is high need to secure the data more.

2. Background and Related Work

M. S. Hossain et al. has proposeda cloud assisted Health-IoT framework to offer the security towards the data of the patient. ECG and other various types of data were collected to secure it from various attacks like identity theft attack. The main research objective was to provide the security to the healthcare data. No input and output parameters were defined in the paper [1]. Chi-Tsun Cheng et al. described that as there can be multiple users who need to fetch or extract or collect the data at the same time, which failed the single data collection processes. To overcome this problem, a novel concurrent data collection tree methodology had been proposed in which multiple can enable their processes concurrently. The main objective of this research was to shorter the delays which was fulfilled by this work[2].

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

Fengrui Shi et al. proposed a methodology which comprises of context awareness routing and deploying citizen centric algorithm in real time environment. The primary objective of this study was to decrease the latency while collection of data from various sources. This study provides better performance levels which includes the amount of transmission delay and number of hops while collection[3].

GhyzlaneCherradl et al. proposed a methodology using MQTT (Message Queue Telemetry Transport) protocol. The primary objective of this proposed work was to propose the technique for the rapid transmission of data. As MQTT is considered as one of the secure protocol, so the main idea of using this protocol was to provide the better security levels [4].Attila Hideg et al. has proposed a methodology where multiple sensors are deployed in the network to collect the heterogeneous data, so to collect this data. SensorHub framework proposed for data collection from distributed mass of sensors. In this paper, actual analysis of collected data using cloud base solutions had been done[5].

Jaejin Jang et al. created a new methodology to handle the secure data streams with more efficiency. In this paper, LDPC code methodology had been used. The primary aim of this work was to propose the technique for efficient performance in terms of power consumption as well as data transmission time consumption while dealing with the security of encrypted data streams. Reduced transmission time as well as power consumption levels had been achieved [6]. GunasekaranManogaran et al. proposed a new methodology comprises of Mega fog redirection, grouping and choosing architecture. Cloud mechanisms are not much secure for data and it also allows the unauthorized access to the data. So, the main objective of this work was to provide the security to data from unauthorized access. In this work, different parameters had been used to provide the efficient results [7].

Yi-NingLiu et al. described that now-a-days confidentiality is one of the major problems through various attacks every day is happening. So, New Methodology had been proposed which was able to preserving the privacy of the raw data. The main goal of this proposed work was to manage the raw data and to unlink the data from its contributors. This methodology discards the privacy leakage problem as helps to provide the proper confidentiality levels[8].Hongtao Li. etal. proposed that in healthcare applications, security among patients' data is highly preferable. So, to maintain that security levels or to provide the

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

more security, a new methodology had been proposed. In this methodology, a client-server model based on PPDC method had been used. The main goal was to secure the patients' data. In this methodology, various dissimilarity matrices were used to prepare the clusters. Desired level of results was achieved by this proposed methodology[9].

EntaoLuo et al. introduced other healthcare methodology to tackle with the high levels threats, vulnerabilities and attacks. This methodology comprises of Privacy Protector Mechanisms and SW-SSS approach. Real data were used to investigate the various incidents, challenges for the data protection. This methodology provides the required level of confidentiality as well as security against high level attacks[10].

Wei Wang et al. have proposed Proxy re-encryption mechanism for secure data collection, access and storage in cloud based mechanism. The aim of this work was to maintain the data confidentiality at the time of the collecting, accessing, storing the data. It offers the safety from the both the parties i.e. insiders and outsiders[11]. Hi Tao e t al. has introduced various ciphers that we use to secure the data. A new methodology using FPGA hardware based cipher to secure the data in the healthcare applications has been proposed. It helps to maintain the confidentiality of data. Various parameters had been used to get the results like frequency rate of hardware, energy consumption, time consumption etc. Efficient and desired results were achieved[12].

