JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-6, Issue-1 E-ISSN: 2347-2693

A Review on various secure data access schemes and techniques in Fog for Internet of Things

Ravula Arun Kumar[1 *(a, b)] Kambalapally Vinuthna[2]

[1*]a. Koneru Lakshmaiah Education Foundation, Vijayawada, India
[1]b. Vardhaman College of Engineering, Shamshabad, India
[2] Koneru Lakshmaiah Education Foundation, Vijayawada, India
Corresponding Author: arunravula12@gmail.com

Available online at: www.ijcseonline.org

Received: 07/Dec/2017, Revised: 20/Dec/2017, Accepted: 10/Jan/2018, Published: 31/Jan/2018

Abstract- Fog computing Provides extending feature for proper Infrastructure, Storage, Computation and services that bring cloud to the edge of network theory, fortunately or unfortunately cloud-Iot Aches from various issues such as network latency, Volume of data uploaded and the data being accessed, privacy and security. There are many schemes and methods that giving the solutions for the research being carried out in iot security, however the practical issues are still exist and in this paper the various schemes such as Distributed computing, Edge computing, homomorphic encryption, fine grained privacy preservation technique, attribute based encryption and other schemes which relates to security are reviewed and check the nature of cloud-iot based encryption schemes, In the meantime the analogy of secure access for proposed schemes such as confidentiality, availability, privacy and Integrity that securely meet the requirements of security in fog and internet of things. The Methodology is find to be metric and generic and it possess a wide range of applications and topologies with respect to networking and security. Now shall be addressing the various research techniques in order to review the security concerns in fog, cloud-IoT

Keywords- Distributed computing, key delegation, Edge computing, CP-ABE, homomorphic encryption, Hierarchical abe, fine grained privacy preservation technique.

I. INTRODUCTION

Cloud has being model for each and every computing paradigm now a days and it provides a elastic nature of computing resource by name of distributed computing and to extend the property of cloud to nature of substance the review has been moved to fog based computing like hosting and working entirely on edge network ends[1,2]. The fogging means in short of edge source and it has distributed computing properties that handles the small processing and the other small resources at the end of the cloud, Fog has the properties of that inherit from the cloud but remember cloud can't just replace the cloud, however it extends the properties of cloud nature[3,4]. An Internet of things has been modeled to solve the real world problems and at the same time it focus on cloud issues related processing structure [5]. Fog has data of analytics and various access points can be connected through the edge placement of the network. The theme of fog in short to reduce the latency and provide security at the edge of the cloud [6,7]. There are techniques that are used and applied in major function of security and privacy. A technique called Homomorphic encryption scheme which has threshold secure combination of variables without revealing of other set of variables [8]. A scheme of methodology called Fine grained privacy preserving query along with location based service ensure the network latency low as per policy[9,10]. Attribute-based Encryption technique are the two main alternatives of ABE schemes to be proposed in variance [11].

There shall be many problems with multi cloud based structure with the IOT devices in order to reduce the cost of constraints and the computation and provides various techniques to address the same of multi tendencies. Secondly internet of things requires a exponential keys to legitimate access for fog, The paper shall address the various challenges for computing IOT. The Chinese remainder theorem calculates the hash of the function and specify the injected data, the light weight preserving scheme typically also plays a vital role in degree of difference attacks. The Internet of things security is susceptible for many active attacks, first is that the most of the time the network is said to be un-attended so the cause will be passive Secondly most of the network issues has been broadcasted and have issues of eaves dropping so the value of the attack will be more and can be actively masquerade the information and identity [19,20].

The main problem is to authenticate and maintain the confidentiality in the neighboring networks. The Main problem with the internet of things is to generate the massive data within the group so it have glitches to which the information has to be passed and RFID cannot help to make the servers to make authentication[19,20]. Attribute-Based Encryption and fog, an innovative creation of mature based encryption technique by assisting impassive nature of Access policy and to make over the control of the decryption possibility and to be a is first Key Policy Attribute-based Encryption scheme and Cipher text Policy.

In two cases, a point of view user has a set of features that assistance with semi use of private key. The character set is used to label a user's Authorizations. In Key Policy-ABE, user's private key is entrenched with an admittance strategy, while cipher text is encoded by a pre-distinct access procedure in Cipher key-ABE existing a enduring self-controllable admission policy so that User would have the crucial switch of the entree to their individual PH[21].

