 JIHPP, vol.1, no.1, pp.1-10, 2019

A Survey on Cryptographic Security and Information Hiding Technology for Cloud or Fog-Based IoT System

Liang Bai[1], Yuzhen Liu[1], Xiaoliang Wang[1, *], Nick Patterson[2] and F. Jiang[2]

Abstract: Internet of Things (IoT) is an emerging paradigm involving intelligent sensor networks that incorporates embedded technology for collecting data, communicating with external environments. Recently, cloud computing together with fog computing has become an important research area of the Internet of Things because of big data processing capabilities. It is a promising technology that utilizes cloud or fog computing / architecture to improve sensor computing, storage, and communication capabilities. However, recently it has been shown that this computing/architecture may be vulnerable to various attacks because of the openness nature of the wireless network. Therefore, it becomes more and more important to ensure the security and privacy in these scenes. Encryption security and information hiding technology can provide authentication, confidentiality, integrity, anti-eavesdropping, availability and so on for these computing models or architectures. The purpose of this review is to look for original articles with novel ideas and solutions to address encryption security and information hiding technologies in cloud or fog-based Internet of Things systems. We hope this review will provide an opportunity for scientists, researchers and industry engineers to study original manuscripts and know developments in all aspects of security, privacy, trust, and covert communication issues in cloud or fog computing/architecture Internet of Things systems.

Keywords: Internet of things, security, privacy protection, trust, Cloud, Fog.

1 Introduction

With the development of information technology, Internet of things (IoT) [Atzori, Iera and Morabito (2010)] is booming. IoT can connect sensors, controllers, machines, people and things together with the local networks or the Internet using wireless communications, which achieves information exchange, remote management control and intellisense [Kaur and Kaur (2017)]. This means that a large amount of data will be generated, and the management of sensitive outsourcing data will be a great challenge [Liu, Peng and Wang (2018)]. Cloud computing is a feasible method for dealing with big data storage and analysis. So the combination of the IoT and cloud computing forms a new computing paradigm called CoT [Aazam, Khan, Alsaffar et al. (2014)].

[1] School of computer science and engineering Hunan University of Science and Technology, Xiangtan, 411201, China.

[2] School of IT Deakin University, Melbourne 3125, Australia.

[*] Corresponding Author: Xiaoliang Wang. Email: fengwxl@163.com.

Although the CoT greatly improves data processing capabilities, this architecture is vulnerable to various attacks and causes some security problems because of the openness nature of wireless transmission channel [Shi (2018)]. In 2011, International Data Corporation (IDC) showed that 74.6% of corporate customers ranked safety as the main challenge. According to a report released by Forbes in 2015, security spending of CoT is expected to grow by 42%. From this we can see that the security of cloud based IoT will be more and more important. Gururaj Ramachandra et al. [Ramachandra, Iftikhar and Khan (2017)] points out several key issues to be paid attention on by CoT.

A. User access management privileged.

B. Compliance.

C. Data location.

D. Data isolation.

E. Data protection and recovery support.

F. Survey support.

G. Long term survival.

At the same time, the cloud security alliance (CSA) released the 12 top threats [IEEE Std., 2006] of cloud computing in 2016, which are as follows:

A. Data leakage.

B. Weak identity, credentials and access management.

C. Unsafe API.

D. System and application vulnerabilities.

E. Account was vulnerable.

F. Malicious insiders.

G. Advanced and continuous threat.

H. Lack of careful assessment and data loss.

I. Abuse of cloud service

J. Denial of service.

K. Privacy problems arising from sharing technology.

It is put forward to solve the problem of delay and sensitivity of cloud computing, fog computing [Sheltami, Shahra and Shakshuki (2018)]. However, there are many similarities between cloud and fog, so the fog computing/architecture in the IoT is also facing some security problems. This paper' s aim is to review the current researches and achievements in security area, and puts forward some suggestions for development. The main content of this paper contains encryption security and information hiding technology based on cloud and fog in IoT.

