ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Detail Review on Fog computing Security

Sourabh Nagar[1], Sonia Setia[2]

M. Tech Scholar, Department of CSE, Echelon Institute of Technology, Faridabad, Haryana, India [1]

Asst. Professor, Department of CSE, Echelon Institute of Technology, Faridabad, Haryana, India [2]

ABSTRACT: Cloud computing can simply be defined as computing depending on the internet. In the past, people were depended on physical computer servers or storage to run their programs. Since, with the cloud computing introduction, people as well as business enterprises can now access their programs by the internet. Because of this ease, software companies and other agencies are moving more towards cloud computing atmosphere. To obtain better operational efficiency in several organizations and medium or small agencies is utilizing Cloud environment for maintaining their data. It is an integration of a no. of computing techniques and concepts i.e. Service Oriented Architecture (SOA), virtualization and other which depend on the Internet. Cloud Computing offers a simple way for accessing, managing and computation of subscriber data, but it also has some critical security risks. Very general risks now days are data theft attacks. Data theft assumed one of the top attacks to cloud computing by the Cloud Security Alliance is. To handle such cases and malicious attackers there are some methods which are utilized to protect subscriber data. A new technique known as “Fog computing” is achieving attention of the cloud subscribers nowadays. Fog computing enhances the Quality of service and also decreases latency. According to Cisco, because of its broad geographical distribution the Fog computing is suitable for real time analytics and large data. Fog computing is a paradigm that explores Cloud computing and facilities to the network edge. Similar to Cloud, Fog offers data, storage, and compute and application services to end-subscribers.

KEYWORDS: Cloud Computing, Fog Computing, Data theft

I. INTRODUCTION

In today's worlds the big as well as small organizations are utilizing cloud computing technique to secure their data and to utilize the cloud resources as and when they require. Cloud is a subscription based facility .Cloud computing is a shared resources pool. The way of utilize computers and record our business and personal information can raise new data security challenges. Encryption techniques not secure the data in the cloud from unauthenticated access. As we know that the conventional database system are often deployed in closed atmosphere where subscriber can access the system only through a limited network or internet. With the rapid development of W.W.W subscriber can access virtually any database for which they have suitable access right from anywhere in the world. By registering into cloud the subscribers are ready to achieve the resources from cloud suppliers and the organization can access their data from anywhere and at any time when they require. But this comfortless comes with particular kind of risk like privacy and security. To overcome by this issue we are utilizing a new technology known as fog computing. Fog computing offers security in cloud atmosphere at a greater extent to obtain the advantages of this technology a subscriber require to get registered with the fog. Once the subscriber is ready by filling up the sign up form he will obtain the email that he is ready to take the facilities from fog computing. First we had cloud computing, which was quite fuzzy enough for most people, but vendors have started talking more about something of late that Cisco has been pleased to call "fog computing". As far as we can tell, "fog computing" means localizing some resources and functionality that people have spent years working out how to put into the cloud. The cloud was everywhere but nowhere; the problem with this, as some resellers and tech suppliers have determined, is that the cloud itself becomes the hazard, and usually there simply isn't the bandwidth to keep the performance levels as high as several business users have come to expect."Fog" dilutes the cloud concept and its real-world representation somewhat let's have a nearby fog, not just a far-away cloud. Let's put some devices, some storage, some compute resources and so on at client level, like in the past. The most useful way to view at the fog concept is to analyse particular use cases, it proceeds. In specific cases, it may well be best to shift towards a localized or partially localized resource - and in other situations, it might all be best uploaded to a web-scale cloud platform. One component in fog could be ‘smarter' routers with more application-level service - so long as the security is fit for objective.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

II. WHAT CAN WE DO WITH FOG?

On the role of Fog computing in the following inspiring scenarios, the benefits of Fog computing fulfils the applications needs in these scenarios:

Smart Grid: balancing applications may operate on network edge devices, i.e. micro grids and smart meters. Depending on energy requirement, presence and the lowest price, these devices automatically move to alternative energies i.e. wind and solar. Fog collectors at the edge process the data produced by grid sensors and devices, and issue control commands to the actuators. They also filter the data to be consumed temporary, and forward the rest to the higher tiers for real-time reports, visualization and transactional analytics. Fog supports ephemeral storage at the lowest tier to semi-permanent storage at the highest tier.