Problem Identification:

A) Keys require large module investigation or Experimentation:

In general we use any of the cipher text technique to use for the encryption process and also for the decryption process as it compass of large exponential values the calculation requires large number of module experimentations and other set of pairings and inversely computation is very high.

B) Key Delegation Problem:

As we use the cipher-text policies for the process it generates the random new set of the private keys for the original set of given attributes and the new set of given keys may misjudge by attacker and it will be difficult to trace the malicious

C) Face Identification and Resolution technique:

In process of meet the various attributes of integrity, Authentication and confidentiality we use the process of identifying the face and get the resolution of some attributes, however me may suffer from the huge competence by gaining more sensitive data to that of what the content that want to be in this scheme.

d) Policy updating:- Traffic Analysis

As of secure transmission of data every part of the information is updated to the remote server to process the content in original, but the problem here is it would not keep a minimal copy in the local server as it creates the huge impact in policy updating in between local to remote access.

e) Heavy Communication and computation – Means of Eaves dropping

The Conventional method of Abe schemes of data can be have with multiple policies. When the data is send from local server to remote server and again from remote to local it grieves a heavy calculation and the communication as a result it suffers from packet loss and eavesdrop.

II. LITERATURE REVIEW

A very large methods have been projected by scholars and researchers in security and confidentiality procedures of fog in Internet of things. In this View, a short analysis of some significant assistance can be done to the existing work can be obtained.

Author name: Hu,*et al.* [12] :

Method Used by the author and brief description:

Face Identification and resolution in fog iot framework firstly suffers from the various security and privacy concerns. In order to set a overcome we use session key agreement, Integrity and data encryption schemes are proposed for the scheme of face Identification and resolution.

Advantage:

The Scheme of face identification and the resolution has a advantage of covering the needs of various privacy, Confidentiality and availability.

Limitation:

In Fog computation the need of more secure information is needed than that of the information receded this is the major limitation

Author name: Jiang,*et al.* [13] :

Method Used by the author and brief description:

Key delegation scheme provides the uniqueness by generating the new set of the private keys for the original subset of attributes

Advantage:

This scheme helps to make an hierarchy of all set of attributes in the system and reduce the size of the cipher and the number of exponentiations in the process of encryption and the process of decryption.

Limitation:

The cipher policy of key delegation generates the new private keys for the main original set of the attributes and it is difficult to trace the attacker

Author name: Huang,*et al*. [14] :

Method Used by the author and brief description:

Fine grained Access control of which the data attributes satisfy the particular policy only can decrypt the original set of attributes the Iot device plays the major role in creating new access policy, with the cloud server the attributes satisfy the access policy only can be decrypt the information and stored in the cloud basis. The sensitive information is uploaded will not leak any sensitive information.

Advantage:

The computation is reduced on the local server significantly it reduces the burden over certain aspects of load in cloud and making HABE trust less workload and provide scalability in IOT devices

Limitation:

The device of IOT generate a massive data send to the remote server without a copy for a local server, there how the problem arise and creates an impact on policy updating.

Author name: Alrawais,*et al.* [15]

Method Used by the author and brief description:

Here the digital signature is verified with the hash of the algorithm and establish a secure network over the fog – cloud over the Internet of things and above to that CP_ABE methods give the accuracy of authentication, confidentiality and access control.

Advantage:

The main advantage here is to require only subset of minimal keys for attributes drawn for decryption process, the secret key along with CP-ABE plays the vital role in generating a random number for each attribute.

Limitation:

The limitation in this scheme provides the accuracy, however it requires the high set of exponentials to derive the theory of research.

Author name: Huang,*et al.* [16]

Method Used by the author and brief description:

Cipher Update along with computation in cloud-fog for IOT was proposed, In this sensitive data is encrypted with the multiple policies and stored in cloud, hence the rule that satisfies only can decrypt.

Advantage:

This scheme reduces the time constraints in process of encryption and decryption and fine granted access theory is more powerful than other schemes.

Limitation:

This Scheme suffers from computation of shared sources from remote server to local server and local server to remote server.

