DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5045

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SURVEY OF VARIOUS SECURITY ATTACKS IN CLOUDS BASED ENVIRONMENTS

Priya Oberoi
M.M. Institute of Computer Technology & Business Management,
Maharishi Markandeshwar University, Mullana, Ambala, Haryana, India

Dr. Sumit Mittal
M.M. Institute of Computer Technology & Business Management,
Maharishi Markandeshwar University, Mullana, Ambala, Haryana, India

***Abstract*:** Security is top concern for the people of IT from the past. With the advent of new technologies the severity of the problem has been changing its shape. A number of threats and their counter measures had been identified. Similar is the Cloud based environments. In spite of large number of features provided by Clouds, they are not able to attain attention of large number of business community. Cloud Security Alliance (CSA) is the top most working group working on the security issues of the Clouds. In this paper we have studied the various security attacks (in general) with reference to the Clouds (as per The Treacherous 12 - Cloud Computing Top Threats in 2016, CSA report defeating insider threat survey(2016) ,Cyber Security Trends Report (2017)) and Malicious Insider attacks (in particular).

***Keywords*:** Cloud computing, Cloud Security, Privacy, Insider threat, Malicious Insiders

1. INTRODUCTION

There is no doubt that on one hand business organizations have cost and efficiency gains on shifting to the Cloud environment, but on the other hand they get more prone to the security attacks or risks. Now cloud security has become an important issue for the boardroom people [1].

Enterprises are shifting their data and applications to the Cloud but still they have a serious concern to the security. Due to the distributed, open source and sharing nature of Cloud computing the attacker are easily able to bypass the organizations security policies and procedures.

Confidentiality, integrity and availability are the three parameters on which security mainly depend upon [2]. The events which can cause damage to the system and result loss in CIA traids are called threats. The weaknesses in the system which can be exploited by the threats are called Vulnerabilities. A large number of threats occur due to the issues among the cloud service providers and users.

The Cloud Security Alliance (CSA) had released its research report titled "The Treacherous 12 – Cloud Computing Top Threats in 2016" in Feb 2016 [3]. Following 12 issues have been identified to be most critical (ranked in order of severity as per survey results) [3], [4], [5]:

A. *Data Breaches*

The top most security threat identified by CSA is the data breaches. The data breach refers to the stealing the protected or confidential data by a malicious or unauthorized person [6]. For example, due to vulnerability in security the Bit defender (an antivirus firm) has to suffer from a big loss as they lost many usernames and passwords. The attacks done by malicious users which have the VMs on the same physical system which is their target can also result into the data breach

.

B. *Insufficient Identity, Credential and Access Management*

It is the new threat identified this report [3]. The failure of use of multifactor authentication, less availability of access management systems for identification of legimate user which are scalable enough, use of less strong passwords and less availability of automatic rotation in the keys used for Cryptography and certificates had lead to a number of data breaches and help attackers to exfiltrate the resources. It may be caused by the authorized (insiders) as well as the unauthorized users. Management of user authentication and access control is most challenging in public and private clouds [7].The access control and user authentication procedures were identified as two of the most important parts of security issues [8].

C. *Insecure Interfaces and APIs*

Insecure Interfaces (IIs) and Application Programming Interfaces (APIs) are used by the customers to interact with the Cloud services. These act as the gateway of the attacks and issues related to the Confidentiality, Integrity, Availability and Accountability. The weak interfaces and APIs may lead to various security issues in the clouds. Mostly the APIs are provided by the cloud providers as third party service. This may result into the third party getting access to the security keys and important information [6].

D. *System Vulnerabilities*

This is also new threat identified this report [3]. These are the bugs within the system (application or Operating System) which attackers use to sneak into a computer system. This type of threat is not new but the multi tenancy of Clouds and accessibility to the resources and memory which is shared had created a new surface for attack to occur.

E. *Account Hijacking*

This threat is more dangerous in the Cloud Computing as the malicious intruders can get accessibility to all the

Cloud activities by using the stolen passwords. The intruder after gaining the access to the Cloud system may provide wrong information, can monitor the transactions and services or can divert users to the falsified web sites which may result into the legal problems for the providers.

