INVESTIGATING PRIVACY AND SECURITY IN HEALTHCARE BASED CLOUDLET ENVIRONMENT USING MULTI-LEVEL AGENTS

[1]Ms.Mary Jacob, Ms.Kalaiselvi K[2]
[1]Department of Computer Science, Kristu Jayanti College,Bangalore
[2]Department of Computer Science, Kristu Jayanti College,Bangalore

Abstract **-** In IoT-based healthcare, medical devices are more vulnerable to numerous security threats than other network devices. Solutions are able to offer security to patients' information during data transmission to certain extent, however cannot avoid certain threats like data leakage and collusion. This article investigates the challenges with privacy protected data collection. To deal with these challenges, a computation offloading architecture is proposed to process huge data generated by IoT devices whilst concurrently meeting real-time deadlines of IoT applications. This paper explores authenticity and integrity of data in cloudlet environment. Initially, for monitoring data transfer among cloudlets and to tighten up integrity for data transferred, hence a higher level security agent concept was proposed. By this, medical advisor can offload his/her handheld device to the nearby cloud through LAN and get work done in short span of time, thus achieving data integrity.

Keywords: **–** IoT, offloading, cloud, authenticity, integrity.

1. Introduction

With the ability of pervasive surveillance, Internet of Things (IoT) directly transforms the method of living and working. If IoT based on various applications attains its fullest potential, it will fundamentally change each perception of our lives. IoT is slowly starting to interlace into healthcare on both doctor and patient. IoT is progressively becoming key enabler in healthcare industry by providing comprehensive enhancements in patient appointment, predominantly when IoT sensor networks can be utilized to examine patients in hospitals and yet at home.

Although, IoT is an evolution of Internet to facilitate numerous novel features to progress patients' everyday lives devoid of interrupting their privacy, these functional features are instances of security and privacy threats and attacks to patients' sensitive data i.e. sent via open wireless channels and data is amassed in back-end servers.

In general, medical sensor network devices in IoT are sourced to be extremely vulnerable to several security attacks than other devices. This article attempts to prevail over these confront to certain extent with privacy protected data collection. Initially, the work examines the challenges with privacy protected data collection. Also, we offer a computation offloading architecture, which attempts to exploit obtainable computing resources in vicinity of authenticity based IoT devices as opposed to offloading computations directly to cloud [1]. The proposed framework leverages parameter to adapt IoT device's authenticity factors, like agents and encryption/decryption, to meet real-time deadline requirements of IoT applications whilst conserving security and privacy of both client and server IoT devices.

Our anticipated computation offloading framework provides diverse benefits over computation offloading schemes. The anticipated framework is cost-efficient unlike certain cloudlets; it does not need deployment of data centres at network environment [2]. Therefore, proposed framework is amenable for remote regions while cloud access is restricted. Furthermore, local processing of information also eases reliability and security issues for IoT devices. This framework provides security advantages as data generated from IoT devices is processed within local network and is not exposed to Internet thus reducing possibilities of risk. The framework imparts reliability benefits as dependency over single cloud server is avoided (no single point of failure) using numerous IoT devices in vicinity of user.

2. Overview Of Proposed Architecture

This section explains a patients' privacy protected data collection environment. Alike of traditional healthcare applications based IoT networks, Authenticity Provider (AP) has four phases:

1) IoT network consists of abundant medical sensor devices and other network devices. IoT sensor devices sense patients' bodies to obtain data.
2) Medical sensor device then broadcasts the collected patients' information to data storage system via communication service provider. The CSP is a significant factor that wishes to generate secret data and distribute secret data to cloud servers, which is a part of distributed storage system.
3) The storage system has patients' data acquired from medical sensors in IoT network and provides querying services to different users that comprises of doctors, healthcare providers, and health professionals.
4) Patients' data access management (PDAM) method is exploited by medical users (healthcare providers) to get access to patients' data and observe patients' health performance.

