Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/5573
DOI URL: http://dx.doi.org/10.21474/IJAR01/5573

RESEARCH ARTICLE

MULTI-TIER SECURITY TECHNIQUE FOR DATA LEAKAGE DETECTION AND PREVENTION IN FOG COMPUTING ENVIRONMENT.

Darakhshinda Parween[1] and Arun Kumar Yadav[2].
1. Sree Dattha Institute of Engineering and Science, Ibrahimpatnam, Hyderabad, 501506, India.
2. ITM University, Gwalior, 475001, India.

Manuscript Info

Manuscript History

Received: 09 August 2017
Final Accepted: 11 September 2017
Published: October 2017

Key words:-
Cloud Computing, Fog Computing, Data Leakage, Multi-Tier Security, EndPoint Protector.

Abstract

In this growing world of technology, Cloud computing is accomplishing stardom because of its usage and storage which is accommodate to users for personal as well as business prospects is rising its requirements. Most of users are devoted cloud computing for its fluidity and ease of access. Cloud computing is a consolidation of service oriented architecture and various computing procedures such as virtualization, fluidity, service-oriented architecture, and assets management. The reinforcement of Cloud computing technology handle various analytical problems such as security, availability, accountability, confidentiality, privacy, data provenance, customization, performance unpredictability, technology bottlenecks, data leakage, data remanence, data inter portability etc., which are addressed in many researches. Very ordinary threat today's in geographical distributed cloud frame is data leakage. It is examined as the top threats to user data in cloud environment. To conquer this threat a technique is required which can detect the malicious activities. Combination of Fog computing and cloud computing are such a paradigm which helps in monitoring and identifying the unauthorized accesses. As we know that Fog computing is well suited for geographical distributed cloud surroundings to provide better security. So, it is important to provide secured Multi-tier technique for data leakage detection and prevention in fog computing environment. In this paper we are introducing resource and security algorithm along with the architecture. It is hard to trust the third party service provider. This algorithm has two accepts such as providing a secure resource between two cloud servers which are geographically distributed and ensuring the high security in multiple level.

Introduction:-

Cloud computing is accomplishing fame every day. The facility of use and storage which is accommodated to users for personal and business ambition is accumulating its demand [1] [2]. It is a ubiquitous, obtainable, on-demand network acquire to a shared pool of configurable computing resources [3]. Software companies are affectionate cloud computing for its adaptable architecture and ease of access. Cloud Computing is a unification of service oriented architecture and certain computing policies such as virtualization and networking. Infect cloud computing

Corresponding Author:- Darakhshinda Parween.
Address:- Sree Dattha Institute of Engineering and Science, Ibrahimpatnam, Hyderabad, 501506, India.

present a surrounding through which organizing and acquiring of data becomes easier but it has some effects such as data leakage, data theft, insider attacks, data provenance, customization, performance unpredictability, technology bottlenecks, data remanence, data inter portability etc.

Very common risks now days are data theft attacks, data leakage etc. Data leakage is considered one of the top threats to cloud computing by the Cloud Security Alliance [4]. To justify these issues a technique which can monitors the data and assist in identifying an unauthorized access of malicious activity. According to Cisco, due to its vast geographical distribution the Fog computing is well applicable for real time analytics. While Fog nodes accommodate localization, since reorganizing low Latency and context awareness, the Cloud includes global centralization [5]. Fog computing holds a dense geographical distribution of network and present a feature of location access. With this any unauthorized action in the cloud network can be identify.

In section 2 we focus on works related to topic. In section 3, proposed design model for resource allocation in fog environment is presented. We propose our algorithm in section also. Simulation Setup and Expected Results define in section 4. Then there is result comparison and conclusion analysis with other algorithms in section 5and 6 respectively.

Related Works:-

This section includes study and review the work of other authors. In data leakage detection and prevention, many authors already have been proposed their work in cloud computing environment. In our work, we are taking an ordinary layer of fog to accomplish the architecture more valuable. Fog is fitted very close to the end users.