Wireless Sensor and Actuator Networks: Conventional wireless sensor networks fall short in applications that go beyond tracking and sensing, but need actuators to exert physical Actions i.e. closing, opening or even carrying sensors. In this scenario, actuators supporting as Fog devices can control the measurement procedure itself, the stability and the oscillatory nature by generating a closed-loop system.

Decentralized Smart Building Control: The applications of this scenario are satisfied by wireless sensors deployed to estimate humidity, temperature or levels of several gases in the building environment. In this case, information can be interchanged between all sensors in a floor, and their readings can be integrated to make flexible evaluations. Sensors will utilize distributed decision making and activation at Fog devices to react to data.

Table 1: Comparison between Cloud and Fog

Features	Cloud	Fog
Latency	High(eventual consistency)	Low(locality)
Services Access	Through core	At the edge/ on handheld device
Access	Static and wireless	Mainly wireless
Main Content Generator	Humans	Devices/sensors
Control	Centralized/hierarchical (full control)	distributed/hierarchical (partial control)
Software virtual Infrastructure	Software virtual Infrastructure	User devices
Content Consumption	End devices	Any Where

III. LITERATURE REVIEW

Kaufman L. et al. (2009) [7] has analysed some security issues and the related regulatory and legal concerns that have risen as cloud computing. Interestingly, a major concern involved in the Security Content Automation Protocol is the deficiency of interoperability among system-level tools. By integrating industry best practices with the oversight National Institute of Standards and Technology US and other entities are growing, we can efficiently address cloud computing future security requirements. They also outline on the of offering data confidentiality which can affect the incident reporting.

Grobauer B. Et al. (2012), [8] offered an overview of susceptibilities in cloud security. They defined the meaning of the term susceptibility that it it's the probability that an asset is not able to protect itself against a attack. They said susceptibilities should always be described in terms of resistance to attacks or threats. Control challenges basically highlight situations in which otherwise successful security controls are not effective in a cloud setting. They have explained about the core cloud computing techniques i.e. web applications and facilities which utilize PaaS and SaaS platforms, virtualization and said that there are some such security needs which are solvable only with the support of cryptographic methods. Hence, these challenges are of particular interest for further cloud computing security research.

Sabahi, F. (2011) [9] specified attacks and reply of cloud computing. He showed a comparison of the advantages and risks of compromised privacy and security. In this paper he has summarized availability and reliability related issues of cloud resources offered by the authorized third party. He talked about the most general attacks nowadays are Distributed Denial of Service attacks. The solution to these attacks can be, cloud technology providing the advantages

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

of flexibility, with the capability to offer resources almost instantaneously as essential to avoid site shutdown [9]. He said that security is the most significant concern in cloud computing because subscriber's whole data is saved at a remote location and that location require to be protected enough that it could handle data thefts and malicious attackers.
Claycomb, W. R. (2012) [10] has featured a hierarchy of administrators within cloud service suppliers and also provide examples of attacks from real insider attack cases. They talked about how cloud architecture let intruders to breach the security. They have also shown two extra cloud related insider risks: the insider who exploits a cloud-related susceptibility to steal information from a cloud system, and the insider who utilizes cloud systems to carry out an attack on user's local resource. They specified the key challenges faced by cloud suppliers and clients for protected their highly confidential data.
Park, Y. Et al. (2012) [11] formulated a method that was a software decoy for protecting cloud data utilizing software. They introduced a software-based decoy system that purposes to deceive insiders, to determine the ex-filtration of proprietary source code. The system makes a Java code which seems as valuable information to the intruder. Further static obfuscation method is utilized to create and transform original software. Bogus programs are combined by software that is automatically transformed from actual source code, but designed to be dissimilar to the original[11].This deception method confuses the insider and also obfuscation supports the secure data by hiding it and making bogus information for insider. Beacons are also inserted into the bogus software to determine the ex-filtration and to build an alert if the decoy software is touched, compiled or executed.
Salvatore J. Stoflio et al. [4] introduced a new technology known as Fog computing. They implemented security by utilizing decoy information technology. They explained two methods i.e. User behaviour profiling and Decoy. In User behaviour profiling they examined how, when and how much amount of information a subscriber is accessing. They scanned their subscriber's activity to examine for any abnormality in the data access nature of the subscriber. The second technique is decoy in which information which is bogus or we can say fraud i.e., honey pots, honey files, etc. are utilized to confuse the intruder or malicious intruder by representing the information in such a way that it appears real.
Madsen.H and Albeanu. G [5] showed the challenges faced by current computing paradigms and explained how Fog computing platforms are viable with cloud and flexible for real life projects. Fog computing is primarily performed for the requirement of the geographical distribution of resources rather than having a centralized one. A multi-tier architecture is adopted in Fog computing platforms. In first tire there is machine to machine communication and the higher tiers handle visualization and reporting. The higher tier is shown by the Cloud. They said that making Fog computing projects are challenging [5] but there are algorithms and techniques exist that handle reliability and assure fault tolerance. With their support such real life projects are possible.