F. ***Malicious Insiders***

A malicious insider like the administrator of the system has full-fledged access to all the Cloud system [3], [4]. This attack has its impact on all the three service models of Clouds. The adverse effect of this attack is the loss of reputation of the organization, financial loss and reduced productivity. The access of malicious insiders to critical systems increases with the levels of cloud i.e. IaaS to PaaS and SaaS [1]. Thus the systems which purely rely on the CSPs for security are more prone to M.I. attacks. Even in case of if the keys available at the time of usage of data only then also the system is prone to MI attacks. There are hobbyist hackers who are administrators and steal data for fun and another type of insiders are corporate espionage who are responsible for stealing information for corporate purpose [6].

G. ***Advanced Persistent Threats (APTs)***

The sneaky and continuous process of hacking done by the humans leads to APTs. The main aim of APTs is either related to business competition or political activities.

H. ***Data Loss***

Data being the biggest asset for any organization, if lost can give terrifying results. The consequences may be more drasting in the case of Clouds.

I. ***Insufficient Due Diligence***

This threat has been identified in all the 14 domains of CSA security guidance reference. The lack of complete knowledge of the CSP environment makes the cloud environments more prone to different types of attacks.

J. ***Abuse and Nefarious use of Cloud Services***

All the Cloud deployment models are prone to this type of attack. The services offered by Clouds like service trails or loosely secured deployment models led to malicious attacks. This malicious use reduces the Cloud capacity by reducing the availability of the resources. This attack has serious effects on service providers than the users of the service. For example, if a malicious user uses the cloud network addresses for spam it may result into the blacklisting of the addresses.

K. ***Denial of Service***

These attacks restrict the users from getting access to the Cloud servicers or to gaining access to their accounts. DDoS attacks led to the authorized users in the confused state that Why the Cloud services are not responding? This attack is worst for the users or clients as they have to pay according to the cycle and disk space.

L. ***Shared Technology Vulnerability (STV)***

As the Clouds offer the benefit of "Sharing" they are more prone to this threat. Even if a very small piece of critical information is shared accidentally or intentionally the complete cloud environment becomes vulnerable to attacks. STV is very critical as it has its impact on the whole of the Cloud at once. STVs are very commonly being used by the attackers to gain access to the Clouds.

The Insider Threat Report given by Vormetric [11] identifies the Insider threats as the threats that are caused by offenders whose actions either maliciously or accidentally put an organization and its data at risk. The actors of insider threats is not limited to employees and privileged IT staff but also include outsiders who have stolen valid user credentials; business partners, suppliers, and contractors with inappropriate access rights; and third-party service providers with excessive admin privileges. All these people have the chances to steal unprotected data if no proper controlling mechanism is applied. As per this report the insider attacks are deceptive and thus need very much attention. The analysis of the survey reveals the fact that 89% of respondents felt that they are more prone to insiders.

According to the recent Cyber Security Trends Report (2017), the most prominently occurring threat in Clouds is the unauthorized access [10]. Unauthorized access to vital information by misusing the employee's credentials and improper access controls has been identified as the largest threat to Cloud security by 61% (figure 1) of respondents. Organizations are concerned about Insider threats (34%) also.