Hence fog computing produce better quality of service in terms of network bandwidth, power consumption, throughput and response time as well as it minimizes the traffic over the internet .Ma Jun, Wang Zhiying, Ren Jiangchun,Wu Jiangjiang, Cheng Young and Mei Songzhu proposed the Application of Chinese Wall Policy in Data Leakage Prevention [6].

The Chinese Wall Policy integrate voluntary and required accept of access control so that it is best option for DLP. This paper enhances the conventional action, compact relationship and represents an effective architecture. Bijayalaxmi Purohit, Pawan Prakash Singh proposed a noteworthy security worries about distributed computing [7]. The significant enclaves of center are: - Information Protection, Virtual Desktop Security, Network Security, and Virtual Security. At present business world, various associations use Information Systems to pledge with their touchy and business vital data. The need to protect such a key segment of the association can't be over stressed. Information Loss/Leakage Prevention has been investigation to be one of the successful methods for rectify Data Loss. DLP adjustment analyze and counteract unapproved endeavors to duplicate or send touchy information, both deliberately or/and unexpectedly, without approval, by individuals why should approved access the delicate data. DLP is deliberated to acknowledge potential information rupture occurrences in opportune way and this happens by investigating information. Information Leakage is an accident when the categorization of data has been traded off. It imply to an illegal transmission of data from inside of an organization to outer side of an organization. The information that is spilled out can either be private in nature and are esteemed classified though Data Loss will be loss of information because of revocation, system crash and so on.

Panagiotis Papadimitriou; Hector Garcia Molina, Peter Gordon proposed an Information Leakage [8] and how it can affect an association. As many types of correspondence are being used intestinal of associations, for example, Instant Messaging; VOIP; and so on, past conventional email, more avenue for information Leakage have aggravate. Normal vectors will be investigated, both outer to the association and from inside. The talk will then address a percentage of the suggestions to associations, from lawful and consistence issues to operational issues. Having exhibited the dangers and their related dangers, the paper then analyzes a percentage of the identification and mitigation arrangements attainable. The expansion for information Leakage is vast, and not bounded to easily email and web. We are much familiarized with conviction of information misfortune from tablet robbery, programmer break-ins, move down tapes being lost or stolen, etc. In what manner would we be able to defend ourselves against the flourish risk of information Leakage Attacks by means of notify, social designing, destructive programmers, and that's just the beginning? Leakage detection has been endorsed by Panagiotis Papadimitriou; Hector Garcia Molina which can promote us to encounter the guilty leaker without changing the equity of the primitive data. Data leakage is the most convincing security thread to the organization. In their paper Papadimitriou and Garcia represented a technique for data leakage detection. In the scheme they address, a

distributer distributes a susceptible data to over all agents according to an individual request that is issued for each one of the agent.CRM system is an example of such a scenario in which data owner which client collaborator to call and the client or collaborator details are dispatched to the third party call agent. If sensitive data is leaked, the data provider would like to be capable to identify the source of leakage or slightly to estimate the prospect of each agent to have been involved in the incident. Therefore, A guilt model is proposed for estimating the possibility that an agent is tangled in a given data leakage. So that, a data allocation method that allot data record through the agent based on the agent's requests and optimization models are presented [8]. Papadimitriou and Garcia consider two types of data request: Explicit request and simple request. An explicit request holds predefine condition where as in simple request the amount of object to be randomly selected from the entire dataset. Common requests are not handled by the proposed algorithms.

There are various techniques which are used for data leakage detection some of these are as follows:
1. Steganography [9]
2. Data allocation technique
3. Watermarking the data [10]
4. Fake object model or Guilty Agent [11]

Proposed Architecture:-
In cloud computing, the efficient resource/data allocation is the main objective to full fill the requirement of client's. Resource allocation plays a significant aspect to upgrade the performance of the whole system and increase the level of customer contentment. The work is based on cloud computing technology integrated with fog computing technology. The main appearance of fog computing is location awareness, mobility, low latency, and distributed geographically [12]. Fog computing is not an alternate option of cloud computing, but it decrease the limitation of cloud computing and make it efficient and cost effective. Various papers are focuses on the efficient resource allocation algorithm and its applicability in fog environment [13]. But our paper is focus on providing multi tier security technique for data leakage detection and prevention in fog computing environment. We first study the many existing algorithms of resource allocation behind that we have designed the model to promote this algorithm. This proposed model is implemented for solving the problem related to resource/data which are not available at run time user requirement.

