Cloud Augmented Fogs for Industrial Internet of Things

N. P. Ponnuviji[1] and Dr. M. Vigilson Prem[2]
[1]Research Scholar, Department of Computer Science and Engineering,
R.M.D. Engineering College, Kavaraipettai, Tamil Nadu.
ponnuviji@gmail.com
[2]Professor, Department of Computer Science and Engineering,
R.M.D. Engineering College, Kavaraipettai, Tamil Nadu.
vigiprem@gmail.com

Abstract: Despite the heavy usage of cloud computing in various fields, the issues related to latency, support to mobility and location awareness remains unsolved. The term fog computing is also known as fogging or fog networking. The computing infrastructure is decentralized where data, compute, storage and applications can be distributed in an efficient place logically between the cloud and the data source. The fog computing extends cloud computing and services to the edge of the network. This brings the advantages and the strength of the cloud closer to where data has been created. The manufacturing industry gets sufficient benefits, when the industrial operators use the Industrial Internet of Things (IIoT), which in turn increases the productivity, revenue opportunities in business, etc. This survey paper discusses the access control, concepts, security and privacy issues of fog computing in the industry sector. It also highlights the challenges and opportunities, as part of future enhancements in the printing and publishing industry.

Keywords: Industrial Internet of Things (IIoT), Discretionary access control

(DAC), Mandatory access control (MAC), Role-based access control (RBAC), Attribute-based access control (ABAC), Usage-control-based access control (UCON), Reference monitoring access control (RMAC), Proxy re-encryption (PRE), Network Function Virtualisation (NFV), Real Time Publish Subscribe Protocol (RTPS), DDS (Data Distribution Service).

Introduction

In the past few years, cloud computing has played a prominent and important role in data storage and computing. The 'pay for use' model was introduced where the cloud became the delivery of on-demand computing resources from various applications to data centers. Many services were offered over the internet on the 'pay for use' way in order to scale and easily meet the demands of the user. With so many advantages, the few pitfalls of cloud are security threat, low bandwidth, location awareness and limited control [1]. In order to overcome these problems, the fog computing technology came into existence. We can term it as the enhancement of cloud computing taken to the edge of the networks.

The fog has no standard architecture, but acts as a system-level architecture making the cloud to the edge of the IIoT network [2]. It acts as an intermediate layer between the cloud and the user devices. Nowadays, various industries have started incorporating the fog model as a supplement to the cloud infrastructure. It also deals with various applications connected to the smart grid, vehicles, wireless sensor and actuator networks [3]. The use of numerous devices getting connected to network has been identified by 2 sources – device users and actuators / sensors. The sensing devices are placed everywhere virtually leading to the Internet of Things (IoT). Wearable computing devices, smart cities have paved way for the ubiquity of devices [4]. Apart delivering various models and playing roles there are some issues on security and privacy that is still a challenge in Fog [5].

This paper mainly focuses on the various access control methods, security and privacy issues on the network faced by using Fog computing in the industrial

sector. It highlights the purpose of fog computing in the printing and publishing sector as part of the future enhancement.

Related knowledge and research status

In Section 3, the paper discusses about the access control models and their essence in providing security to the Fog. These models help to design access control in fog.

It also highlights the characteristics of each access control model.

In Section 4, the paper further highlights the standard protocols used in Internet of Everything (IoE) [2]. It further explains how the layers are named in the IoE communication stack.

In Section 5, the paper elaborates an application scenario focusing on the use of wearable devices, smart glasses and how computation of video streaming is handled for data transmission, the battery and life span of such devices and the role of fog computing during data transmission [3][4].

In Section 6, the paper elaborately explains how data is searched before being outsourced to the fog node. It briefs about few searchable encryption schemes. The user performs the search over encrypted data with the help of keywords without decryption [5][6].

In Section 7, we have briefly discussed our proposed work that would be incorporated in the printing and publishing industry. It describes about how a cloud could be augmented in fog, for publishing textbooks.

In Section 8, we conclude the challenges faced in industries and mainly discuss on the challenges in the printing and publishing industry and also about the future enhancements that could be dealt to minimize the challenges.

Access Control Models in Fog Computing

There are various access models designed to provides solutions for applications in fog environment.