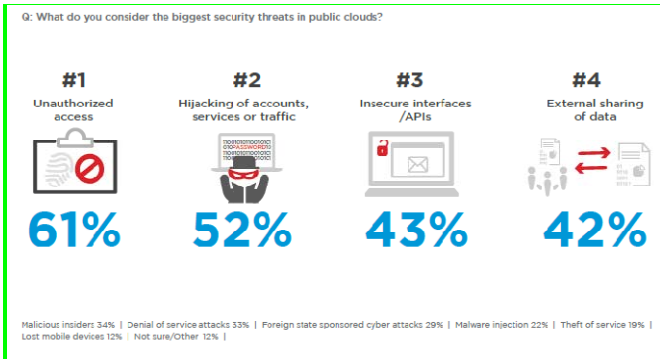

Figure 1

I. 2. WHAT TYPE OF INSIDER ACTORS POSES THE BIGGEST THREAT TO THE ORGANIZATION?

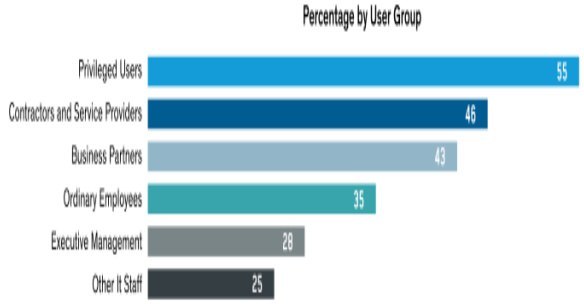

Figure 2

There are different categories of Insiders. As shown in figure 2 the privileged users are identified as the most risky type of insiders as compared to the other types of insiders like Contractors and service providers, business partners or ordinary employee etc [9]. The Insider Threat Report survey

results show that senior management is also concerned about the insider attacks by the privileged users [11].

Figure 3

Also according to the results of 2016 Vormetric report (451 Research conducted the surveys in October and November of 2015) around 58% (figure 3) respondents agreed to the fact that the privileged user accounts (IT Admins, DBAs etc) are the biggest threat actors for the insider attacks [12] .

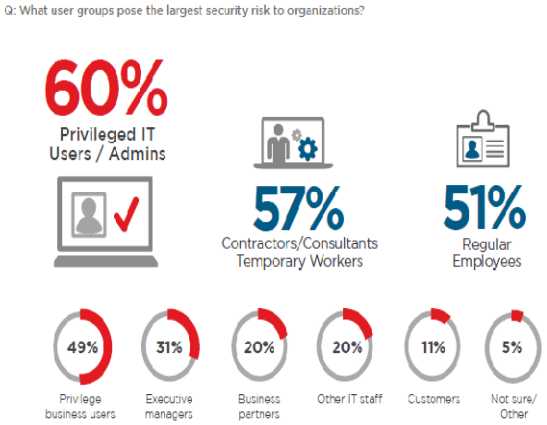

Figure 4

The insider threat report (2016) [13] clearly shows the fact that the biggest insider threat is the privileged IT users (60 percent)., such as administrators with access to sensitive information(figure 4). This is followed by contractors and consultants (57 percent), and regular employees (51 percent).

Thus from the above study the fact which becomes more prominent is that the privileged users pose more problem for the security. As from last few years privileged IT users/ admins are constantly being identified as biggest user group posing a challenge to security. It generates an alarm to security people to develop tools to protect from the Insider threats.

3. WHAT MAKES THE DETECTION OF INSIDER THREAT IS DIFFICULT?

The modern malware attacks like APTs, Insiders etc. use falsifying methods and techniques to attacks which prevent the security controls on the networks to detect them. Also they resemble the network traffic and user access patterns as normal ones.

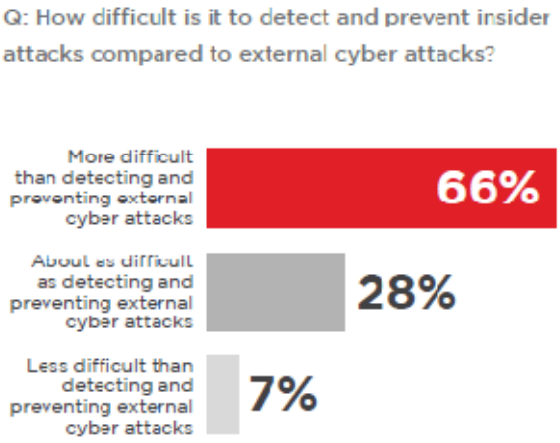

Figure 5

Referring to figure 5, a majority of respondents (66%) said that the insider attacks are more difficult to detect than the external attacks [13].

