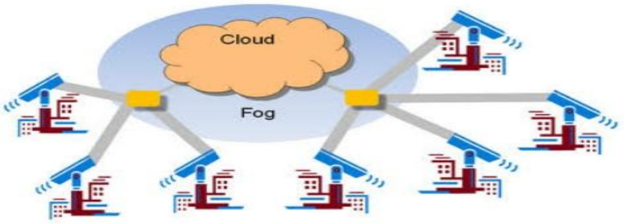
Fog Computing: A Survey

Sakshi Bhardwaj[1],
[1]GITAM, Kablana,
Jhajjar, Haryana

Sonia Tomer[2],
[2] Assistant Professor
CSE Department, GITAM,
Kablana, Jhajjar, Haryana

Fog computing is a term created by Cisco that refers to extending cloud computing to the edge of an enterprise's network. Also known as edge computing or fogging, fog computing facilitates the operation of compute, storage and networking services between end devices and cloud computing data centers. The cloud is ba a clusters of multiple servers attached within a network. The cloud computing is a network based environment that focuses on sharing computations or resources. The main problem that accours in cloud computing is security.And now a days security and privacy both are the main concern that needed to be considered. To overcome the problem of security the new technique which is called as Fog Computing was introduced .Fog Computing is not a replacement of cloud computing it's just extends the cloud computing by providing security in the cloud environment. With Fog services we are able to enhance the cloud experience by isolating users data that need to live on the edge. The main aim of fog computing is to place the data close to the end user.

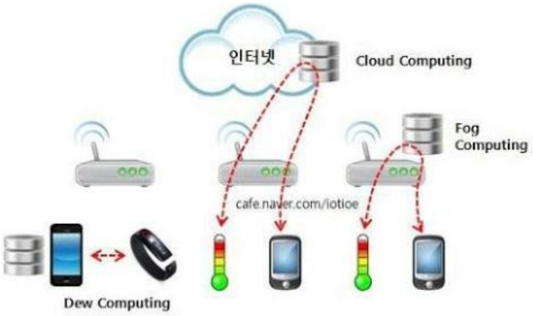
Keywords: Cloud, Cloud Computing, Decoys technique, Fog Computing, Cisco



I. INTRODUCTION

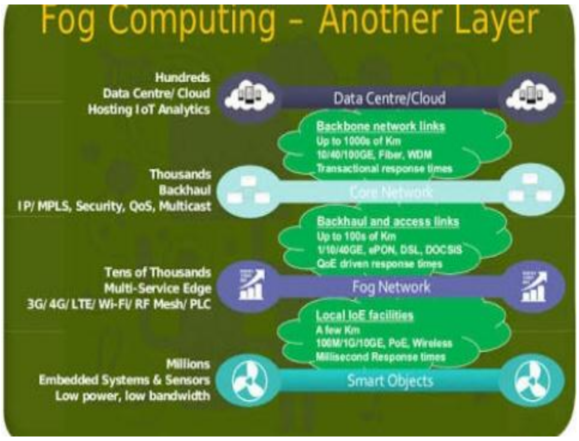
In today's world the small as well as big organizations are using cloud computing technology to protect their data and to use the cloud resources as and when they need .The Cloud computing is a subscription based service .Cloud is a shared pool of resources. The way of use computers and store our personal and business information can arise new data security challenges. Encryption mechanisms does not protect the data in the cloud from unauthorized access. As we all know that the traditional database system are usually developed in closed environment where user can access the system only through the restricted network or internet. With the fast growth of W.W.W user can access virtually any database for which they have proper access right from anywhere in the world. By registering into cloud computing the users are ready to get the resources from cloud providers and the organization can access their data from anywhere at any time when they need. But with all this comfort there is also the risk present of security and privacy. To overcome by this problem we use the technique known as fog computing. The Fog computing provides security in cloud environment in a greater extend to get the benefit of this technique a user need to get registered with the fog. Once the user is ready by filling up the sign up form he will get the message or email that he is ready to take the services from fog computing.

There are so many ways to use cloud services to save files and store files and media in remote services that can be accessed whenever user connect to the Internet. The problem that arises in cloud is to maintain security for users data in way that guarantees only authenticated users and no one else gain access to that data. The issue of providing security to confidential information is core security problem, that it does not provide level of assurance most people desire. There are many methods to secure data in cloud computing using standard access control and encryption methods.



II. SECURING CLOUDS USING FOG

It is good to say that all the standard approaches used for providing security have been demonstrated to fail from time to time for a variety of reasons, including faulty implementations, buggy code, misconfigured services, insider attacks, and the creative construction of sophisticated and effective attacks not envisioned by the implementers of security procedures. Building a secure and reliable cloud computing environment is not enough, because continue attacks happen on data, and when they attacks do, and information gets lost, there is no way by which we can get it back. There is needs to get solutions to such accidents. The basic idea is that we can limit the damage of stolen data if we decrease the value of that stolen data to the attacker. We can achieve this through a "preventive" decoy (misinformation) attack. We can secure Cloud services by implementing given additional security features.

