INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of Second International Conference on Innovation in Engineering Sciences (ICIES-2021)

A Review on Data protection and privacy in Fog Computing Network

Babitha M N[1], Dr. M Siddappa[2]
[1]Research Scholar, Dept., of Computer Science and Engineering, Sri Siddhartha Institute of Technology Tumakuru , Karnataka, India.
[2]Research Guide, Dept., of Computer Science and Engineering, Sri Siddhartha Institute of Technology Tumakuru , Karnataka, India.
babithamn@ssit.edu.in[1], siddappa.p@gmail.com[2]

Abstract

Fog computing involves processing at network edge before the data is moved to core network or centralized clouds. Especially with grow of billions of *IoT* devices, Fog computing processing at network edge has many advantages in the form of efficient data processing, ability to react the event quickly, reduction in networking bandwidth and reduction in storage size at cloud etc. The advantages come with a risk in terms of data security and information leakage. With computing at network edge, the breach on privacy of data generator is also a severe risk. These works studies the existing solutions for information protection in and secure information processing as well as load balancing at network edges of Fog computing network. The goal of this work is to identify the open areas in information protection and load balancing on Fog computing network.

Keywords: Edge computing, Fog computing, Internet of Things, Load balancing.

1. Introduction

Cloud computing enables computing to moved at virtual machines at data centers there by providing resources on demand. Internet of Things (IoT) allows devices to be connected to internet for different applications such as smart industries applications, smart cities, smart agriculture, smart healthiness, etc. Growth in semiconductor industry has increased rapidly small devices with powerful processing ability and network capabilities getting connected to IoT network in larger scale. Cloud data centers are at the backbone of IoT network with storing and processing of large volumes of data generated by IOT devices. Use of cloud computing for data processing on IOT device data incurs huge network overhead and processing delay. This could have been reduced, if the processing nodes are located near the network edge close to the devices. Fog computing is an evolution of Cloud computing in this direction of proximity of data processing near network edges instead at centralized servers of cloud. Compared to cloud computing, Fog computing has an advantage in terms of significantly lower data transfer latency, which is one of the most important requirements for time-critical applications. There is plenty of opportunities for attackers to gain access or even manipulate sensitive information in case of Fog computing. Although some of the threats originate from cloud implementation, some are new to Fog computing and unique to it. The data privacy and security problems impede the adaptation of Fog Computing. Fog computing has many characteristics that make data protection more challenging than that of cloud computing. Each of the characteristics are listed

Reduced physical protection	Due to wild deployment of Fog computing, malicious attackers can get easier access into Fog computing nodes.
Direct access to confidential information	Attacker can reroute device data to itself by using the location proximity in Fog computing and can use the sensitive data for his needs
Resource scarcity	Cryptographic data protection and obfuscation methods are computationally complex and require more resources. But end devices in Fog computing are resource limited.

With the above factor, providing data privacy and protection is very challenging in Fog computing environment compared to Cloud environment. Many techniques have been proposed in literature review of data privacy and protection in Fog computing environment. In this survey, we study the existing data protection schemes in Fog computing in detail and identify open issues for further refinement.

2. Survey

In [1] authors, presented the case for implementing the data protection is a adaptive manner. This work activates data protection only at needed times to minimize the resource consumption and it selects the more suitable protection mechanism from many choices depending on the data sensitivity and current fog configuration. Author also addressed the challenges to realize adaptive data protection in Fog computing. The adaption policy is only based on resource availability rather than sensitivity of the data in [2] authors considered the problem of privacy in location of the user for mobile edge clouds (MECs). MEC's are minimal version of clouds located in close locality to users. Their offering is similar to that of Fog computing. Chaff service is applied to defend against malicious eavesdropper from tracking the location of the user. The eavesdropper is prevented from gaining access to user location by selection of optimal strategy for variation of location. This approach is not scalable. Authors in [3] identified the key challenges in secure sharing of data for the case of Fog computing environment. It is defined by designing a policy management framework to enforce the specification expressed in the form of relevant schemas. A proof of concept implementation is done to check the feasibility of the framework. The policies are mentioned in the form of conditions on time, user profile attributes etc and decision on policy condition is grant or deny. The work did not consider the case of malicious attacker presence in the network, and there is more chance for policy enforcement node is exposed to attack. But it adopts Dynamic policy configuration The work in [4] designed a novel framework to enforce access control on patient health records stored in cloud. The patients records are encrypted using ABE (Attribute Based Encryption) and only user with valid attribute values can decrypt the patient record. The key management and key distribution need to be revised for the case of Fog computing. It supports Authenticate and efficient load balancing but not considered light weight security.

