A SURVEY PAPER ON CLOUD ENVIRONMENT IN EDGE/FOG COMPUTING TO UNDERSTAND THE INTELLIGENT SECURITY AND OPTIMIZATION

`Dr. J Bhuvana[1], AnanyaSaha[2],
[1]Associate Professor, Jain [Deemed to be]University, Bangalore
[2]Research Scholar, Jain [Deemed to be] University, Bangalore
Assistant Professor, The Oxford College of Science, Bangalore

ABSTRACT: Cloud computing validate the mobility support, location awareness and low visibility by misrepresenting the cloud resources and services to the outline. Researchers and the specialist have adopted the cloud computing as a new advance which has the capacity to subtle the impact in our day to day basis life and world's economy. Principally, security and privacy protection is one of the demanding concern in the improvement and modification of cloud environment in edge/fog computing. Company name cisco originated this fog computing as an alternative of cloud computing. Fog computing locates closure to the users in terms of storage and security.it is easier to capitalize on the existing computing power present in those devices. This improves user experience and reduces burdens on the cloud as a whole. To escape, the system delicacy and sustain against liability exploration from cyber attacker, different cyber security techniques and tools have been developed for cloud environment. This appropriate issue concerned on the demanding topic of Intelligent Security and Optimization in Cloud Computing and also inviting the state of the art of research outcomes.

Keywords: Cloud computing, fog computing, cyber security, Intelligent Security, Optimization in Cloud Computing

I] INTRODUCTION

Cloud computing, as the part of edge computing, has been growing rapidly in the past few decades. It serves users as absolute computing resources as ‘‘each thing-as-a-Service’’ [1–3] pattern. By adopting the services of cloud, users can approach nearly moderate computation resources by their claim from data centers of cloud. As huge amount of data used to upload into the centralized cloud platform, sometimes at single point of time, it creates network traffic as a result it cause the data. To implement this issue, researchers recommended a novel scheme, which directs the estimation task near the end of the network [5,6], to overcome the network traffic and computing pressure on cloud data centers. By the side of light but meaningful computation tasks formed by IoT devices can be solved in a real-time way[7,8].Cloud computing carried out at the peak of the network, which fully utilizing the resting of computer resources at the point of device to address the computational task narrowly. In terms of fog computing, to give a quick service by cloud computing to the mobile devices, such as smartphones, cloud data centers and users of cloud handles this computational task, In general, both edge /fog computing are important part to face the challenges in terms of failure to the available computation resources.

Despite of all, edge/fog computing paradigm are under the number of multiple threats.

Firstly, as user's different electronics devices, end devices are designed under economic friendly. Subsequently, those devices are too energetic and functionally strained to equipment the current security access [9,10]. Secondly, the layer of the network edges cannot be fully controlled and administered by the service providers. Hence, edge devices are disclosed to highly dynamic and uncertain environments that attract attackers [11]. Thirdly, communications between the edge devices are also decrepit to be settled. The attackers can remotely controlled the devices if they get connected with the malicious public Wi-Fi. Lastly, the data which are collected by different IoT devices can be possessed by the honest-and-interested service provider [12].

Therefore, this devices are not be fully protected and function able, vulnerable to the different thread agents and also due to lack of user's knowledge. The challenges in perspective of security in edge/fog computing now a days marked as checked list for the development and innovation of new applications of this next-generation computing scheme.

As a prominent technology which gives a profound encounter on the world, intelligent algorithms powering the security assertion process and also optimize the techniques that can surely beneficial for the edge/fog computing [13,14].

Altogether together the different innovative techniques not only promoting the interactions between multi disciplines but also bricking the academia and industrial knowledge. Therefore suggestion, is to collect the novel researches in different phases of security and optimization topic, then evaluate, discuss and improve the solutions that address the security issue in edge/fog computing.

In this survey, we had accepted 8 different highly quality based papers. Each of the papers has been remanded by the accurate review and evaluation process. The end decision taken by considering both the phases of research quality and balance dimension. This represents newly innovative solutions and showing the advance paths on the basis of security, privacy, polices, different models and their architectures in edge/fog computing; privacy in formation of network and managing the edges of computing and its functionality.

1. Special issue contents

In this section, we have discussed about the Future Generation Computer System Journal gathered papers by open call. Here in this paper, especially we noticed in publishing in FBCS Journalism 2018, from volume 85 to volume 90. As we have focused on below aspects, papers which are selected into this special issue are in high quality with covered multiple significant aspects moving towards traditional cartographical algorithm to machine learning based threat detection algorithm.