TajRahman et al. described that large amount of data can be transmit from multiple sensing nodes which can create congestion and delay related challenge. So to tackle with this problem CDCAPC mechanism waspproposed. The main objective was to decrease the traffic congestion problem, decrease the problem related with throughput, problems related with continuous object detection[13]. Pan Wang et al. has proposed a smart gateway data collection method using MDA plug-in mechanism over traditional gateway data collection method to provide the better quality of performance. Moreover, in this method cloud controller has been used to deal with the control policies[14].

Zhijing Qin et al. has described that when data is aggregated from the various IoT nodes and later updated in cloud repositories or in local repositories, then there can be delays in this process. So, to minimize the delays a probabilistic model for many- to-one communication

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

process has been proposed[15].Zhitao Guan et al. has introduced an APPA (An anonymous and privacy preserving data aggregation) mechanism. The main objectives were preserving privacy, authenticating data sources, verifying the integrity of the data, enforceability and anonymity of device. It provides the accurate results and proves that this proposed methodology is one of the best choice for devices which are having constrained resources[16].

Ata Ullah et al. have proposed two different algorithms- message receiving and message extracting in order to aggregate the data more securely and efficiently. Message receiving algorithm is to aggregate the data at aggregator node whereas message extracting algorithm is proposed to use at fog server. After the proper aggregation of data, it was stored using local repositories and later uploaded to cloud repositories. This method has shown less energy consumption, storage requirements, good transmission ratios etc.[17]. Guorui Li. et al. introduced a Compression sensing theory to transmit the compressed data as well as to increase the network lifetime. This proposed scheme was divided into two partitions- clustering of data based on their spatial correlation and other is reconstruction of data at edge of the network. This reconstruction of data was done by ADMM algorithm[18].

N.A.M. Alduaiset al. have proposed a data collection method or algorithm for tracking the wearable and mobile devices within IoT systems. This was proposed to collect the complex data even at very minimum energy consumption. The algorithm was partitioned into three phases- Initial phase, IoT edge phase and Fusion Center phase. Results were evaluated using real datasets[19].Siyao Cheng et al. described that biggest challenge is to integrate the data because data is usually heterogeneous in nature. In order to remove this problem, a model based on Hidden Markov Process for integrating heterogeneous data was proposed. Cooperative event detection case study also used in this mechanism. Later, good performance in terms of power consumption and accuracy were achieved[20].

Anfeng Liu et al. have proposed new multi representative re-fusion method for the data collection from multi sensors with high performance in terms of energy consumption as well as network lifetime. In this methodology, data coverage set values were used. This reading of data coverage set values is expressed as R-node. This set value is smaller near the sink node and higher when the sink node is far away. This whole methodology was proposed to

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

decrease the energy consumption[21].Xuemei Xiang et al. introduced a delay and energy-efficient method for data collection based on matrix filling theory to gather the randomly generated data. This paper shows how TDMA theory has been used for efficient transmission. Moreover, DEEDC method used clustering data aggregation method[22].

3. Conclusion

IOT devices are used in real life applications like health centres, smart devices, traffic control systems etc. A Massive amount of data is generated by IOT devices. For storage and processing of large amount of data clout based IOT systems are in use. However, lot of security issues are there in these clouds based systems. Fog computing is removing these security dangers. Fog Computing isn't a trade for Cloud Computing. Fog Computing is a major advance to a disseminated cloud by controlling information in all node focuses, fog registering permits transforming data centre into a circulated cloud stage for clients. Fog is an expansion which builds up the idea of cloud administrations.Fog Computing stretches out the Cloud Computing worldview to the edge of the system therefore helps in developing new applications.Analysis of different data acquisition techniques and methodologies has been done to collect and analyse the data from IOT devices by using Fog Computing to find the future possibilities of improving them.

.

REFERENCES

[1] M. S. Hossain and G. Muhammad, “Cloud-assisted Industrial Internet of Things (IIoT) - Enabled framework for health monitoring,” *Comput. Networks*, vol. 101, pp. 192–202, 2016.