IV. SECURING CLOUDS USING FOG

When a subscriber may link to the Internet, a particularly vexing issue before such services The proposals for cloud based facilities define mechanisms to store files, documents and media in a remote service that may be accessed are widely accepted concerns ensures for protecting a subscriber's data in a way where that ensures only the subscriber and no one else can gain access to that data. The issue of offering security of secret information remains a core security issue that, to date, has not offered the levels. Some proposals have been built to protect remote data in the Cloud utilizing encryption and standard access controls. It is right to say all of the standard techniques have been established to fail from time to time for variety of insider attacks, faulty implementation buggy code, mis-configured services, and the innovative construction of efficient and sophisticated attacks not seen by the implementers of security techniques.
Cloud services are basically made existed through a community cloud, hybrid cloud, private cloud or public cloud. Normally speaking, services offering by a public cloud will be provided across the internet and are operated and owned by a cloud service supplier. Some examples involve facilities at the general public, i.e. online photo storage services, e-mail services or social networking sites in the web. In public cloud, facilities for enterprises can also be provided. Since, cloud infrastructure is operated strictly for a particular organization or a third party. In a cloud community, various organizations share the service and made existed only to those groups. The cloud service supplier may be owned and operated the infrastructure. The subscribers utilized to save business information, personal data in the cloud computing. With this a security changes reached in computing that the data in cloud i.e. the business information and personal information is attacked. To resolve this Fog computing takes to protect the data storage in the by utilizing decoy information. This technique launches disinformation against malicious insiders, preventing real sensitivity data to worthless data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A. Cryptographic Hash Function

A hash function h(m) is a message digest; in some manner, the message is condensed. Hash functions are routinely utilized to examine integrity or for error determination of transferred messages. Alex and Nick must agree on a hash function. If Nick is forwarding a message to Alex, he might generate a hash message and transfer it along with the message. After obtaining the message, Alex generates a hash message that he obtained utilizing the hash function that he and Nick has agreed to utilize. The two hashes should be the similar. If they are, Alex can consider that the message has not been modified intentionally or unintentionally at the time of transmission.

Hash functions should receive messages of any length as input, generate a static-length output, and be fast.

A hash function that will be utilized for cryptographic objectives should have some other features:

1. A cryptographic hash function should be one-way. Knowing an output h of the hash function it should computationally unviable to determine a message m which hashes to that output; i.e., for which h(m) = h. (This property is known as pre-image resistant.)
2. A cryptographic hash function should also be second pre-image resistant – provided a message m1, it should be computationally unviable to determine another message m2 with m m 1 2 ≠ having h h (m m 1 2 = ( ) .
3. A cryptographic hash function should be potentially collision free. It should be computationally unviable to determine two different inputs that have the same hash; i.e., it should be computationally unviable to find messages m m 1 2 ≠ having h h (m m 1 2) = ( ) .

Of course, the no. of inputs is much greater than the no. of outputs; so, collisions will take place but collisions should be unlikely.

There are two broadly utilized families of cryptographic hash functions – the MD family (MD = message digest) and the SHA family (SHA = secure hash algorithm). Rivest and RSA laboratories formulated MD4 and now MD5. The original MD was never published; MD2 was the first of the family to seen, and it was adopted by MD4. The NSA formulated SHA-1 and SHA-2. Around February 2005, issues with SHA-1 became public.