A. Design Model:-
To handle the problem of resource allocation at run time in fog environment, we have proposed a design model. My architecture is design in Multi-Tier cloud as well as fog environment. So, the model has four layer names as
1. Client layer
2. Fog layer
3. Cloud layer
4. Middle ware

All clients of the fog cluster server and the cloud cluster server are geographically distributed. Each fog layer and cloud layer has number of fog cluster server (FCC) and cloud cluster server (CCS) and there are number of client's respectively. Each and every fog cluster server (FCC) and cloud cluster server (CCS) wills contains fog cluster server manager (FCM) and cloud cluster server manager (CSM) which will check the possibility to provide resource/data to the clients. Primitively, any client will submit their request to any local fog cluster server (FCS), and then fog cluster server loads the request to its fog cluster server manager (FSM). Fog cluster server manager (FSM) will process the resource/data request in following conditions. If all the requesting resources/data are available to fog cluster server, then it provide the resources/data to the client and Stop.

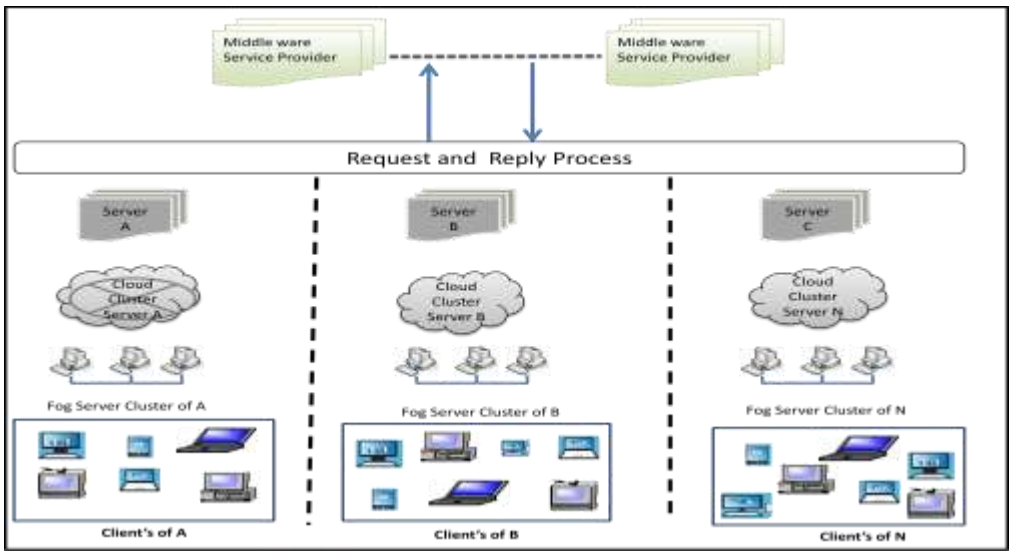

Fig.2:- Multi-Tier Secure Architecture for Fog Computing

Otherwise request is propagated to cloud cluster server by the fog cluster manager. Cloud cluster server manager (CSM) will process the resource/data request in following conditions. If all the requesting resources/data are available to cloud cluster server, then it provide the resources/data to the client .If no resource/data are available to the local cloud cluster server (CCS) request is propagated to middle ware by the cloud cluster manager. Cloud cluster server will be communicating with the middle ware for providing resources/data to the other geographically distributed cloud cluster servers. And middle ware communicates with the cloud cluster server. If another cloud cluster server is agreeing to supply there services then it inform to middle ware and middle ware inform to the cloud cluster server A. Now, cloud cluster will direct communicate with another cloud cluster server.