Data compression was used as the strategy for data protection in [5]. The data from Fog computing to Cloud node is sent in a compressed form for enhanced safety and reduced network bandwidth. Using compression for data protection is not secure against inference attacks. Authors in [6] proposed ECQV Implicit Certificates and Datagram Transport Layer Security (DTLS) protocol for security in IOT. Mutual authentication between devices is done using Elliptic curve cryptography based ECQV implicit certificate and key exchange. After authentication, the data is encrypted using the key generated using ECQV and transferred using Datagram Transport Layer Security (DTLS). Fine grained access control on data is not supported in this work. A fuzzy IBE (Identity Based Encryption) is proposed in [7]. It is designed for highly secure transmission of data in IOT networks. The model is very secure and more suitable for IOT due to short public parameters. Processing on encrypted data is impossible in this method as result decryption is needed for any computations at network edge. A light weight Homomorphic encryption with minimum computations for encryption and key generation is proposed in [8]. This light weight Homomorphic encryption is more suitable for Fog computing as operations can be done on the encrypted data and due to low complexity, response time is not

increased. Public auditability for data security in cloud is considered in [9]. Integrity of the data stored in cloud is ensured by a third party auditor. It checks for any data tampering at frequent intervals and alert the data owner. A role based encryption (RBE) scheme is proposed in [10]. Cryptographic techniques along with role based access control are used in this work. Another contribution in this work is use of hybrid cloud involving both public and private cloud. Based on data sensitiveness, the data is redirected to public or private cloud. The only problem when applied to Fog computing is that computations becomes difficult in this solution. Direct Anonymous Attestation (DAA) protocols for selectively hiding sensitive information before data transfer and integrity verification at receiver end is proposed in [11]. The authentication of the hidden attributes can be verified easily in this method. Transmitting sensitive information to Fog computing nodes using DAA will ensure data privacy and data integrity, but a fixed attestation policy opens up chances of inference attack. A data perturbation method is proposed in [12]. It is light weight and based on pseudo random perturbation. The data is perturbed at device end before transmitting to Fog computing nodes. The work assumes a reputed trust relationship between device and Fog computing node but the scheme fails for internal attackers in Fog network. Author in [13] proposed a model for ABE with outsourced decryption which is CCA (chosen cipertext attacks) secure. The security is realized using non transformable public key encryption. Due to this decryption has to be done only once at storage end. A single key based access on multiple mobile cloud services using the concepts of bilinear pairing cryptosystem with dynamic nonce generation is proposed in [14]. Communication and computation time is reduced I in this approach. A single key based access would be more useful in scenario of Fog computing to process the data by multiple network edge nodes but the scheme needs appending of audit logs to track the modification history. A light weight mutual authentication scheme is proposed in [15] and it is based on ECC. Without the need for a trusted third party authentication is realized with additional advantage in terms of privacy and anonymity. This scheme would be more suitable for Fog computing nodes and IoT devices to mutually authenticate before data exchange. Authors in [16] suggested a secure framework for cloud storage. It is a three-layered security framework consisting for firewalls and access control at lowest layer, identify management at second layer and encryption at third layer. A distributed model of CCAF would be more suitable for Fog computing. In [17] authors proposed a secure framework for IOT. It uses SDN based management of Fog Nodes at edge computing layer and blockchain for key management. The approach is able to reduce the latency in IOT applications. As part of work, a data offloading algorithm is proposed.. The algorithm is able to manage the processing time at SDN switches. The solution considers only IOT device authentication before communication in the SDN network and data security is not considered. Authors in [18] proposed a novel secure middleware architecture for Fog and Cloud integrated environment, the middleware preprocess data at network edge. The data is processed locally or sent to cloud depending on the decision made by the middleware. The middleware is able to offload computation and security from resource constrained IOT devices thereby enhancing the computation capacity of the IOT Network. single point of failure and deployment architecture for the middleware is not considered in this work. In [19] new policy for load balancing was proposed which increases throughput, network utilization, data consistency but they are not considered data security

3. Issues

The open issues in the existing solutions for data and information security in Fog computing environment is listed below

1. In Middleware based solution, deployment strategy for middleware and how to handle single point of failure is not considered
2. Most of the solution are not secure against insider attacks
3. Adaptive attribute level security on data with support for operations on encrypted data is not considered
4. Protection of data from being routed to malicious attackers is not considered.

5. Accountability on the operation done by different edge components in Fog is not considered in any of the solutions.

4. Discussion on Open Issues

Issue 1: In middleware based security solutions, the strategy for placement of middleware, scalability of the solution and how to handle the single point of failure in the middleware and ensuring fault tolerance is not considered in any of the existing solutions.

Issue 2: Insider attacks are a serious problem in Fog computing environment. The attacker can steal and tamper the data. Also it can be used to compromise the user data privacy and user location privacy. Protecting against insider attacks is not considered in any of the previous solution.

Issue 3: Adaptive data protection is best strategy to be adopted in Fog environment to reduce the latency and computational complexity. Providing adaptive data protection with support for operations on encrypted sensitive data is needed to realize the full potential of Fog computing.

Issue 4: The data from IOT devices can be redirected to malicious attackers exploiting the proximity property in Fog environment. Protection against it has not been considered in any of previous works.

Issue 5: Accountability on the computations did on data is lacking in many solutions for Fog computing environment.