In the paper we mainly focused on ''Compulsory traceable cipher text-policy attribute-based encryption against privilege abuse in fog computing'' [15], authors noticed on how to define the privilege abuse problem in cipher text-policy attribute-based encryption (CAABE) under fog environment. This term was firstly introduced in this paper, which is referred as an unauthorized access to the fog data by the different promotions of spiteful users. Two kinds of privilege abused here. One is caused for illegal sharing of user's attribute key to unauthorized users, which takes to an unauthorized access to the sensitive data on fog node. And on the other hand kind of abuse was a result of illegal sharing of decryption device to an unauthorized users, were the sensitive cipher-text were under threat. Along with this unauthorized users, we cannot trace and monitored this kind of privilege abuse.

Now to address this issue, Qiao [15] suggested a novel black box traceable CP-ABE scheme to track the action of malicious users. By this we can identify the decryption key, which is used to build the black box decryption. Hence, providers started identifying the real owner for mentioned black box. Moreover, author also suggested a compulsory desirability idea to find out the difference between the normal cipher-text by malicious users. The proposed approach

was proved to be compulsory and be scalable and light-weighted to fit the fog environment.

Now a days data science and machine learning is rapidly growing, numbers of research interest were found in this domain specifically biometric based authentication system instead of normal traditional role based or attribute based system. Meanwhile biological data makes sure the security of the whole system, which users in person collects the data and upload it for identification, should not harm the user's privacy. It also ensures the security awareness for the whole system, users personal information used to collect and upload for identifying, which could be harm to user's privacy.

The titles "Edge-centric multi modal authentication system using encrypted biometric templates'' [16] discussed the dilemma above and designed a system to solve it. Mainly this system concentrate on the accuracy of biometric authentication. Under this speech recognition, it was evaluated by Mel-frequency cepstral coefficients and perceptual linear prediction coefficients, and facial recognition was measured by Eigen faces. To decide the authentication decision based on the three metrics, starting from user data privacy perspective, data was encrypted after collected by edge devices to provide data privacy and security.

The work ''PrivBox: Verifiable decentralized reputation system for online marketplaces'' [17] also paid attention to the user's privacy data that collected at the edge of network. The traditional online reputation system was designed in a form of centralized trusted system, which could leak the user's sensitive information in user's feedback comments. In this work, PrivBox, a decentralized reputation system was proposed. Homomorphism cryptographic system cooperated Dec. 2013with non-interactive zero-knowledge proof to ensure data privacy and well-formed ness with low computation complexity.

In this paper we surveyed ''Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model'' [18] by existing methods in protection for the new distributed and heterogeneous cyber systems. Authors also find out the first elaborated deficiency in security parameter model for edge/fog computing. And afterwards many challenges and future trends in edge/fog computing were discussed. Individually distributed system architectures developed from verticals to horizontal was fully discussed and divided into three logical layers. Finally, a threat detection framework was proposed at the end of this article.

In another paper, ''Secure data De-duplication using secret sharing schemes over cloud''[19], author discussed about the area of data security under cloud data De-duplication process. By using data De-duplication we can delete the repeated data information to increase the storage space in cloud environment, currently this de-duplication approaches are the key point vulnerability. To overcome this issue, both convergent key information and content information obfuscated into multiple shared based on Chinese Remainder Theorem. Broad researches identifies their model which could resist single point failure and ensure data confidentially and integrity. Apart from this, their model showed 25% percent of De-duplication rate that outperformed existing state-of-the-art performance.

As a substitute, constructing the protected mechanism of users data security, some suggested models were inactively recognized the threat agent and also proposed a punishment to those malware automatically.

The entitled paper ''Identifying cyber threats to mobile-IoT applications in edge computing paradigm'' [20], by Abawajy et al suggests a mobile malware detection model. In this, it started with the survey about the different malware problems, current mobile scenario and novel malware mobile phases. Here they listed the previous approaches about the both dynamic and static malware analysis, one is focused on challenges in detecting the malware practice in

mobile environment. These software, if its takes permission to access camera or memory space, it can cause the users privacy leakage. Author of this paper, concentrated on classified the malware, where the feature extractor and discriminators are trained under high numbers of labeled data. Evaluations carried out showed this model could effectively distinguish the malware.

Similarily, In Homayoun's paper work ''DRTHIS: Deep ransom ware threat hunting and intelligence system at the fog layer'' [21] to detect the mulware they used machine learning technologes. In this work, they also paid attention to the counter measure that ransom ware can encrypted user's personal data and carried out extortion.

By taking the risk to the sensitive data stored in fog nodes. Therefore, Deep Ransom ware Threat Hunting and Intelligence System (DRTHIS) model was proposed to find out multiple ransom ware in shorted time along with that is also tries to classify ransom ware and normal software. Here deep neural network is deployed to find the consistent of convolutional neural network and pertained long and short term memory network. Additionally softmax stage, starts producing the final clarification outcomes. As a first stage result, it shows the pre-trained LSTM was give preference compare to the CNN in detecting task. As a future research, for malware detection deep learning technology can be used.