The following sections will be structured as follows: In Section 2 cloud and fog applications is introduced in the IoT. In Section 3 related works are presented about the cryptographic security of cloud or fog computing. In Section 4, integration is introduced for the cloud or fog-based IoT. The conclusion and expectation are proposed in Section 5.

2 Related applications based on Cloud or Fog

Nowadays, since the Cloud and Fog technology can provide new paradigms for the development of distributed, heterogeneous and complex systems that are characterized by large storage space, large amounts of data, high-end computing capabilities and interoperable networks, a system based on Cloud or Fog can provide different conveniences for IoT [Arfat, Aqib, Mehmood et al. (2017)]. In this section, we will analyze the application of cloud and fog in the IoT.

2.1 Related applications based on the Cloud

In the IoT, because of the storage and computing limitations of related devices as well as the big data processing requirements, cloud computing or cloud architecture are brought into IoT applications. Díaz et al. [Díaz, Martín and Rubio (2016)] present a survey of integrated components: cloud platforms, cloud infrastructures, and the middleware of IoT. At the same time, they also introduce existing data analytics techniques and integration proposals as well as address open research issues and challenges.

Although cloud computing and the IoT are two distinct technologies, they have become an integral part of our lives. The adoptions of both become increasingly common, making them an important part of the future Internet. The new paradigm of combining cloud computing with the IoT is seen as a breakthrough for some application scenarios. Botta et al. [Botta, de Donato, Persico et al. (2016] pay their attention to the integration of Cloud and IoT, forming a paradigm called Cloud IoT. Beginning with an analysis of the fundamentals of the IoT and cloud computing, they discuss their complementarities and describe in detail the factors driving their integration. Moreover, they identify some open issues and future directions in this field, which provide the prospect of the Future Internet.

Adopting the concept of combination of content-based image retrieval (CBIR) technology and cloud storage technology, Xia, Zhihua et al. [Xia, Lu, Qiu et al. (2019)] present a secure retrieval scheme for encrypted images in the YUV color space, which can help cloud users quickly access images and ensure the privacy of images.

Stergiou et al. [Stergiou, Psannis, Kim et al. (2018)] also combine cloud computing with the IoT to discover the benefits of integration. They think the integration can restrict and eliminate the need of hardware equipment and have some features such as energy efficiency, computationally capable. They also present security issues in IoT and Cloud Computing integration.

Younas et al. [Younas, Awan, Ghinea et al. (2018)] introduce new developments in cloud computing in the IoT. They speculate the cloud computing can provide new service level in the fields of enterprise, education, science, research and government organizations in the future.

The work of Boukerche et al. [Boukerche and De Grande (2018)] combine cloud computing with the emerging vehicle network in the IoT to form a vehicular cloud that will facilitate intelligent transportation systems.

Considering content-based image retrieval (CBIR) has been widely studied along with the increasing importance of images in daily life. Xia et al. [Xia, Xiong, Vasilakos et al. (2017)] propose a scheme dealing with the outsourcing of CBIR on the cloud servers. It

supports CBIR over the encrypted images without revealing the sensitive information to the cloud server.

2.2 Related applications based on Fog

Sheltami et al. [Sheltami, Shahra and Shakshuki (2018)] point out that cloud computing and its service models (SaaS, PaaS, and IaaS) and their features (such as on-demand services, fast resilience and scalability) still have many problems that prevent some applications from taking advantage of this computing paradigm. The latency, the long distance between the terminal and the cloud server may be the biggest problem for some real-time applications, such as online games and content delivery. As a new paradigm, fog computing can solve some problems of the cloud computing.

Aazam et al. [(Aazam, St-Hilaire, Lung et al. (2016)] point out that the Fog is a localized form of the Cloud that underlies IoT. By analyzing the behavior of nodes and estimating resources, it can provide solutions to those applications requiring fast response times and minimizing latency in the IoT.

Mutlag et al. [Mutlag, Ghani, Arunkumar et al. (2018)] introduce the advantages of fog computing in detail. Taking the field of medical care as an example, they analyze that fog computing is more suitable for real-time, high response time and low delay applications.