However, the development of public-key cryptography computationally plays an important, visible role in cryptanalysis and cryptography. The building of hash functions, since, remains mostly non-mathematical and is possibly more an art than a science.

Hash functions permits authentication to take place without double encryption of the whole message.

Alex and Nick must agree on a hash function. Then Nick can (for security) forward his message utilizing Alex's public key. Also, he generates a hash of the plaintext and (for authorization) forwards it utilizing his private key. Utilizing his private key, Alex decrypts the cipher text encrypted with his public key and generates a hash of the plaintext utilizing the hash function that he and Nick have agreed to utilize. Alex also decrypts the cipher text of the hash utilizing Nick's public key. The two hashes should be the same. If they are, Alex can consider that the message is protected and that it came from Nick.

B. Decoy System

Decoy data i.e. decoy documents, honey pots and other fake information can be created on demand and utilized for determining unauthenticated access to information and to „poison" the thief's ex-filtrated information. Serving decoys will confuse an intruder into believing they have ex-filtrated helpful information, when they have not. This technique may be combined with subscriber behaviour profiling technique to protect a subscriber's data in the Cloud. Whenever unauthenticated and abnormal access to a cloud service is observed, decoy information may be returned by the Cloud and delivered in such a manner that it seems completely legitimate and normal. The legitimate user, who is the information owner, would readily determine when decoy information is being returned by the Cloud, and thus could modify the Cloud's responses by a variety of means, i.e. challenge questions, to report the Cloud security system that it has incorrectly determined an unauthenticated access. In the case where the access is correctly determined as an unauthenticated access, the Cloud security system would provide unbounded amounts of fake information to the intruder, hence protecting the subscribers true data from can be implemented by provided two extra security characteristics: (1) validating whether data access is authenticated when abnormal information access is determined, and (2) confusing the intruder with fake information that is by offering decoy documents.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

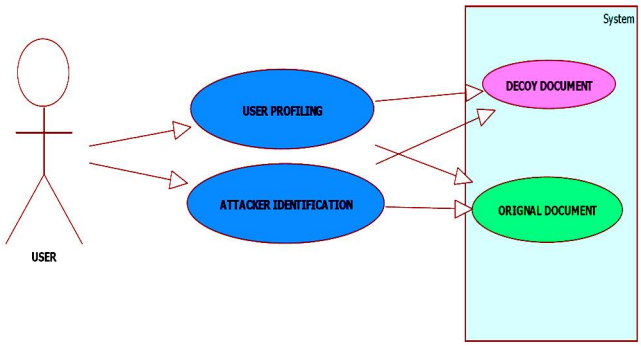

Fig -1: Decoy System

We have used above concepts to determine unauthenticated data access to data saved on a local file system by. intruders who view of legitimate subscribers after stealing their confidential information. Our experimental results in a local file system setting represent that integrating both mechanisms can lead better detection results .This results show that this technique may work in a Cloud atmosphere, to build cloud system more transparent to the subscriber as a local file system.

V. CONCLUSION

With the increment of data theft attacks the protection of subscriber data security is becoming a critical problem for cloud service suppliers for which Fog Computing is a paradigm which supports in monitoring the subscriber behaviour and offering security to the subscriber data. Cryptographic hash functions are a helpful building block for various cryptographic applications. The most significant are surely the protection of information authentication and digital signatures. Cryptographic hash functions are a helpful tool in the protection of information integrity. Thus the requirement available for probably secure and effective constructions. For the time being only a restricted no. of probably secure constructions available, that is very ineffective. Some theoretical results are presented to support practical constructions, but most of our knowledge on practical systems is generating from trial and error methods. Thus it is significant that new proposals are measured thoroughly by various independent researchers and that they are not implemented too frequently. Furthermore, implementations should be modular such that algorithm upgrade is viable. The choice between different algorithms will also base on the existed hardware.