Proposed Algorithm:-

First we implement the algorithm in client and cloud layer via fog layer to full fill the requirement of resources/data for client in run time environment by the local cloud cluster server. If no resources/data are available in local cloud cluster server then move the request to other cloud cluster server with the help of middle ware which are geographically distributed.

A. Client Allocation Algorithm:-

We assume that Client's are authenticated according to their server Logical Unit number. There are number of servers which are connected to the different data centers. LUN filtering organized how the device are accessed and viewed from the host server. Every LUN number will have a unique ID at data center. Each server assigns a unique identified called World Wide Name (WWN).

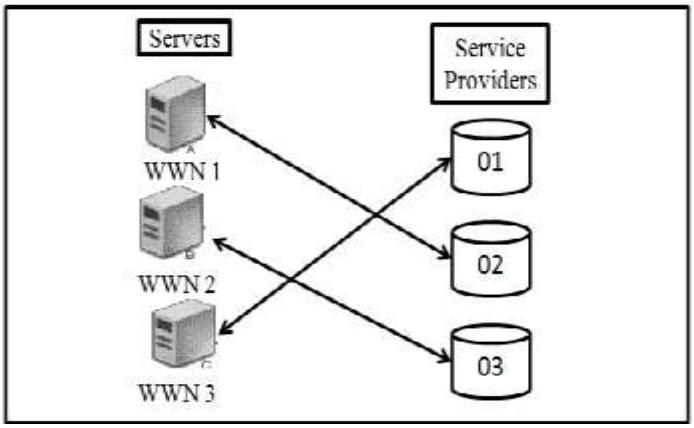

Fig. 1:- LUN Masking with server

As below table show server A with WWN 310000C09E031D15 has a unique ID 01 and so on. If requests are receiving to the same server then we assume that client's are authorized otherwise cloud server manager reject the request.

Table 1:- Example of LUN Masking

WWN	LUN ID	LUN ID	LUN ID
310000C09E031D15	1	XX	XX
310000C09E01DE2F	XX	2	XX
310000C09B22DE15	XX	XX	3

B Resource Allocation Algorithm:-

Request i_f: The request of resource/data from clients to the fog cluster server.
Request i_c: The request of resource/data from fog cluster server to cloud cluster server.
FCS_i: Fog cluster server process the request.
CCS_i: Cloud cluster server process the request.
FSM: Each fog cluster server contains fog server manager.
CSM: Each cloud cluster server contains the cloud server manager.
Request MW: The request from cloud server to the middle ware.
CSP: Cloud service Provider.
DR: The dummy resource provided by CCS
O_e: Original Extension
EPP: End Point Protector.
MU: Malicious User
ACK: Acknowledgement sends by user.

(1) For each request i_f
(2) Each request i_f is send to nearest located fog cluster server as client's location.
(3) Each FCS_i will process the resource/data request.
(4) FSM will process the service request in following conditions.
(5) IF all requesting processes are available to the local FCS.
ENDIF
THEN FCM provides the resource/data to the client.
ELSE

No resources/data are available to the local FCS, then request is propagated to the nearest CCS as user's location.

(6) Each CSM will process the resource/data request.
(7) CSM will process the service request in following condition.
(8) IF all requesting processes are available to the nearest CCS
ENDIF
CCM provide the resource/data to the client
ELSE

No resources are available to nearest CCS, THEN request is propagated to MW.

(9) MW communicates with other geographical distributed CCS to provide their services.
(10) IF geographically distributed CCS are agreeing to supply there services.
THEN it informs to MW and MW inform to CCS1.
(11) Now local CCS will directly communicate with geographically distributed CCS.

C. Security Algorithm

For security algorithm, we assume that resources/data are not available in their local fog cluster server and cloud cluster servers. So local cloud cluster server is directly communicated with other geographically distributed cloud cluster server with the help of middle ware.

For security reason, cloud server provider installs My Endpoint protector client setup in geographically distributed cloud server. To secure our sensitive data leakage, My Endpoint Protector closely analyzes all action at endpoints and other exit points. My Endpoint Protector accede individuals and companies of all sizes to accomplished all their endpoints from one centralized online console, be it Desktops, Notebooks or Netbooks, used in the office, at home or on the road. My Endpoint Protector removes the risks of data loss and data theft that are posed by portable devices, data transfers and mobile devices.