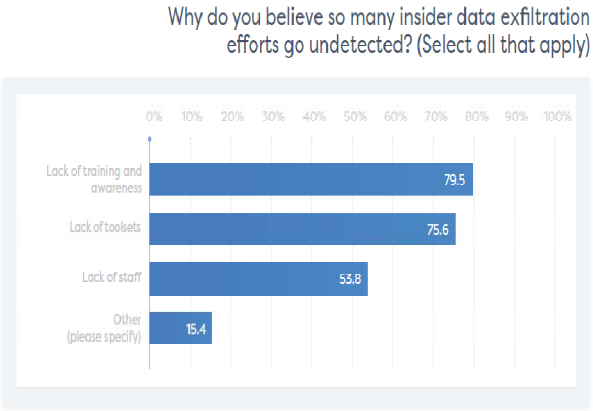

Figure 6

As per the CSA insider threat survey report [14] (figure 6), a large number of respondents said that the lack of training and awareness (79.5%) and lack of toolsets (75.6%) are responsible for the insider data exfiltration being went undetected. This reveals the fact there is great need of new toolsets to detect the insider attacks.

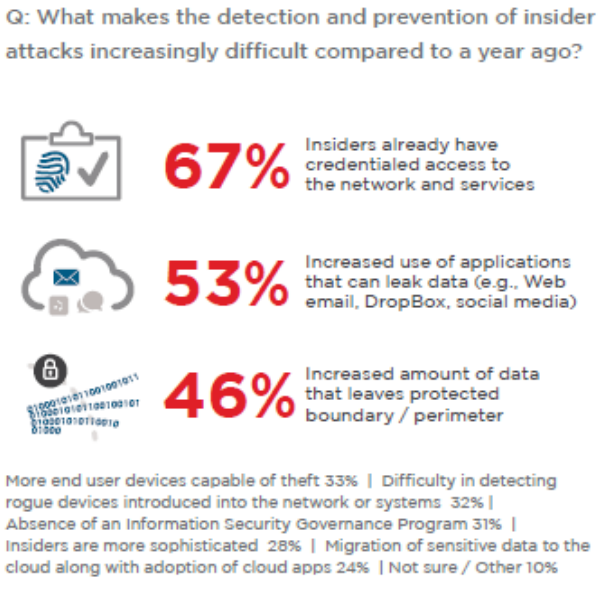

Figure 7

The Insider threat report [13] recognizes (figure 7) that the main reason in detecting insider attacks is that they have access to systems and sensitive information (67%), followed by the increased use of cloud based applications (53 percent), and the rise in the amount of data that is leaving the protected network perimeter (46 percent).

4. NEED OF SPECIALIZED TOOLS FOR CLOUD SECURITY TO DETECT MIS

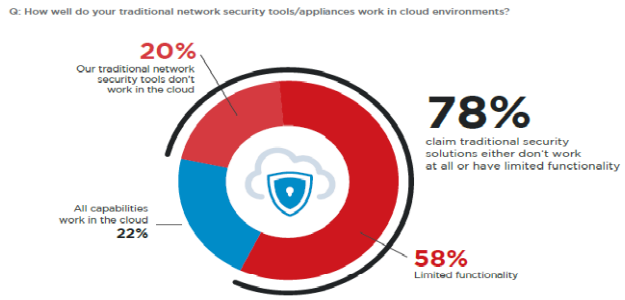

Figure 8

When asked about the suitability of traditional security tools in Cloud environments (figure 8), a large number of respondents; 78% people said that they are not suitable for the Cloud environments [10]. The traditional tools are not capable enough to cope up with the challenges posed by the virtual and dynamic nature of the Clouds.

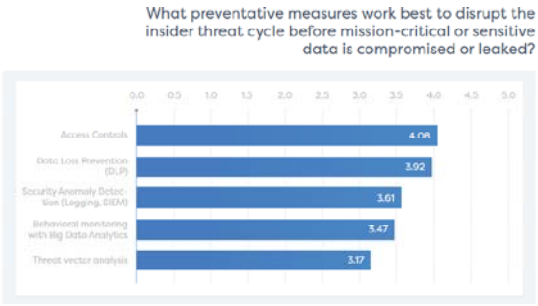

Figure 9

A mix of old and new techniques is the need of the Cloud based environments to deal with the insider data exfiltration [13],[14] (figure 9).