III. SCOPE AND RESEARCH OBJECTIVE AND POSSIBLE OUTCOMES:

a)In order to develop the secure policy updating information via remote and local server better to generate a update key, so the update key has provided with the task update the information without leaking.

b) Design a scheme for connecting a thousands of objects to internet without any burden with ease of scalability and reliability. The ABE scheme reduce the workload on unique authority to set the attributes for it.

c) Design an Intrusion detection scheme to make an additional layer to monitor and detect the unusual performance and attacks in internet of things environment and decrease the number of errors in the IDS.

d) Design a technique for identification of IOT data when loading from fog nodes and protect the data by using some data preserving schemes.

E) Develop the encryption scheme for exchange of keys and provide the efficiency in terms of size of the message and other communication overheads in the IOT.

The following content play the major role in the security in fog – IOT:

Attribute Authority:

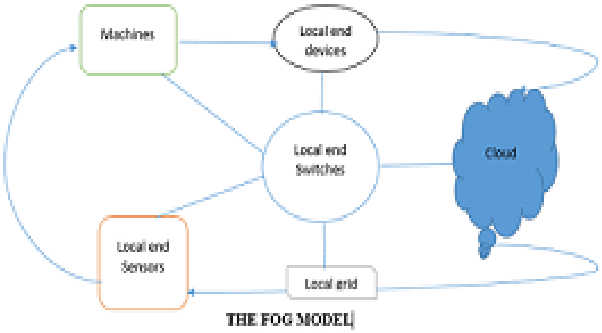
The Attribute Authority has a role of trusted functionality to generate the secret key for requested user, the authority has a right to accept it or reject it however it uses an set-up mechanism to use Key-Gen scheme for the owners to have high encryption scheme.

Cloud service Provider:

The cloud can’t be trusted fully and it is said to be semi trusted party with the high capacity of online storage and computation and the cloud has the right to check the valid signature before accepting any issues with respect to the access policies given.

Fog node:

Fog node is a edge network deployed at the edge of the network and provide the charge of cipher text update and helping the users to decrypt with CSP.Fog computing has created a huge impact on societal needs by inheriting the properties of security, privacy and other confidential trivia the major access would be of edge network and can be implemented by fog



THE FOG MODEL

Possible outcomes:

The performance of the schemes mentioned are calculated based on metrics depends on cost, time and usage of the network and delay of response time and encryption and decryption process. Now shall in the paper the discussion is on methods, existing papers and other metrics and now shall discuss the evaluation parameters to improve the accuracy.

Existing work: Hu, P.,*et al.* [12]

Method used:

Face Identification and Resolution scheme

Evaluation Parameters:

Response time (ms) differ at senses of face resolution and try to improve the accuracy by not detecting sensitive information.

Existing work: Hu, P.,*et al.* [15]

Method used:

Key exchange protocol by secure communication of Fog-Cloud and IOT

Evaluation Parameters:

It completely depends on runtime of encryption process and decryption process and other communication part based on key exchange.

Existing work: Hu, P.,*et al.* [17]

Method used:

Module mapping Algorithm is used for secure charting of information

Evaluation Parameters:

Depends on Response time and the energy consumed of data being used

Existing work: Hu, P.,*et al.* [18]

Method used:

Light weight data preserving scheme

Evaluation Parameters:

It depends on computation speed on control devices and fog devices.

Conclusion:

Fog computing and cloud computing both have the capable endurance of enabling set of theory in new applications and sciences. Defining the solutions for fog computing has a wide spread of geographical distribution of computation and strong virtual presence of stream object with real time applications. This paper mainly focused on Problems of key delegation, Large Scale Module Experimentation, Face recognition and resolution, Policy updating and Latency overhead problems along with the multiple schemes that support to the problems and fog is the right platform for maintain such critical IOT services and numerous presentations consider namely smart grid, cities and other platforms etc, and there is much scope for the research in fog-IOT as the security is the major concern in cloud platform and now moving towards fog computing. The future scope for Fog Iot security plays the vital role and 2030 of the world will be completely of IOT and there could be much scope of research in IOT security by applying different techniques to the given schemes.

References:

[1] Chen, Y. C., Chang, Y. C., Chen, C. H., Lin, Y. S., Chen, J. L., & Chang, Y. Y. (2017, May). Cloud-fog computing for information-centric Internet-of-Things applications. In Applied System Innovation (ICASI), 2017 International Conference on (pp. 637-640). IEEE.

[2] Alotaibi, Asma, Ahmed Barnawi, and Mohammed Buhari. "Attribute-Based Secure Data Sharing with Efficient Revocation in Fog Computing." Journal of Information Security 8.03 (2017): 203.