Discretionary Access Control (DAC) model: In this model, the data owner decides everything. The owner grants access permissions based on the user's identities for some groups. This model is considered more flexible but provides less security. This is widely used in UNIX operating systems.

Mandatory Access Control [MAC] model: This model has been designed depending on the requirement of user-resource mapping. This is well supported in the distributed system than the DAC model. It proposes two key rules – no-write-down and no-read-up to maintain confidentiality of the information.

Role-Based Access Control [RBAC] model: The RBAC allows the users to access objects in the system using their roles and the task assigned to them. The objects can be a smartphone or any wearable devices or systems. It is more scalable than the DAC and MAC and is well geared to be used in the fog or cloud environment. Tracking is not possible with fixed identities. All the models have been developed for allocated with static user permissions, whereas the relationship between the users and resources is dynamic in fog and cloud computing.

Attribute-Based Access Control (ABAC) model: This model permits the data owner directly to set the access policy in order to protect data privacy. It has been proposed to satisfy the security and flexibility of cloud computing. It is considered as fine-grained access control [1], where the data is related to access policies and users are assigned some attributes.

Usage Control-based Access Control (UCON) model: This model helps to manage sessions used by the users after access rights have been granted. The main characteristics includes with attribute mutability and attribute update, the evaluation of access decision as this model is based on patterns such as object, subject and environment properties.

Reference Monitoring Access Control (RMAC) model: This model comprises of a set of validation reference mechanisms. But this model is central-based traditional architecture and is considered unsuitable for fog computing.

Proxy Re-Encryption (PRE) model: It uses primitive cryptographic keys. The primary idea is to provide secure and efficient computing techniques in fog application.

ABE-Based Access Control model: In this model, the access policies are proposed only by the data owner on granting rights for user to access the kind of data.

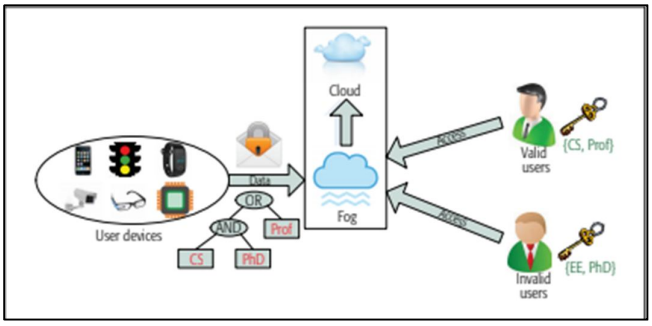

Figure 1. Scenario of ABE-Based Access Control

It satisfies the requirements of both cloud and fog in different security domains. Even though, the ABE-Based Access model suits for fog computing, the challenges on latency and policy management still pose hiccups.

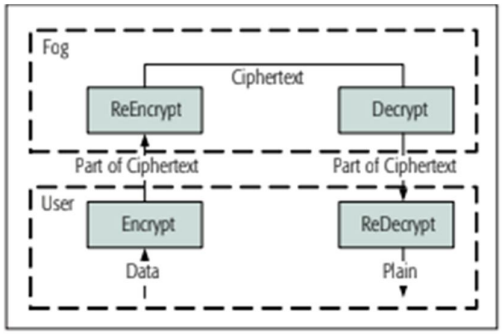

Figure 2. Outsourcing of CP-ABE-Based Access control

The heavy outsourcing in this model uses four algorithms – setup, keygen, encrypt, decrypt. Hence, this model supports both encryption and decryption outsourcing in fog devices.

Standard Protocols in Internet of Everything (IoE)

In this section, the communication stack of the IoE system and its standard protocols are discussed. The protocols are different for each layer of the IoE communication stack.

Table 1 Protocol Stack of Internet of Everything

SESSION / COMMUNICATION LAYER (CoAP, DDS, XMPP, HTTP, MQTT, etc.)
NETWORK / TRANSPORT LAYERS (IPv4, 6LoWPAN, IPv6, RPL)
DATA LINK LAYER (CDMA, RFID, Bluetooth, ZigBee, etc.)
PHYSICAL LAYER (USB, PLC, Wireless, etc.)