5. RECOMMENDATIONS FOR DEALING WITH INSIDER THREAT ACTIVITY

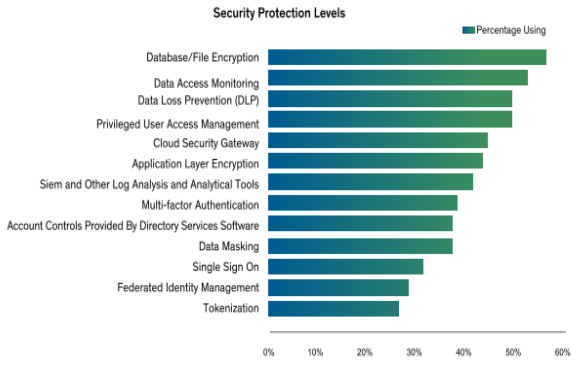

Figure 10

In Clouds based environments the users are very much diversified and thus the strategy to get protected from the insiders is also diversified and is still growing. The insiders like Contactors, Admins, IT people or malicious outsiders with the stolen user credentials are capable enough for putting the data at risk. Figure 10 shows the various solutions used by the organizations for protection against the insider attacks [9]. Data encryption is the most popular technique while the other methods include data monitoring by SIEM i.e. Security information and event management, multi-factor authentication etc.

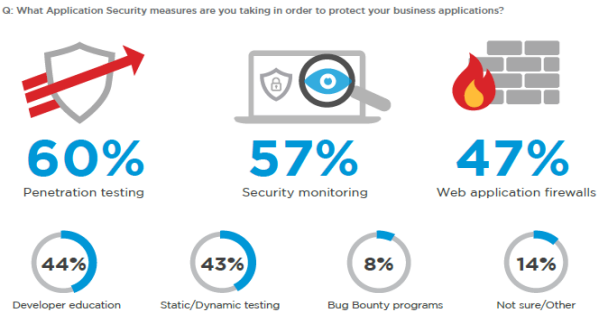

Figure 11

A majority of organizations are taking proactive measures (figure 11) to protect their business applications [27]. We dug deeper to find out how companies were protecting their applications in the cloud. The most popular application security measures are penetration testing (60%, virtually unchanged from 59% last year), followed by security monitoring (57%, significantly up from 38% last year), and web application firewalls (47%, down from 54% last year).

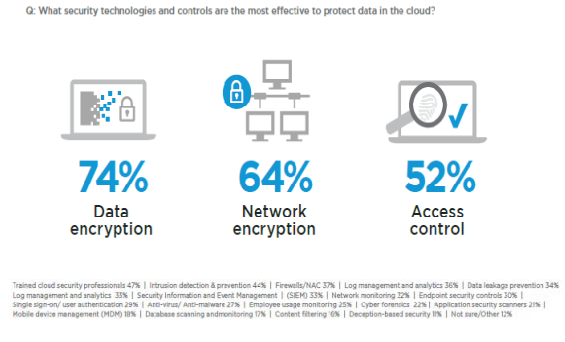

Figure 12

Technology and processes are used to implement the security capabilities and policies [10]. The Cyber security threats report (figure 12) identified Encryption as the most popular method of protection in Clouds followed the Access control (52%), trained cloud security professionals (47%), IDPS (44%) and more.

Figure 13

Most organizations (figure 13) continue to place their insider threat management focus and resources on deterrence tactics (61 percent), followed by detection (49 percent) and analysis and forensics (35 percent) [13].

The need is to have a unified and layered security strategy which is capable enough to detect the insiders timely and effectively.

6. LITERATURE REVIEW

H. G. Goldberg has used the ranking or scoring based method along with the temporal aggregation for anomaly detection. PRODIGAL system is used to conduct the research [15].

A. Coden et al proposed a quantifying approach to detect the insiders by using the data mining methods with the semantic knowledge. Markovian Bayesian network is used to compute the anomaly scores. It is a domain knowledge driven fusion method. The proposed method is not tested on the real data [16].

T. Chen also presented a framework using the quantitative approach. The intention of the attacker is identified by the Bayesian network and success probability of the attack is computed using the probabilistic model with the help of Markov decision process (MDP) [17].