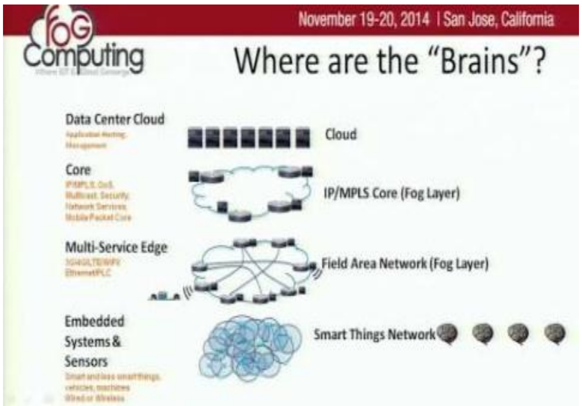


III. DECOY SYSTEM

Decoy data, such as honey pots ,decoy documents, and other fraudulent information can be generated on demand and used for detecting unauthorized access to information and to "poison" the thief"s ex-filtrated information. Serving decoys will confuse an attacker into believing they have ex-filtrated useful information, when they have not. This technology may be integrated with user behavior profiling technology to secure a user's data in the Cloud. Whenever abnormal and unauthorized access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way that it appear completely normal and legitimate. The responsible user, who is the owner of the information, would readily identify when decoy information is being returned by the Cloud, and hence could alter the Cloud's responses through a variety of means, such as challenge questions, to inform the Cloud security system that it has incorrectly detected an unauthorized access. In the case where the access is correctly identified as an unauthorized access, the Cloud security system would deliver absolute amounts of bogus information to the attacker, thus securing the user's true data from can be implemented by given two additional security features:

(1) Validating whether data access is authorized when abnormal information access is detected, and

(2) confusing the attacker with bogus information that is by providing decoy documents. We have applied above concepts to detect unauthorized data access to data stored on a local file system by scammer, i.e. attackers who view of legal users after stealing their sanction. Our experimental results in a local file system setting show that combining both techniques can yield better detection results .This results suggest that this approach may work in a Cloud environment, to make cloud system more clear to the user as a local file system.



IV. CHARACTERISTICS OF FOG COMPUTING

The different characteristics of fog computing are:

1) Geographical distribution : The services and application objective of the fog is widely distributed for example fog will play an important role in delivering high quality spill to connected vehicles through proxies and access points positioned nearby.

2) Edge location location awareness, and low latency : Fog computing support endpoints with bluecoat services at the edge of the network.

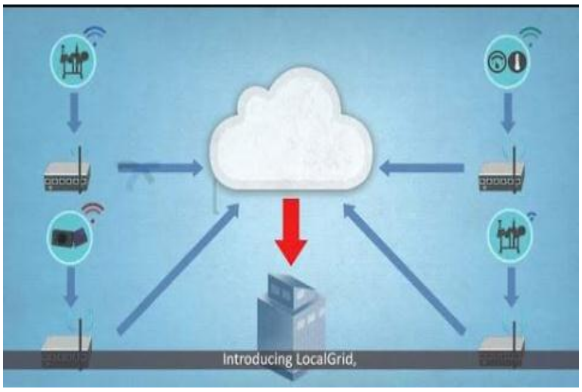
3) Real time interactions : fog computing requires real time interactions for speedy service.

4) Support for mobility : Using LISP protocol fog devices provide flexibility techniques like decouple host identity to location identity.

5) Heterogeneity : Fog nodes can be deployed in a wide variety of environments.

6)Interoperability : Fog components must be able to interoperate in order to give wide range of services like cascade.

7) Support for on-line diagnostic and interplay with the Cloud: The Fog is sited to play a crucial role in the absorption and processing of the data close to the source.



V. APPLICATION AREAS OF FOG COMPUTING

According to CISCO the important areas where fog computing would play a vital role are the following:

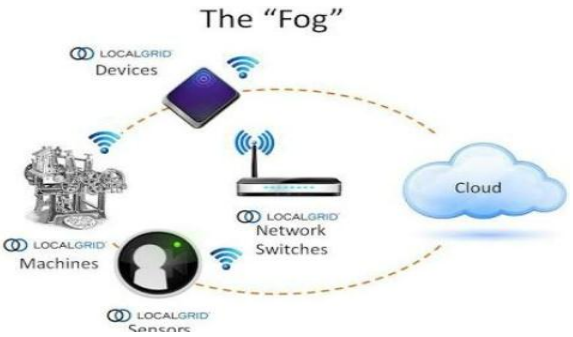
Smart Grids: Smart grid is another application where fog computing is been used. Based on demand for energy, its low cost and obtain-ability , these smart devices can switch to other energies like winds and solar. The edge process the data collected by fog collectors and generate control command to the sectators. The filtered data are consumed locally and the balance to the higher tiers for visualization, real-time reports and transactional analytics. Fog supports semi-permanent storage at the highest tier and momentary storage at the lowest tier.