REFERENCES

[1] Hashizume K., Rosado D. G.,Fernandez- Medina E. and Fernandez E. B. “An analysis of security issues for cloud computing”. Journal of Internet Services and Applications, 4(1), pp. 1-13, 2013
[2] Marinos A. & Briscoe G., Community Cloud Computing (pp. 472-484). Heidelberg: Springer, 2009, pp. 472-484.
[4] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012
[5] Madsen, Henrik, et al. "Reliability in the utility computing era: Towards reliable Fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. IEEE, 2013
[6] Zhu, Jiang, et al. "Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture." Service Oriented System Engineering (SOSE), IEEE, 2013
[7] Kaufman, L. M. “Data security in the world of cloud computing”. Security & Privacy, IEEE, 7 (4), pp.61-64, 2009,
[8] Grobauer, B., Walloschek, T., & Stocker, E. “Understanding cloud computing vulnerabilities”. Security & Privacy, IEEE, 2011, pp. 50-57.
[9] Sabahi, F. “Cloud computing security threats and responses”, In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on pp. 245-249, 2011
[10] Claycomb, W. R., & Nicoll, A. “Insider Threats to Cloud Computing: Directions for New Research Challenges”, In Computer Software and Applications Conference (COMPSAC), IEEE 36th Annual, July, pp. 387-394, 2012
[11] Park, Y., & Stolfo, S. J. “Software decoys for insider threat”, In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, May, pp. 93-94, 2013
[13] Kamyab Khajehei,” Role of virtualization in cloud computing”, International Journal of Advance Research in Computer Science and Management Studies, ISSN: 2321-7782, Volume 2, Issue 4, pp 15-23, April 2014.
[14] Thogaricheti Ashwini and Mrs. Anuradha.S.G,” Fog Computing to protect real and sensitivity information in Cloud”, International Journal of Electronics and Computer Science Engineering, ISSN- 2277-1956, Volume 4, Number 1, pp 19-29

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

[15] Divya Shrungar J, Priya M P and Asha S M," Fog Computing: Security in Cloud Environment", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 8, pp 803-807, August 2015.
[19] Shanhe Yi, Cheng Li and Qun Li," A Survey of Fog Computing: Concepts, Applications and Issues", Mobidata'15, June 21, 2015.
[20] Durairaj. M and Kannan.P," A Study On Virtualization Techniques And Challenges In Cloud Computing", International Journal of Scientific & Technology Research, ISSN 2277-8616 , Volume 3, Issue 11, pp 147-151, November 2014
[21] Kc gounda, Anurag Patro, Dines Dwivedi and Nagaraj Bhat "Virtualization approaches in cloud computing" International Journal of Computer Trends and Technology (IJCTT), Vol. 12, Issue 4, pp161-166, June 2014.
[22] Ivan Stojmenovic and Sheng Wen," The Fog Computing Paradigm: Scenarios and Security Issues", In the Proceedings of Federated Conference on Computer Science and Information Systems, Vol. 2, pp. 1–8, 2014.
[23] Swati Agarwal, Shashank Yadav and Arun Kumar Yadav," An Efficient Architecture and Algorithm for Resource Provisioning in Fog Computing", I.J. Information Engineering and Electronic Business, pp 48-61, January 2016
[24] Clinton Dsouza, Gail-Joon Ahn and Marthony Taguinod," Policy-Driven Security Management for Fog Computing: Preliminary Framework and A Case Study", IEEE IRI 2014, No. 13, pp 16-23, August 2014.
[25] K.P.Saharan and Anuj Kumar," Fog in Comparison to Cloud: A Survey", International Journal of Computer Applications (0975 – 8887), Volume 122 – No.3, pp 10-12, July 2015.
[26] T.Rajesh Kanna, M. Nagaraju and Ch.Vijay Bhaskar," Secure Fog Computing: Providing Data Security", International Journal of Research in Computer and Communication Technology, Vol 4, Issue 1, pp 53-55, January– 2015.
[27] D.C.Saste, P.V.Madhwai, N.B.Lokhande and V.N.Chothe," FOG COMPUTING: Comprehensive Approach for Avoiding Data Theft Attack Using Decoy Technology", International Journal Computer Technology and Application, Vol 5(5), pp 1768-1771, Sept.-Oct. 2014.
[28] Tom H. Luan, Longxiang Gao, Zhi Liz, Yang Xiang, Guiyi Wey, and Limin Sunz," Fog Computing: Focusing on Mobile Users at the Edge", arXiv:1502.01815v3 [cs.NI] , pp 1-11, 30 Mar 2016.