5. Proposed Work

The existing security solutions are not sufficient to protect data in fog platform there is a chance of Improving the performance by providing solutions to data integrity, insider attack, resource access policy management, user encryption and authentication.

- Significant monitoring technique is necessary to efficiently and productively able to monitor, analyze, plan fog computing.
- Optimization algorithm must be extended that can efficiently manage with decision making on the different foglets.
- A efficient and self adaptive data analytics technique is expected in fog computing to identify sensitive user data.
- The technique of Collecting, preprocessing and analyzing data must be improved at foglets.
- Light weight security techniques must be adopted for improving load balancing.
- Intrusion Detection Scheme IDS can be built on the fog node by tracking and analyzing the log file to detect disruptive actions, which mitigates insider attack.
- Using flexible attestation method is necessary to maintain accountability of user data computation.
- The use of ABE Attribute Based Encryption within fog nodes appears to be an interesting solution for meeting data protection requirements, according to the study [19].

Conclusion

Fog computing comes off as the bridge between the rise of the IoT and upcoming applications. The contribution of the architecture of the fog will solve a variety of issues. The existing solutions are not sufficient to protect the data and privacy. The paper summarizes the current works in data protection and security in Fog computing environment has been detailed and the problems in each solution are documented. The open areas for further search on providing data security and protection are listed with discussion on the issue and prospective solution for those issues. Further work will be on design on efficient solutions to address the identified open issues.

References

[1]. Zoltan Adam Mann, "Data protection in fog computing through monitoring and adaptation", Fog Computing 2018, Technical Report, TechnischeUniversity¨at Wien, pp. 25-28, 2018.

[2]. T. He, E. N. Ciftcioglu, S. Wang, and K. S. Chan, "Location privacy in mobile edge clouds: A chaff-based approach," IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2625–2636, 2017

[3]. C. Dsouza, G. J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in 2014 IEEE 15th International Conference on Information Reuse and Integration (IRI), pp. 16-23, 2014.

[4]. Ming Li,Shucheng Yu,KuiRen, Wenjing Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings",International Conference on Security

and Privacy in Communication Systems,2010

[5]. DubeyH, YangJ, ConstantN, AmiriAM, YangQ,MakodiyaK(2015)Fogdata:enhancingtele health bigdata through fogcomputing. In: ProceedingsoftheASEBigData&SocialInformatics2015.ACM.p14

[6]. An Ha, Duy&Tho Nguyen, Kha&Zao, John. (2016). Efficient authentication of resource-constrained IoT devices based on ECQV implicit certificates and datagram transport layer security protocol. 173-179. 10.1145/3011077.3011108..

[7]. MaoY, LiJ, Chen MR, LiuJ, XieC, ZhanY "Fully secure fuzzy identity-based encryption for secure IoT communications."Comput Standards Interfaces, 2016,44:117–121.

[8]. M.R.Baharon, Q.Shi, D.Llewellyn-Jones ,"A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing",2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications.

[9]. C. Wang, Q. Wang, K. Ren, W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing", Proc. 29th IEEE Int. Conf. Compute.Commun. (INFOCOM), pp. 1-9, Mar. 2010.

[10]. L. Zhou, V. Varadharajan, M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage", IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947-1960, Dec. 2013

[11]. L. Chen, R. Urian, "DAA-A: Direct anonymous attestation with attributes", Proc. 8th Int. Conf. Trust Trustworthy Comput. (TRUST), pp. 228-245, Aug. 2015.

[12]. M. Bahrami, M. Singhal, "A light-weight permutation based method for data privacy in mobile cloud computing", Proc. 3th IEEE Int. Conf. Mobile Cloud Compute. Services Eng. (Mobile Cloud), pp. 189-198, Mar./Apr. 2015.

[13]. C. Zuo, J. Shao, G. Wei, M. Xie, M. Ji, "CCA-secure ABE with outsourced decryption for fog computing", Future Generat.Comput. Syst., vol. 78, pp. 730-738, Jan. 2018.

[14]. L. Tsai, N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services", IEEE Syst. J., vol. 9, no. 3, pp. 805-815, Sep. 2015.

[15]. K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication", Future Generat. Comput. Syst., vol. 81, pp. 557-565, Apr. 2018

[16]. Chang V, Ramachandran M (2016) Towards achieving data security with the cloud computing adoption framework. IEEE Trans ServComput 9(1): 138–151.

[17]. AmmarMuthanna,Abdelhamied A. Ateya, "Secure IoT network structure based on distributed Fog computing, with SDN/Blockchain", J. Sens. Actuator Netw. 2019

[18]. WissamRazouk,DanieleSgandurra,"A New Security Middleware Architecture Based on Fog Computing and Cloud To Support IoT Constrained Devices",In Proceedings of International Conference on Internet of Things and Machine Learning (IML 2017). ACM.

[19]. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, 2007, pp. 321-334, doi: 10.1109/SP.2007.11.