This work does not spotlight on first two authenticity strategies, i.e. privacy in data acquisition phase and CSP phase. The work mainly concentrates on security and privacy in communication characteristics that deals with third and fourth strategies. In third phase, patients' data storage is distributed to environment composed of numerous cloud servers. In such framework, other network devices impede with medical sensor devices under related IoT networks. They may carry diverse security and privacy threats to medical

devices. Therefore, transmitted data offered by medical sensor devices is typically vulnerable. Devoid of recognizing any alterations of received patients' data, when data is transmitted over upstream cloud server through CSP, data cannot be protected [3]. Such information extremely impacts overall health monitoring superiority and quality of service.

Further, dominance of IoT medical device sensing is unleashed merely by appropriately collecting unprotected data from diverse medical sensors whose data may be customized before transmission. Despite of whether transmitted data is confined or not, they can be altered during transmission from medical to cloud server by cloud service providers (CSP). Certain medical sensors continuously offer protected data, while others may create compromised, biased, or even fake data owing to attacks [4]. Based on this, data collected at cloud server has to be convoy by trustworthiness of data from individual sensor nodes.

In our proposed framework, authenticity-based IoT devices offer priority to devices within local network for computation offloading devoid of direct offloading to cloud. In addition, our anticipated computation offloading framework, computing nodes adjust their authenticity factors to meet real-time deadline needs of offloaded applications.

3. Operational Model

In this section, the strategies of client and server nodes are discussed to resourcefully execute offloaded application. Assume that every computing node in IoT cluster was aware of every other computing node's parameters through registration process, which is performed when an IoT device is coupled to IoT cluster as in figure 1.

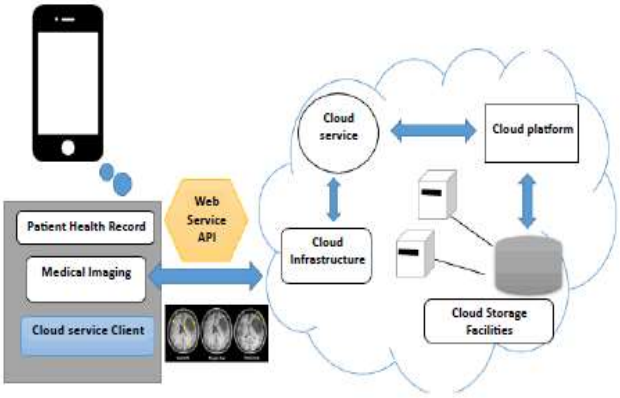

Fig 1: Pictorial representation of IoT cluster

Client IoT Node's functionality: If client IoT node acquires request to application execution, it either selects application for processing its own resources or chooses other IoT server nodes to offload application/tasks. While offloading, client IoT node tags deadline of task along with offloaded data. If server IoT node responds to client node with an acknowledgment, server node accepts offloading request, thus client node waits for server node to fulfil the offloaded task. If it does not receive any acknowledgment from server

node, client node moves to another server node to offload task. If the offloaded task's execution is completed, it sends task completion status to client node, so that client node can download the outcomes from server node.

Server IoT Node's functionality: When server IoT node upon receives offloading request, it determines whether tasks can be completed in specified deadline. The server node adapts itself based on task list already in server queue, available energy, operating frequencies range, and other parameters. If the server node, cannot offload within specified deadline, then it offloads tasks to another server node (if available) to the cloud. However, the server IoT node transmits negative acknowledgement signal to client IoT node informing that server IoT node cannot process offloaded tasks.

To guarantee data security and privacy, an authenticity based framework is anticipated over distributed cloud storage, data encryption and data compression approaches [5]. This work demonstrates the partition of data into block followed by encryption and compression relating to the user preferences. At last, the data is stored on the distributed cloud environment in order to enhance the security strategy. The data is uploaded to the cloud service providers' end to retain the safe data and unauthorized users cannot modify the stored content.

The method elaborates the security operations of mobile devices, i.e. partitioning the data into multiple blocks, encryption/decryption of blocks and regenerating the original data as in figure 2. The service providers can only offers data storage alone. This process provides better security even when there is an un-trusted cloud and as well reduces the computational complexity of security operation.