Additionally we can add this edge/fog computing to support the wearable medical electronic devices. Due to the lowliness features of the fog computing, the fog based medical system was fast in rapid responses and energy preserving.

In paper ''Optimization of signal quality over compatibility in textile electrodes for ECG monitoring in fog computing based medical applications'' [22], authors suggested a novel fog-based wearable electrocardiogram (ECG) signals monitoring system. To optimize the EFG signal quality with high signal-to-the-noise ratio, textile electrodes were deployed.

Acknowledgments

We are thankful to all authors, various reviewers and editors for their continuous efforts to this special suggestion. We hope that the achievements gathered in this special issue will give a huge value to the world of cloud computing and readers from the worldwide.

References:

[1] A. Ferrer, J. Marquès, J. Jorba, Towards the decentralised cloud: Survey on approaches and challenges for mobile, ad hoc, and edge computing, ACM Comput. Surv. 51 (6) (2019) 111.

[2] K. Gai, M. Qiu, Z. Xiong, M. Liu, Privacy-preserving multi-channel communication in edge-of-things, Future Gener. Comput. Syst. 85 (2018) 190–200.

[3] K. Gai, Y. Wu, L. Zhu, L. Xu, Y. Zhang, Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks, IEEE Internet Things J. PP (99) (2019) 1–13.

[4] K. Gai, M. Qiu, H. Zhao, Energy-aware task assignment for mobile cyberenabledapplications in heterogeneous cloud computing, J. Parallel Distrib. Comput. 111 (2018) 126–135.

[5] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646.

[6] K. Gai, M. Qiu, H. Zhao, L. Tao, Z. Zong, Dynamic energy-aware cloudletbased mobile cloud computing model for green computing, J. Netw. Comput. Appl. 59 (2016) 46–54.

[7] P. Zhang, J. Liu, F. Yu, M. Sookhak, M. Au, X. Luo, A survey on access control in fog computing, IEEE Commun. Mag. 56 (2) (2018) 144–149.

[8] M. Qiu, M. Zhong, J. Li, K. Gai, Z. Zong, Phase-change memory optimization for green cloud with genetic algorithm, IEEE Trans. Comput. 64 (12) (2015) 3528–3540.

[9] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, H. Zhao, Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry,

Future Gener. Comput. Syst. 80 (2018) 421–429.

[10] K. Gai, M. Qiu, Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers, IEEE Trans. Ind. Inf. 14 (8) (2018) 3590–3598.

[11] K. Gai, M. Qiu, Z. Ming, H. Zhao, L. Qiu, Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks, IEEE Trans. Smart Grid 8 (5) (2017) 2431–2439.

[12] K. Gai, K. Choo, M. Qiu, L. Zhu, Privacy-preserving content-oriented wireless communication in internet-of-things, IEEE Internet Things J. 5 (4) (2018) 3059–3067.

[13] K. Gai, M. Qiu, Reinforcement learning-based content-centric services in mobile sensing, IEEE Netw. 32 (4) (2018) 34–39.

[14] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, Y. Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks, IEEE Internet Things J. (2018).

[15] H. Qiao, J. Ren, Z. Wang, H. Ba, H. Zhou, Compulsory traceable ciphertextpolicy attribute-based encryption against privilege abuse in fog computing, Future Gener. Comput. Syst. 88 (2018) 107–116.

[16] Z. Ali, M. Hossain, G. Muhammad, I. Ullah, H. Abachi, A. Alamri, Edgecentric multimodal authentication system using encrypted biometric templates, Future Gener. Comput. Syst. 85 (2018) 76–87.

[17] M. Azad, S. Bag, F. Hao, PrivBox: Verifiable decentralized reputation system for online marketplaces, Future Gener. Comput. Syst. 89 (2018) 44–57.

[18] R. Rapuzzi, M. Repetto, Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model, Future Gener. Comput. Syst. 85 (2018) 235–249.

[19] P. Singh, N. Agarwal, B. Raman, Secure data deduplication using secret sharing schemes over cloud, Future Gener. Comput. Syst. 88 (2018) 156–167.

[20] J. Abawajy, S. Hudal, S. Sharmeen, M. Hassan, A. Almogren, Identifying cyber threats to mobile-IoT applications in edge computing paradigm, Future Gener. Comput. Syst. 89 (2018) 525–538.

[21] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, K.-K.R. Choo, D.E. Newton, DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer, Future Gener. Comput. Syst. 90 (2019) 94–104.

[22] W. Wu, S. Pirbhulal, A. Sangaiah, S. Mukhopadhyay, G. Li, Optimization of signal quality over comfortability of textile electrodes for ECG monitoring in fog computing based medical applications, Future Gener. Comput. Syst. 86 (2018) 515–526.