Vehicular ad-hoc networks (VANETs) are the symbolic applications of realizing the intellectualized city using IoT concept. Kai et al. [Kai, Cong and Tao (2016)] describe the growing interest about fog computing in VANETs due to the special requirements of mobility, location awareness and low latency of VANETs. The integration of fog computing and VANETs can provide more services at the edge of an IoT. This integration deploys highly virtualized computing and communication facilities near mobile vehicles so that these vehicles can obtain services with low latency and short distance connections through fog computing. The paper also introduces current research status and prospects of fog computing in VANETs.

3 Related works based on cloud or fog security

3.1 Related works based on cloud security

Khan [Khan (2016)] investigate security threats and corresponding security issues. They analyze and categorize the existing security problems and possible solutions in the literature. By the comparison of the different threats faced by the different cloud platforms, various intrusion detection and prevention frameworks are suggested to solve security problems. It also analyzes the security mechanism between trusted cloud computing and cloud service providers. In addition, the future direction is put forward for cloud security and its possible countermeasures.

Yang et al. [Yang, Han, Huang et al. (2018)] propose a new scheme called FREDP (File Remote Keying Encryption and Data Protection). The proposal involves three party interactions between mobile terminals, private cloud and public cloud. Private clouds share ciphertext files to the public cloud until the mobile terminal and trusted third-party private clouds complete the encryption of plaintext files using a remote keying encryption algorithm. In order to ensure the security of mobile terminals when using data, as a third

party, private cloud periodically verifies the integrity of data in the public cloud. Finally, the mobile terminal and the private cloud decrypt the ciphertext file, allowing the mobile terminal users to use the data.

Potey et al. [Potey, Dhote and Sharma (2016)] focus on the security of data storage in the Cloud. They use fully homomorphic encryption formats to keep data. These data are stored in the DynamoDB of the public cloud of Amazon Web services (AWS). The data processes are performed on encrypted form in public cloud and the result of data process can be downloaded on the client machine. In this proposal, user's data will never be stored in the public cloud in plain text so that it ensures user's data security.

The work of Praveen et al. [Praveen, Kumar and Pja (2018)] makes a comprehensive investigation of various existing key policies and ciphertext policy attributes based encryption schemes using access structures and multi-privilege algorithms. In addition, the author also discusses the encryption of policy attributes of encrypted text, such as hiding strategy, proxy encryption, revocation mechanism and encryption based on hierarchical attributes. This paper proposes a new attribute based on encryption method.

Singh et al. [Singh and Raman (2018)] propose a reversible data hiding scheme based on Shamir's secret sharing, which performs legal ownership verification in the encrypted domain. It blurs the cover information by spreading the information among random stocks and embedding owner-specific secret information into some encrypted stocks before outsourcing the media information to the cloud server.

Benarous et al. [Benarous and Kadri 201] provide a way to protect security, privacy, and authentication on future Vehicular Ad hoc Networks (VANETs) in terms of resource sharing and on-board cloud deployment. This approach effectively improves the security of cloud computing over VANET.

The convenience of cloud computing has attracted smart campus to outsource their huge amount of data to cloud servers. Although the outsourcing of data can reduce the computational and storage burden on smart campus, the privacy preserving becomes the biggest concern. Xia et al. [Xia, Ma, Shen et al. (2018)] propose an effective and practical privacy-preserving computation outsourcing protocol for the local binary pattern (LBP) feature over huge encrypted images.

3.2 Encryption security and information hiding technology in fog computing

In Wang et al.'s [Wang, Zhang, Bhuiyan et al. (2018)], a hierarchical trust mechanism based on fog is proposed to solve the defects of trust mechanism in order to solve these network security defects. Moreover, the scheme performs well in saving network energy, quickly detecting malicious nodes and recovering misjudged nodes.

Wang et al. [Wang, Wang and Domingo-Ferrer (2018)] propose the concept of anonymity and security aggregation schemes (ASAS) in fog-based public cloud computing. They not only use pseudonyms to hide and protect the identity of terminal devices, but also use homomorphic encryption technology to ensure data security.