[3] Koo, D., Shin, Y., Yun, J., & Hur, J. (2016, December). A Hybrid Deduplication for Secure and Efficient Data Outsourcing in Fog Computing. In Cloud Computing Technology and Science (CloudCom), 2016 IEEE International Conference on (pp. 285-293). IEEE.

[4] Su, J., Cao, D., Zhao, B., Wang, X., & You, I. (2014). ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things. Future Generation Computer Systems, 33, 11-18.

[5] Deng, R., Lu, R., Lai, C., Luan, T. H., & Liang, H. (2016). Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption. *IEEE Internet of Things Journal*, *3*(6), 1171-1181.

[6] Liu, Y., Dong, B., Guo, B., Yang, J., & Peng, W. (2015). Combination of cloud computing and internet of things (IOT) in medical monitoring systems. *International Journal of Hybrid Information Technology*, *8*(12), 367-376.

[7] Khairnar, Sonali, and Dhanashree Borkar. "Fog Computing: A New Concept To Minimize The Attacks And To Provide Security In Cloud Computing Environment." IJRET: International Journal of Research in Engineering and Technology 3.06 (2014).

[8] Zouari, Jaweher, Mohamed Hamdi, and Tai-Hoon Kim. "A privacy-preserving homomorphic encryption scheme for the Internet of Things." Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International. IEEE, 2017.

[9] Yang, Xue, Fan Yin, and Xiaohu Tang. "A Fine-Grained and Privacy -Preserving Query Scheme for Fog Computing-Enhanced Location-Based Service." Sensors 17.7 (2017): 1611.

[10] Yang, Lei, Abdulmalik Humayed, and Fengjun Li. "A multi-cloud based privacy-preserving data publishing scheme for the internet of things." Proceedings of the 32nd Annual Conference on Computer Security Applications. ACM, 2016.

[11] Vishwanath, Akhilesh, Ramya Peruri, and Jing (Selena) He. Security in fog computing through encryption. DigitalCommons@ Kennesaw State University, 2016.

[12] Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y., & Yao, X. (2017). Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. IEEE Internet of Things Journal.

[13] Jiang, Y., Susilo, W., Mu, Y., & Guo, F. (2017). Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. Future Generation Computer Systems.

[14] Huang, Qinlong, Licheng Wang, and Yixian Yang. "DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices." World Wide Web (2017): 1-17.

[15] Alrawais, A., Alhothaily, A., Hu, C., Xing, X., & Cheng, X. (2017). An Attribute-Based Encryption Scheme to Secure Fog Communications. IEEE Access.

[16] Huang, Qinlong, Yixian Yang, and Licheng Wang. "Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things." IEEE Access 5 (2017): 12941-12950.

[17]Taneja, Mohit, and Alan Davy. "Resource aware placement of IoT application modules in Fog-Cloud Computing Paradigm." Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on. IEEE, 2017.

[18] Lu, R., Heung, K., Lashkari, A. H., & Ghorbani, A. A. (2017). A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT. IEEE Access, 5, 3302-3312.

[19] Luigi Atzori a, Antonio Iera b, Giacomo Morabito c,* The Internet of Things: A survey, Computer Networks 54 (2010) 2787–2805

[20] Dan Boneh, Matthew Frankliny, Identity-Based Encryption from the Weil Pairing Appears in SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

[21] Mrinmoy Barua*, Xiaohui Liang, Rongxing Lu and Xuemin Shen, ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing, *Int. J. Security and Networks, Vol. 6, Nos. 2/3, 2011*

Authors Profile

Mr Ravula Arun Kumar has done his B.tech in Biet affiliated jntu Hyderabad and M. tech at anurag group of institutions and presently pursing Ph.d in Koneru Lakshmaiah Education Foundation and working as assistant professor in Vardhaman college of engineering and has 2 years of teaching experience and working domain is Internet of things and ongoing research is on providing security for fog IOT platform and having more than 8 papers covering some technical domains and IOT is a platform where industry is badly needed the search of IOT developers this is how the interest has moved in the field of IOT.

Dr. Kambalapally Vinuthna presently working in Koneru Lakshmaiah Education Foundation and working as Associate professor and working domain is on data mining and IOT having a vast experience in teaching and as researcher and has found to be more technical when come to mining concepts as the research where done on data mining and ware housing and to add potential to that interest started working on IOT projects.