Connected car: Autonomous vehicle is the new trend taking place on the road. Tesla is working on software to add automatic steering, enabling literal "hands free" operations of the vehicle. Starting out with testing and releasing self-parking features that don't require a person behind the wheel. Within 2017 all new cars on the road will have the capability to connect to cars nearby and internet. Fog computing gives real time interaction that's why fog computing will be the best option for all internet connected vehicles. Cars, traffic lights and access point will be able to interact with each other and so it makes safe for all. At some point in time, the connected car will start saving lives by reducing automobile accidents.

Smart Traffic lights: Fog enables traffic signals to open lanes on sensing flashing lights of the ambulance. It detects presence of bikers and pedestrian, and measures the speed and distance of the close by vehicles. Sensor lighting turns on, on indentifying movements and vice-versa. Smart lights serves as fog devices synchronize to send warning signals to the coming vehicles. The interactions between vehicle and access points are enhanced with 3G,WiFi, road side units and smart traffic lights.

VI. FOG COMPUTING

Fog Computing system is trying to work against the attacker specially malicious insider. Here malicious insider means Insider attacks can be performed by malicious employees at the providers or users site. Malicious insider can access the private data of cloud users. A malicious insider can easily obtain passwords, cryptographic keys and files.

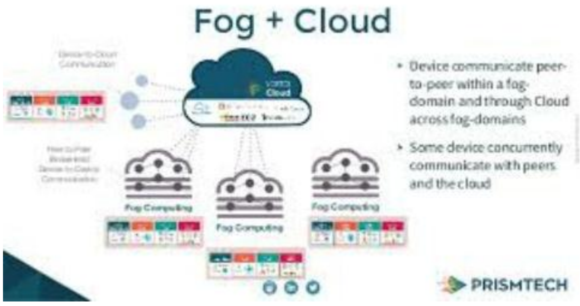


The threat of malicious attacks has increased due to lack of transparency in cloud providers processes and procedures . It means that a provider may not know how employees are granted access and how reports as well as policy compliances are analyzed or how this access is monitored . Above fig. defines the actual working of the fog computing .In two ways login is done in system that are “user login” and “admin login” .When admin login to the system there are again two steps to follow:

step1:-Enter username

step2:-Enter the password .

After successful login of admin he can perform all admin related tasks, but while downloading any file from fog he have to answer the security Question if he answer it correctly then only original file can be download. In other case ,when user or admin answer incorrectly to the security question then decoy document (fake document) is provided to the fake user .


Fog + Cloud
Device-to-Cloud Communication
Peer-to-Peer Brokered Device-to-Device Communication
Vortex Cloud
Fog Computing
Fog Computing
Fog Computing
• Device communicate peer-to-peer within a fog-domain and through Cloud across fog-domains
• Some device concurrently communicate with peers and the cloud
PRISMTECH

VII. CONCLUSION AND FUTURE SCOPE

The system was developed only with email plan but we have also implemented the SMS technique. In Fog Computing we presenting a new approach for solving the problem of insider data theft attacks in a cloud using dynamically generated decoy files and also saving storage required for maintaining decoy files in the cloud. So by using decoy technique in Fog can minimize insider attacks in cloud .Fog computing has the ability to handle the data deluge created by Internet of Things. The characteristics of fog computing like proximity to end-users, flexibility, low latency, location awareness, assortment and due to its real-time applications fog computing platform is considered as the appropriate platform for Internet of Things. From the above analysis, it can be seen that fog computing is entering an exciting time, where it can positively affect operational costs. Fog computing resolves problems related to congestion and inactivity. Fog computing also provides an intelligent platform to manage the distributed and real-time nature of emerging IoT infrastructures. Developing these services at the edge through fog computing will lead to new business opportunities and models for network operators.

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, 2013, 4(1), pp. 1-13.

[2] Marinos A. & Briscoe G., Community Cloud Computing (pp. 472-484). Heidelberg: Springer, 2009, pp. 472- 484.

[3] Archer, Jerry, et al. "Top threats to cloud computing v1. 0." Cloud Security Alliance (2010).

[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), 2013 IEEE.

[7] Kaufman, L. M. “Data security in the world of cloud computing”. Security & Privacy, IEEE, 2009, 7 (4), 61-64.

[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 (2011, May),(pp. 245-249).

[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, 2012, July, pp. 387-394.

[11] Park, Y., & Stolfo, S. J. “Software decoys for insider threat”, In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, 2012, May, (pp. 93-94).

[12] Bonomi, Flavio, et al. "Fog computing and its role in the internet of things." Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012, pp. 13-16).