The main idea behind the IoE, IoT, IIoT is the communication. The Constrained Application Protocol (CoAP), allows less radiating sensors over the internet to communicate with the devices. The Message Queue Telemetry Transport (MQTT) is a light-weight packet that mainly saves both usage of memory and consumption of power. This protocol converts the telemetry data messages to communicate with the server at a later stage. Data Distribution Service (DDS) depends mainly on broker-less architecture. It is well-designed for communication between machines to integrate highly intelligent machines. The XMPP (Extensible Messaging and Presence Protocol) is decentralized in nature and helps communication and exchange of information between people and devices such as XML data, voice, video calls.

Device ubiquity on Augmented Reality (AR) and Real-time video analytics

The applications of augmented reality are popular on devices such as tablet, wrist watches, smartphones and smart glasses. Google Glass, Sony SmartEyeglass and

Microsoft HoloLens, Google StudyMarvel is dome of the projects based on the augmented reality. These applications require more power for computation to process the streaming of videos with high bandwidth for data transmission. But there tends to be huge delay in transmission due to the above mentioned factors. But fog computing provides necessary resources for computation and storage of captured video streams.

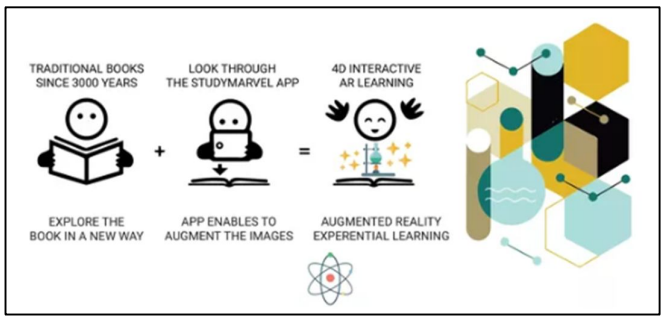

Figure 3. Traditional stages of learning to 4D interactive AR learning

The real-time processing and high-end video streaming are achieved with the help of fog computing. The privacy-preserving techniques can be incorporated at the fog end to ensure the personal privacy is protected in surveillance systems in public places. The augmented reality technique eases the learning in education sector as shown in Figure 3, making learning more interactive and practical among students.

Secure and Private Data search

The encryption is widely used to protect sensitive and private date from end users, before transmitted to the fog node. The foremost service is searching data through keyword search, among encrypted data files.

Searchable encryption schemes are devised that allows searching data through keywords without decrypting the data. This helps to achieve secure data transmission between Industrial IoT (IIoT) devices. Few other techniques such as homomorphism encryption allow aggregation of preserving privacy collecting

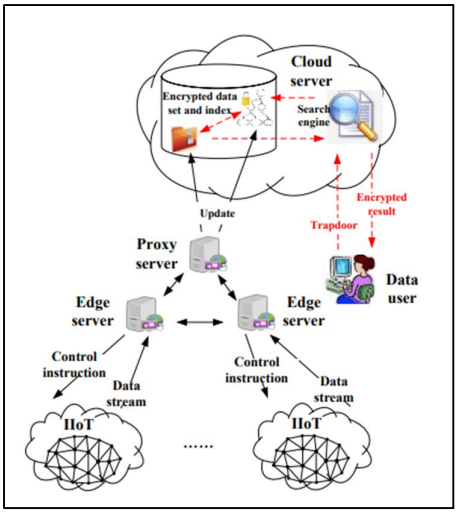

Figure 4. Data process, storage and retrieval in IIoT

sensitive data that is generated by the sensors in factories and end devices. This can be done at the local gateways without decryption [5].

In Figure 4, the IIoT data processing system consists of five main areas – IIoT, Edge server, Proxy server, Cloud server and Data users. The black arrows show the steps of collecting data, processing it and outsourcing it. The red arrows show the process of querying a data in a secured manner. It can be observed that the IIoT collects data from devices continuously and then transmits to the Edge server. Primarily it extracts the time-sensitive data, processes it from the edge server and finally drops the data when it is no longer needed for future use [6].

Proposed work

In this paper, we have made a detailed survey on variety of analysis that could be taken more suitable and incorporated for the printing and publishing industry. The scenario of printing textbooks in huge or bulk numbers would end up in a mess with confusions hovering around the subjects and the contents.