Wang et al. [Wang, Liu and Sun (2017)] propose a secure, privacy-preserving navigation scheme using fog-based VANET onboard space crowdsourcing. Fog nodes are used to generate and release crowdsourcing tasks, and to collaborate with finding the best route

according to the real-time traffic information collected by vehicles in their coverage area. At the same time, vehicles carrying out crowdsourcing tasks can be reasonably rewarded. When the query vehicle enters its coverage area, the navigation results can be retrieved from each fog node in turn. And the next fog node can be reached according to the best route until it reaches the desired destination. The scheme satisfies the security and privacy requirements of authentication, confidentiality and conditional privacy protection. Some encryption primitives, including Elgamal encryption algorithm, AES, random anonymous credentials and group signatures, achieve this goal.

Piao et al. [Piao, Shi, Yan et al. (2018)] propose a framework for differentiated privacy in the publication of government statistics based on fog computing. On this basis, a data publishing algorithm using MaxDiff histogram is developed, which can be used to protect user privacy based on fog computing. Applying differential method, Laplace noise is added to the original data set, and even if the attacker gains strong background knowledge.It can also prevent citizens' privacy leakage. According to the maximum frequency difference, the adjacent data boxes are grouped, and then a differential privacy histogram with minimum mean error is constructed.

4 The security of integration of cloud and fog

Because cloud computing, fog computing and the IoT all have their own security problems, the cloud or fog-based IoT system which combines them may also have similar security problems in cloud computing, fog computing and the IoT. Based on cloud or fog, there are security problems in the IoT system.

Stergiou et al. [Stergiou, Psannis, Gupta et al. (2018)] regard there are many security and privacy holes in providing more green and sustainable computing to protect the ability of cloud computing (CC) infrastructure to process data in fog. A new cloud computing system is proposed, which integrates the IoT as the basic scenario of big data. In addition, the article tries to build a framework to protect network security and improve security. The proposed solution is to install a security wall between cloud servers and the Internet in order to eliminate privacy and security issues.

Bousselham et al. [Bousselham, Abdellaoui and Chaoui (2017)] ensure security and privacy, a new security approach is designed using software-defined network (SDN) technology, using pseudonyms, key management, and revocation lists to provide authentication, confidentiality, integrity, and availability.

Chen et al. [Chen, Lin, Castiglione et al. (2016)] protect the anonymity of passengers and ensure the robustness of payment systems, a new smart card-based MoD payment solution is proposed for mobile cloud authorized public transport systems, which not only ensures the anonymity of passengers, but also uses personal trust devices to protect passengers. Sensitive information so that he can enjoy multimedia content during long travel.

Hussain et al. [Hussain, Rezaeifar, Lee et al. (2015)] propose a novel security and privacy-aware service called traffic information at the top of the cloud computing stack to prevent opponents from abusing user privacy and/or building profiles for target users. In addition, for location confidentiality and privacy, a novel location-based encryption technology is proposed, which can prevent internal and external attackers from

manipulating the content of messages. In addition, the proposed TIaaS retains conditional privacy, and with the help of an effective revocation mechanism, revocation agencies can revoke any node in case of dispute.

Libing et al. [Wu, Chen, Choo et al. (2018)] propose an efficient and secure searchable encryption protocol using the active gate permutation function (TPF). The protocol is designed for cloud-based IoT (also known as the "Internet of Things"), such as cloud computing on the battlefield and military clouds. Compared with other existing SE protocols, the proposed SE protocol has lower computational cost.

5 Conclusion

Through the above article, we discuss the security issues of cloud or fog-based (IoT) systems, including (1) Using pseudonyms, key management and revocation lists to provide authentication, confidentiality, integrity and availability. (2) Install safety wall to eliminate privacy and safety problems. (3) Ensure the anonymity of users based on smart cards. (4) Key technologies such as data encryption and hiding technology. This paper briefly analyzes the current research situation in various technical fields, and discusses the issues needing further study in view of the existing problems.