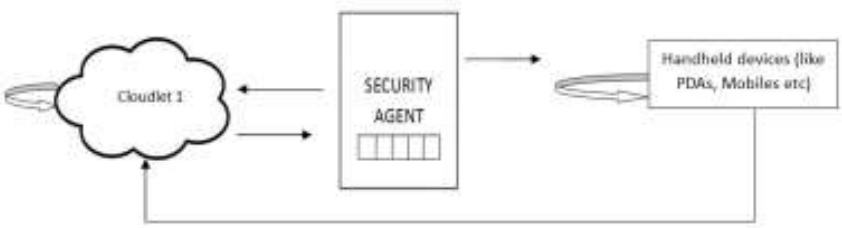

Fig 2: Representation of the proposed architecture

a. Architecture of First Level- Agent based Data Authenticity

1) Higher level security agent generates table to maintain the details of available cloudlet and generates unique ID along with the assessment of cloudlet availability.
2) Health care providers transmit READY status to offload application to higher level security agent. The agent maintains the MAC address of the received node in the generated table.
3) The security agent transmits MAC address to the cloudlet, subsequently, cloudlet ID is transmitted to the available node.

b. Architecture as Second Level- transmitting Encrypted Data from mobile Devices to Cloudlet

1) Agent transmits dynamically generated public key to cloudlet.
2) Cloudlet encrypts the data with available public key.
3) Health care provider (physician) transmits data to the cloudlets.
4) Higher level security agents transmits dynamically generated private key to cloudlet.
5) Cloudlet decrypts the received data from health care provider using private key.
6) Acknowledgement is transferred from cloudlet to the security agent, in order to maintain the time slot.

c. Architecture as Third Level - Sending encrypted data from Cloudlet to mobile Devices (physician)

1) Agent transmits dynamically generated public key to cloudlet.
2) Cloudlet encrypts the data with available public key.
3) Cloudlet transmits data to the health care provider (physician)
4) Higher level security agents transmits dynamically generated private key to health care provider.
5) Health care provider decrypts the received data from cloudlet using private key.
6) Acknowledgement is transferred to the security agent, in order to maintain the time slot.

4. Conclusion

A computation offloading is proposed based on offloading the tasks to other IoT devices for preserving and authenticating data related to health care system, in order to maintain the patients' privacy. Cloudlet is an efficient technique to relate the mobile devices to the cloud. Here, the physician can get the data of any patients in his device to achieve privacy with operating cloud in a speedy time slot. Hence, the delay in accessing the data is reduced. But, security of data leads to a major concern. The work utters about transmitting data to the cloudlet by maintaining a table to regulate the order. Based on encryption/decryption methods, the data transmitted among the physician and the cloudlet are regulated for integrity. This higher level agents provides security in two levels i.e., security for efficient transmission and privacy for data transmission over internet.

References

[1] K. Kumar and Y. H. Lu, "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?" Journal of Computer, vol. 43, no. 4, pp. 51–56, April 2010.

[2] A. Botta, W. de Donato, V. Persico, and A. Pescap, "Integration of Cloud computing and Internet of Things: A survey," Future Generation Computer Systems, vol. 56, pp. 684 – 700, March 2016.

[3] A. Aragues et al., "Trends and Challenges of the Emerging Technologies toward Interoperability and Standardization in E-Health Communications," IEEE Commun. Mag., vol. 49, no. 11, Nov. 2011, pp. 182–88.

[4] P. Belsis and G. Pantziou, "A k-Anonymity Privacy-Preserving Approach in Wireless Medical Monitoring Environments," J. Personal Ubiquitous Comp., vol. 18, no. 1, 2014, p. 6174.

[5] M. Z. A. Bhuiyan et al., "Deploying Wireless Sensor Networks with Fault-Tolerance for Structural Health Monitoring," IEEE Trans. Computers, vol. 64, no. 2, 2015, pp. 382–95.