Collecting the raw document: The first step would be to collect the raw content from the author and check whether the document satisfied the standardization given. This would be taken care by the Editorial team.

Role of Production team: The content in the finalized edited format would be sent to the Production team, where it would be incorporated in the InDesign or similar publishing software.

Second and final-level checking of Editorial team: The content in InDesign would now be sent back to the Editorial team, where the wrapper, grammar, language, standardization and pagination will be checked and taken care. This process takes place between the Production and the Editorial team until the final content is reached. It would be reviewed by the author at the last stage.

Ready for Pre-print: At the end, the final document would be reaching its pre-print stage. The PDF would be created and sent to the printing press with the help of the IIoT devices.

Conclusion

The challenges lie on at every stage, in maintaining the bulk documents after every level of editing and flowing. The storage and security becomes more challenging, in handling appropriate document and its contents. When transmitting the files in bulk, it may lead to heavy network traffic, where in optimal algorithms need to be used. We are currently heading towards using a heuristic deployment algorithm [15] to minimize the challenges. Indirectly we have seen the eight pillars of fog computing – Security, Scalability, Openness, RAS (Recirculating Aquaculture System), Agility, Hierarchy and Programmability. The use of augmented reality in the field of education, in future will change the system of learning. Further planning on the logistics area would also be analysed after successful implementation at the printing level.

References

[1] Peng Zhang, Joseph K. Liu, et al., “A Survey on Access Control in Fog Computing”, IEEE Communications Magazine, February 2018, pp. 144-149.

[2] B. Chanakya, P. Sai Kiran, “A Comprehensive Survey of Fog Computing with Internet of Everything”, International Journal of Control Theory and Applications, vol. 9, ISSN: 0974-5572, 2016, pp. 99-106.

[3] Shanhe Yi, Cheng Li, Qun Li, "A Survey of Fog Computing: Concepts, Applications and Issues", ACM Mobidata '15, DOI: http://dx.doi.org/10.1145/2757384.2757397.

[4] Luis M. Vaquero, Luis Rodero-Merino, "Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing", ACM SIGCOMM Computer Communication Review, vol. 44, number 5, October 2014, pp. 27-32.

[5] Shanhe Yi, Zhengrui Qin, Qun Li, "Security and Privacy Issues in Fog Computing: A Survey", http://www.cs.wm.edu/~zhengrui/papers/wasa15-fog.pdf.

[6] Junsong Fu, et al., "Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing", IEEE Transactions on Industrial Informatics,, January 2018.

[7] J, Zheng et al., "The Internet of Things", IEEE Communications Magazine, vol. 49, no. 11, November 2011, pp. 30-31.

[8] "Cisco Fog Computing Solutions: Unleash the Power of the Internet of Things", Cisco 2015.

[9] Ahmed Banafa, "Fog Computing Vitsl for a Successful Internet of Things (IoT)", https://www.linkedin.com/pulse/fog-computing-vital-successful-internet-things-ahmed-banafa, 15 June 2015.

[10] Tara Salman, "Networking Protocols and Standards for Internet of Things", https://doi.org/10.1002/9781119173601.ch13.

[11] "IoT Standards and Protocols", www.postscapes.com/internet-of-things-protocols/

[12] CoAP Protocol – IETF Draft. http://tools.ietf.org/html/draft-ietf-core-coap-18 Accessed: August 2014.

[13] MQTT Protocol – OASIS Specification. http://www.oasis-open.org/committees/mqtt/ Accessed: August 2014.

[14] https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf

[15] Hua-Jung Hong, Pei-Hsuan Tsai, Chen-Hsin Hsu, Copyright IEICE – The 18th Asia-Pacific Network Operations and Management Symposium (APNOMS) 2016.

[16] Goiuri Peralta, et al., "Fog Computing Based Efficient IoT Scheme for the Industry 4.0", IEEE International Workshop of ECMSM, 15 June 2017.

[17] Maria Rita Palattella, et al., "Standardized Protocol Stack for the Internet of (Important) Things", IEEE Communications Surveys and Tutorials, vol.15, Issue:3, Third Quarter 2013.