Therefore, in the cloud or fog-based IoT system, we need to learn more from the security problems and solutions of each individual in the three to enhance the security of cloud or fog-based IoT system.

The future of cryptographic security and information hiding technology in cloud or fog-based (IoT) systems will depend on the following areas: (1) The expansion of application patterns: providing "cloud or fog security components". (2) Encryption technology advances: protection of user privacy authentication, confidentiality, integrity, and availability. (3) Strengthening of hardware devices: enhancing the firewall capability of cloud devices. (4) The authority and credibility of the third party trustworthy institutions. (5) Mature use of IoT based on cloud or fog.

Acknowledgement: This work was supported by Cooperative Education Fund of China Ministry of Education (201702113002, 201801193119); Hunan Natural Science Foundation (2018JJ2138), Excellent Youth Project of Hunan Education Department (17B096), the H3C Fund of Hunan Internet of Things Federation (20180006) and Degree and Graduate Education Reform Project of Hunan Province (JG2018B096).

References

Aazam, M.; Khan, I.; Alsaffar, A. A.; Huh, E. (2014): Cloud of things: integrating internet of things and cloud computing and the issues involved. *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology*, pp. 414-419.

Aazam, M.; St-Hilaire, M.; Lung, C. H.; Lambadaris, I. (2016): MeFoRE: QoE based resource estimation at Fog to enhance QoS in IoT. *23rd International Conference on Telecommunications*, pp. 1-5.

Arfat, Y.; Aqib, M.; Mehmood, R.; Albeshri, A.; Katib, I. et al. (2017): Enabling smarter societies through mobile big data fogs and clouds. *Procedia Computer Science*, vol. 109, pp. 1128-1133.

Atzori, L.; Iera, A.; Morabito, G. (2010): The internet of things: a survey. *Computer Networks*, vol. 54, no.15, pp. 2787-2805.

Benarous, L.; Kadri, B. (2017): Ensuring privacy and authentication for v2v resource sharing. *Seventh International Conference on Emerging Security Technologies*, pp. 1-6.

Botta, A.; de Donato, W.; Persico, V.; Pescapé, A. (2016): Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, vol. 56, pp. 684-700.

Boukerche, A.; De Grande, R. E. (2018): Vehicular cloud computing: architectures, applications, and mobility. *Computer Networks*, vol. 135, pp. 171-189.

Bousselham, M.; Abdellaoui, A.; Chaoui, H. (2017): Security against malicious node in the vehicular cloud computing using a software-defined networking architecture. *International Conference on Soft Computing and its Engineering Applications*, pp. 1-5.

Chen, C. L.; Lin, Y. F.; Castiglione, A.; Palmieri, F. (2016): A secure payment system for multimedia on demand on mobile VANET clouds. *Security and Communication Networks*, vol. 9, no. 17, pp. 4378-4390.

Díaz, M.; Martín, C.; Rubio, B. (2016): State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer Applications*, vol. 67, pp. 99-117.

Hussain, R.; Rezaeifar, Z.; Lee, Y. H.; Oh, H. (2015): Secure and privacy-aware traffic information as a service in VANET-based clouds. *Pervasive and Mobile Computing*, vol. 24, pp. 194-209.

IEEE Std. (2006): 1609.2-2006-IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management.

Kai, K.; Cong, W.; Tao, L. (2016): Fog computing for vehicular Ad-hoc networks: paradigms, scenarios, and issues. *Journal of China Universities of Posts and Telecommunications*, vol. 23, no. 2, pp. 56-96.

Kaur, J.; Kaur, K. (2017): A fuzzy approach for an iot-based automated employee performance appraisal. *Computers, Materials & Continua*, vol. 53, no. 1, pp. 23-36.

Khan, M. A. (2016): A survey of security issues for cloud computing. *Journal of Network and Computer Applications*, vol. 71, pp. 11-29.

Liu, Y.; Peng, H.; Wang, J. (2018): Verifiable diversity ranking search over encrypted outsourced data. *Computers, Materials & Continua*, vol. 55, no. 1, pp. 37.