My Endpoint Protector is a fully cloud, client-server application. As per any cloud service, the server part does not demand any setup or alignment as it is organized and maintained by My Endpoint Protector. The clients have to be deployed on the endpoint we want to protect.

The functionality of the My Endpoint Protector is designed to be around several physical entities.

- Computers (PCs or MACs with My Endpoint Protector client installed)
- Devices (the devices, which are currently supported by My Endpoint Protector. e.g.: USB devices, digital photo cameras, etc.)
- The cloud/server side of My Endpoint Protector is the Administration and Reporting Tool.

It is responsible for centrally managing devices, computers, users, groups and their behavior together.
The cloud cluster may be able to add dummy resources/data with original extension in order to improve his effectiveness in detection of malicious agents. Dummy resources/data with same extension may impact the correctness of what malicious do.
(1) CSP allocate DR with O_e on client's run time demand.
(2) IF MU access DR with O_e EPP show notification
"Security warning- My Endpoint Protector

An unauthorized user wants to access these resources/data. Remove now or contact the administrator for authorization."
(3) ELSE IF client's get DR with O_e send message to SP.
(4) Now CSP provides OD with O_e.
(5) IF requirement are full fill then client's send ACK to CSP.

Data Leakage Prevention Using EndPoint Protector:-
My Endpoint Protector has complete client-server architecture, equipping data security to clients who do not have the time and resources to supervise their own on premise endpoint security solution. My Endpoint Protector is a full Device Control, Data Loss Prevention (DLP) and Mobile Device Management (MDM) cloud-based solution accessible for Windows, Mac OS X and iOS and Android mobile gadgets. Versatile storage gadgets such as USB flash drives, gadgets / tablets, e-mail significance like as Outlook and Gmail and cloud services like Dropbox, iCloud, Google Drive, etc. may cause severe concern when it comes to supervising use of confidential data. With My Endpoint Protector we can reduce the possibility of data loss, data theft and data leakage and also handle the mobile device rapid from a single consolidate online console from anyplace, at any time. My Endpoint Protector permit individuals and companies of all sizes to accomplish all their endpoints from one private online console, be it Desktops, Notebooks or Netbooks, used in the office, at home or on the road. My Endpoint Protector reduces the risks of data loss and data theft that are posed by portable devices, data transfers and mobile devices. Controlling ports, USB devices, data transfers and mobile devices through a server in the cloud is the best solution to centrally handle our network. My Endpoint Protector is accessible as a free version for private as well as small office use. The commercial version contain extra features like Content Aware Protection for Macs, unlimited amount of managed computers and mobile devices, e-mail alerts, expended reporting options, etc.

Online Administration and Reporting Tool:-
In the online Administration and Reporting Tool we can organize the behavior of our protected computers and get the details regarding their device activity, file transfers and the mobile device fleet. Access to Administration and Reporting Tool is controlled by a username and password pair and desire reorganized credential to login. After logging into My Endpoint Protector, we will see the available sections and modules.

Dashboard:-
Lets you view statistics of the server such as the number of clients and devices currently connected, the total number of protected computers, last logged action, newest added client, etc.

Fig.3:- Dashboard of EndPoint Protector

Device Control:-

It is used for administration of Devices, Computers, Groups, and Client Users. This is one of the most vital parts of My Endpoint Protector. In this segment the administrator can organized and execute security strategy by allotting certain privilege to devices, computers and computer groups. In this section, the administrator can chose, organize rights and settings or even eliminate devices, computers or groups. It also provides the choice to generate groups and append or discard client users.