[2] C. T. Cheng, N. Ganganath, and K. Y. Fok, “Concurrent data collection trees for IoT applications,” *IEEE Trans. Ind. Informatics*, vol. 13, no. 2, pp. 793–799, 2017.

[3] F. Shi, U. Adeel, E. Theodoridis, M. Haghighi, and J. McCann, “OppNet: Enabling citizen-centric urban IoT data collection through opportunistic connectivity service,” *2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016*, pp. 723–728, 2017.

[4] G. Cherradi, A. El Bouziri, and A. Boulmakoul, "Smart Data Collection Based on IoT Protocols," *Jdsi'16, Issn 2509-2103*, no. November 2017, 2016.

[5] A. Hideg, L. Blazovics, K. Csorba, and M. Gotzy, "Data collection for widely distributed mass of sensors," *7th IEEE Int. Conf. Cogn. Infocommunications, CogInfoCom 2016 - Proc.*, no. CogInfoCom, pp. 193–198, 2017.

[6] J. Jang, I. Y. Jung, and J. H. Park, "An effective handling of secure data stream in IoT," *Appl. Soft Comput. J.*, vol. 68, pp. 811–820, 2018.

[7] 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," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 375–387, 2018.

[8] Y. N. Liu, Y. P. Wang, X. F. Wang, Z. Xia, and J. F. Xu, "Privacy-preserving raw data collection without a trusted authority for IoT," *Comput. Networks*, vol. 148, pp. 340–348, 2019.

[9] H. Li, F. Guo, W. Zhang, J. Wang, and J. Xing, "(a,k)-Anonymous Scheme for Privacy-Preserving Data Collection in IoT-based Healthcare Services Systems," *J. Med. Syst.*, vol. 42, no. 3, 2018.

[10] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, 2018.

[11] W. Wang, P. Xu, and L. T. Yang, "Secure data collection, storage, and access in cloud-assisted Iot," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 77–88, 2018.

[12] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 410–420, 2019.

[13] T. Rahman, X. Yao, and G. Tao, "Consistent Data Collection and Assortment in the Progression of Continuous Objects in IoT," *IEEE Access*, vol. 6, pp. 51875–51885, 2018.

[14] P. Wang, F. Ye, and X. Chen, "A Smart Home Gateway Platform for Data Collection and Awareness," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 87–93, 2018.

[15] Z. Qin, D. Wu, Z. Xiao, B. Fu, and Z. Qin, "Modeling and Analysis of Data Aggregation from Convergecast in Mobile Sensor Networks for Industrial IoT," *IEEE Trans. Ind. Informatics*, vol. 14, no. 10, pp. 4457–4467, 2018.

[16] Z. Guan *et al.*, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, 2019.

[17] A. Ullah, G. Said, M. Sher, and H. Ning, "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," *Peer-to-Peer Netw. Appl.*, 2019.

ISSN: 0971-1260
Vol-22-NO-30 Special Issue-December-2019

[18] G. Li *et al.*, "Energy efficient data collection in large-scale internet of things via computation offloading," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4176–4187, 2019.

[19] N. A. M. Alduais, I. Abdullah, and A. Jamil, "An Efficient Data Collection Algorithm for Wearable / Mobile Tracking System in IoT /WSN," *2018 Electr. Power, Electron. Commun. Control. Informatics Semin. EECCIS 2018*, pp. 250–254, 2018.

[20] S. Cheng, Y. Li, Z. Tian, W. Cheng, and X. Cheng, "A model for integrating heterogeneous sensory data in IoT systems," *Comput. Networks*, vol. 150, pp. 1–14, 2019.

[21] A. Liu, X. Liu, T. Wei, L. T. Yang, S. Rho, and A. Paul, "Distributed multi-representative re-fusion approach for heterogeneous sensing data collection," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 3, 2017.

[22] X. Xiang *et al.*, "Delay and energy-efficient data collection scheme-based matrix filling theory for dynamic traffic IoT," *Eurasip J. Wirel. Commun. Netw.*, vol. 2019, no. 1, 2019.