Mutlag, A. A.; Ghani, M. K. A.; Arunkumar, N.; Mohamed, M. A.; Mohd, O. (2018): Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, vol. 90, pp. 62-78

Praveen, P. K.; Kumar, P. S.; Pja, A. (2018): Attribute based encryption in cloud computing: a survey, gap analysis, and future directions. *Journal of Network and Computer Applications*, vol. 108, pp. 37-52.

Piao, C.; Shi, Y.; Yan, J.; Zhang, C.; Liu, L. (2018): Privacy-preserving governmental data publishing: a fog-computing-based differential privacy approach. *Future Generation Computer Systems*, vol. 90, pp. 158-174

Potey, M. M.; Dhote, C. A.; Sharma, D. H. (2016): Homomorphic encryption for security of cloud data. *Procedia Computer Science*, vol. 79, pp. 175-181.

Ramachandra, G.; Iftikhar, M.; Khan, F. A. (2017): A comprehensive survey on security in cloud computing. *Procedia Computer Science*, vol. 110, pp. 465-472.

Sheltami, T. R.; Shahra, E. Q.; Shakshuki, E. M. (2018): Fog computing: Data streaming services for mobile end-users. *Procedia Computer Science*, vol. 134, pp. 289-296.

Shi, C. (2018): A novel ensemble learning algorithm based on ds evidence theory for iot security. *Computers, Materials & Continua*, vol. 57, no. 3, pp. 635-652.

Singh, P.; Raman, B. (2018): Reversible data hiding based on Shamir's secret sharing for color images over cloud. *Information Sciences*, vol. 422, pp. 77-97.

Stergiou, C.; Psannis, K. E.; Gupta, B. B.; Ishibashi, Y. (2018): Security, privacy & efficiency of sustainable cloud computing for big data & IoT. *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174-184

Stergiou, C.; Psannis, K. E.; Kim, B. G.; Gupta, B. (2018): Secure integration of IoT and cloud computing. *Future Generation Computer Systems***,** vol. 78, pp. 964-975.

Wang, H.; Wang, Z.; Domingo-Ferrer, J. (2018): Anonymous and secure aggregation scheme in fog-based public cloud computing. *Future Generation Computer Systems*, vol. 78, pp. 712-719.

Wang, L.; Liu, G.; Sun, L. (2017): A secure and privacy-preserving navigation scheme using spatial crowdsourcing in fog-based VANETs. *Sensors*, vol. 17, no. 4, pp. 668.

Wang, T.; Zhang, G.; Bhuiyan, M. D. Z. A.; Liu, A.; Jia, W. et al. (2018): A novel trust mechanism based on fog computing in sensor-cloud system. *Future Generation Computer Systems.*

Wu, L.; Chen, B.; Choo, K. K. R.; He, D. (2018): Efficient and secure searchable encryption protocol for cloud-based internet of things. *Journal of Parallel and Distributed Computing*, vol. 111, pp. 152-161.

Xia, Z.; Lu, L.; Qiu, T.; Shim, H.; Chen, X. et al. (2019): A privacy-preserving image retrieval based on ac-coefficients and color histograms in cloud environment. *Computers, Materials & Continua*, vol. 58, no. 1, pp. 27-44.

Xia, Z.; Ma, X.; Shen, Z.; Sun, X.; Xiong, N. N. et al. (2018): Secure image LBP feature extraction in cloud-based smart campus. *IEEE Access*.

Xia, Z.; Xiong, N. N.; Vasilakos, A. V.; Sun, X. (2017): EPCBIR: an efficient and privacy-preserving content-based image retrieval scheme in cloud computing. *Information Sciences*, vol. 387, pp. 195-204.

Yang, L.; Han, Z.; Huang, Z.; Ma, J. (2018): A remotely keyed file encryption scheme under mobile cloud computing. *Journal of Network and Computer Applications*, vol. 106, pp. 90-99.

Younas, M.; Awan, I.; Ghinea, G.; Grønli, T. M. (2018): Editorial: new developments in cloud and IoT. *Future Generation Computer Systems*, vol. 86, pp. 723-725.