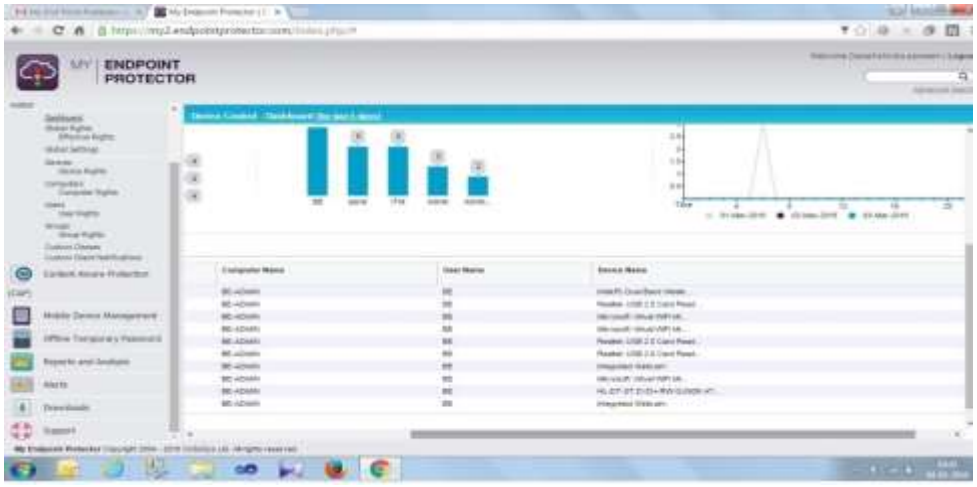

Fig.4:-Device Control by EndPoint Protector

Content Aware Protection:-

This section is used for authorization of File Transfers Policies.

This is also one of the main three modules of My Endpoint Protector. In this option the administrator can organize and enforce strong content aware security policies for an effectively control over data leaving the company network through any removable media, email, cloud storage or other online applications.

Fig.5:- Content Aware Protection

Mobile Device Management:-
This segment is used for authorization of the mobile device convey.
Reports and Analysis – It is aim to offer the administrator information concerning the past and current action on the system (Server and Clients). It incriminates several components for example Online Computers, User History, Statistics, Graphics, etc.

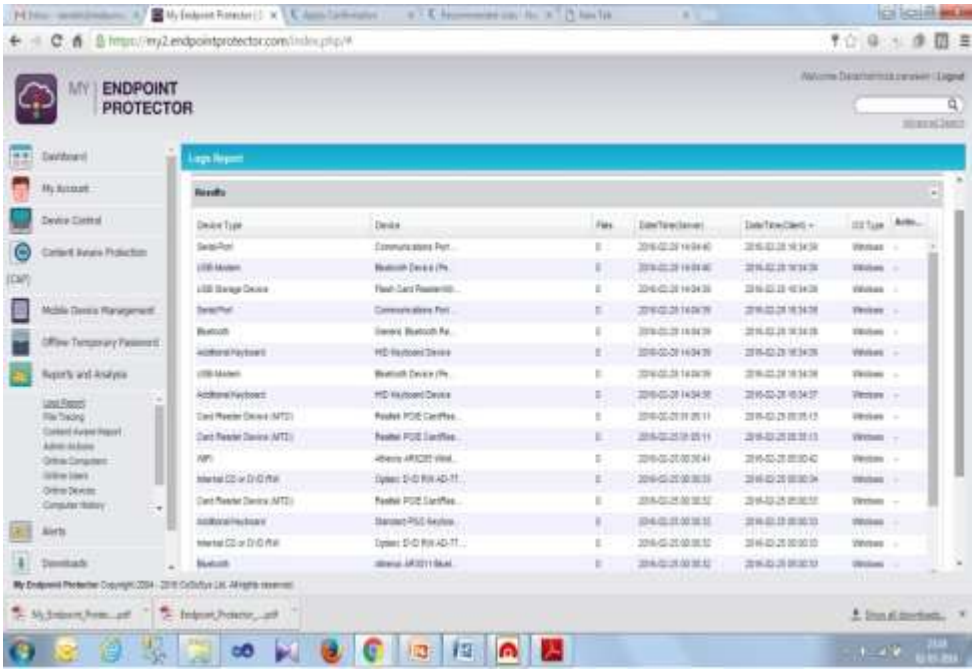

Fig. 6:- Report Analysis by EndPoint Protector

Offline Temporary Password: - In this segment administrator allows defining Offline Temporary Passwords. Way of generating a password is by selection a user computer from the Device Control> Computer list, with the action Offline Temporary Password.

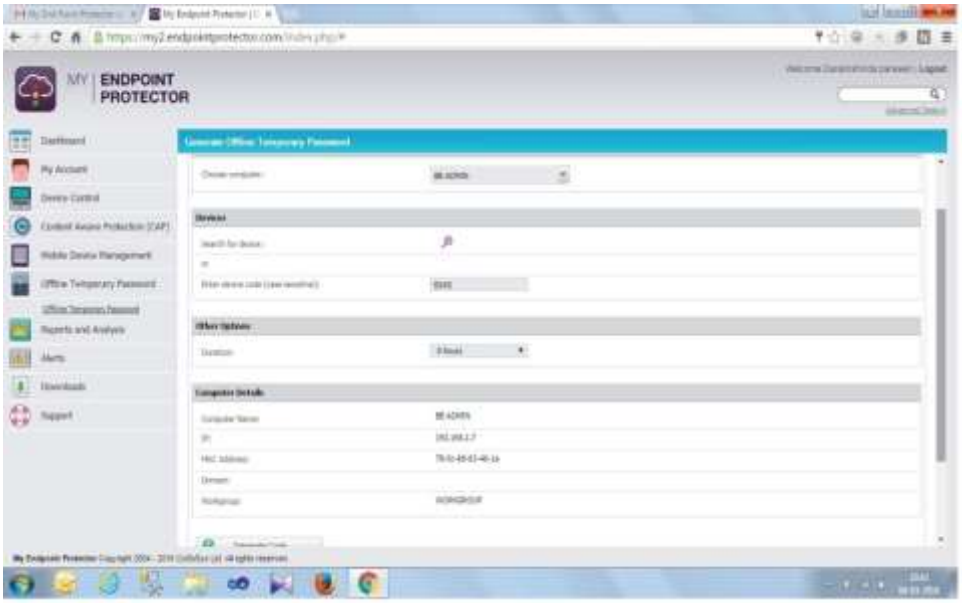

Fig.7:- Temporary password generated by endpoint protector

System Alerts:-

This part offer the generation of System Alerts – notifications, arranged by administrators, which will aware them if a new device was connected or accessed, a user performed a certain action, etc.

My Account – Provides information related to our account and allows subscriptions and clients management to us.

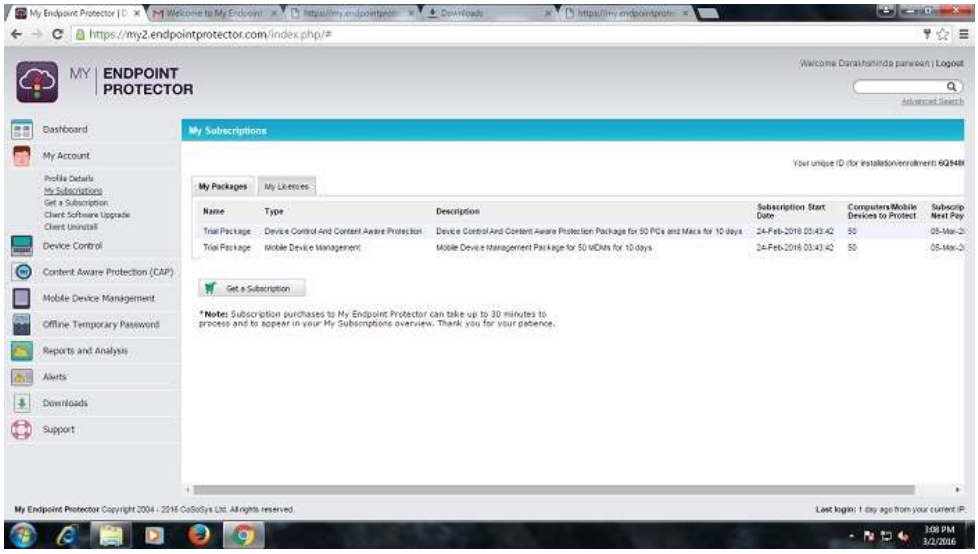

Fig. 8:- Account information

Conclusion and Future Scope:-

Fog computing is used in our research methodology because it upgrade efficiency of cloud computing. In this paper concludes the problem of comfortably detecting data leakage and guilty agents in a very large observation database collected by system. Sensitive data can be leaked by the agents mistakenly or maliciously and even if we had to provide sensitive data, in an impeccable world, we can use the abstraction of Dummy resource/data so that we find the malicious user. This paper also includes data leakage prevention technique which is handling by My Endpoint Protector. We have surveyed number of techniques related to data leakage detection and prevention but Data leakage detection and prevention can be implementation more effectively including Multi-tier Security Technique in fog Computing Environment.

Limitations and Future Directions:-

In this work protection are controlled by administrator but not by client. This paper mainly focuses on data leakage detection and prevention at run time environment. The future work can be extended towards the SaaS services. In other way, we can say that MyEndpoint protector controlled by the administrator of service provider. Some time client may also reassign the role/privileges to other client in secure manner but the existing proposed system does not provide the same which may be upgraded in future**.**

Reference:-

1. Archer, Jerry (2010). Top threats to cloud computing v1. 0. Cloud Security Alliance.
2. Bijayalaxmi Purobit, Pawan Singh. Data leakage analysis on cloud computing, International Journal of Engineering Research and Application ()2013, vol.3,issue 3,May-June 2013,page no. 1311-1316.
3. Bonomi, Flavio (2012). Fog computing and its role in the internet of things. Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, pp. 13-16.
4. Hashizume K., Rosado D. G., Fernandez- Medina E. and Fernandez E. B. 2013 An analysis of security issues for cloud computing". Journal of Internet Services and Applications, 4(1), pp. 1-13
5. IBM Blue Cloud project [URL] (2009). http://www03.ibm.com/ press/us/en/press release/22613.wss/, access on October.
6. Ma Jun,Wang Zhiying, Ren Jiangchun,Wu Jiangjiang, Cheng Yong and Mei Songzhu (2012). The Application of Chinese Wall Policy in Data Leakage Prevention In International Communication Systems and Network Technologies,
7. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph,R . Katz, A.Konwinski, G. Lee, D. Patterson, A.Rabkin,I. Stoica, and M.Zaharia (2010). A view of cloud computing , Common .ACM, vol. 53, no. 4,,pp.50-58.
8. Miss S.W. Ahmad, Dr G.R.Bamnote (2013). Data Leakage Detection and Data Prevention using Algorithm, International Journal Of Computer Science And Applications Vol. 6, No.2, ISSN: 0974-1011 (Open Access) Available at: www.researchpublications.org
9. Narendra Babu Pamula, M.Siva Naga Prasad K.Deepti. (2013) Preventing Data Leakage in Distributive Strategies by Steganography Technique, International Journal of Computer Science and Information Technology, vol 4 (2), ,220-223
10. Panagiotis Papadimitriou; Hector Garcia Molina, Peter Gordon. (2015) Data Leakage Detection of Guilty Agent In International journal of Scientific and Engineering Research vol 3,issu, 6,.
11. P. Mell and T. Grance (2009). The NIST Definition of Cloud Computing, National Institute of Standards and Technology, vol. 53, no. 6, p. 50,. [Online]Available http://csrc.nist.gov/groups/SNS/Cloud-computing/cloud-def-v15.doc
12. Swati Agarwal, Shashank Yadav, Arun Kumar Yadav(2015). An architecture for elastic resource allocation in Fog computing, International Journal of Computer Science and Communication, Vol. 6 Number pp. 201-207.
13. V.Shobana and M. Shanmuga Sundaram. (2013) Data leakage detection using cloud computing, International Journal of Emerging Technology and Advanced Engineering, vol. 3, page 111-115.