Z. Abduljabbar used the user's iris to generate the code in the form of a message for every user's login in order to prohibit malicious attacks like Insiders, forgery, dictionary etc. Crypto hash function (SHA -1) algorithm is used along with the 2-D Gabor filter which is capable of extracting features from the iris [18].

I. Khan proposed a protocol for prevention of the insider attacks in IAAS clouds using the method of digital watermarking. The advantage of the method is that the watermark is not even disclosed to the cloud system administrator himself. The protocol is tested using ProVerif in Intel based system. Testing in actual environment and with AMD based system is not done [19].

S. Guha proposed a method to detect the cyber attacks using Artificial Neural Network(ANN) along with the genetic algorithm for selecting the features which are extracted from the network traffic data on the connecting links of the infrastructure of the Clouds. Efficiency of some steps need improved [20].

C. V. Neu presented an IDS to detect insider attacks in SDN Open Flow networks. The proposed IDS is capable of detecting insider attacks which exist in encrypted form. The OpenFlow switches provides the statistical information requested by the Open Daylight controller and the proposed IDS works on this statistical information. Implementation is done in simulated environment not in the actual SDN environment [21].

W. Meng identified that collaborative intrusion detection networks (CIDNs) in which the multiple IDS nodes are capable to communicate with each other; depend on the assumption that a malicious node will always send feedback opposite to its truthful judgment. It was found that existing IDS were not capable enough to detect the number of insider attacks. A new CIDN is proposed and a new insider attack called random poisoning attack has been identified. It has been proved experimentally that this new attack enables a malicious node to send untruthful information without decreasing its trust value at large [22].

J. Nikolai presented a method for anomaly detection in order to detect insider attacks in Infrastructure as a Service (IaaS) nodes. System state data and system metric anomalies are used in the system profiling method. In order to score the number of active users on nodes and bytes sent over the network the k-nearest neighbour's anomaly detection algorithm is used. The combination of login, data transfer and system state is capable to detect the insider attacks with zero percent false positive rates. Future scope include a) testing of scalability of the approach in IaaS b) exploring different anomaly detection approaches and c) use of techniques of machine learning cam result into better detection [23] .

R. Gamble applied the algorithm for detecting the attacks using the behaviour profiling method to compute the anomaly scores. For validating the malicious sender's identity useless responses are generated for misleading them. This method reliabiliy detects the attack and has some performance degradation but it is reasonable. Future work involves the decision of behaviour profiling is to be done as on individual service or on a class of similar type of services [24].

K. Kourai proposed remotely offloaded IDS with remote virtual machine introspection (VMI) for IaaS clouds. The proposed IDS overcome the limitations of the offloaded IDS, such as they can easily be disabled by the insiders. In the proposed system the IDS runs outside the semi-trusted clouds and thus cannot be disabled by the insiders. The remote hosts initiates the remote VMI and VMs introspection is done with the help of VMI engine in the trusted hypervisor inside clouds. the remote offloading of the IDSes is done by the RemoteTrans along with the Transcall. Future work involves the performance analysis with a number of VMs running on a host and to introspect target VMs when there is large network delay [25].

X. Feng identified that APT and insider threats are forced by some incentives and proposed a non-zero sum three-player game model. The model is based on the Fliplt game model of two players. Firstly a scenario is considered where attacker is not clearly visible but the defender is visible. In second scenario a third person i.e. insider is introduced with a double role i.e. it can help defender as well as the attacker also. Different insights are derived for gaining the cost-effective defense mechanism [26].

I. Agrafiotis used real data of a MNC to test the CITD system for the detection of insider attacks. The statistical data was provided by the security head of the MNC. This data was used to update the system and make it more efficient. The PCA combined with anomaly detection using standard deviation was used to detect the attacks. Issue of scalability was identified while implementing the system on real data. Future work involves identification of problematic behaviour , which will help the policy makers to gain knowledge about the changes in the polices. The PCA approach with the three tier architecture successfully identified the attacks with less number of false positives alerts [27].

7. CONCLUSION

All the literature available (research papers, reports etc.) clearly indicate that the insider threat attacks should not be taken lighting. These attacks should not be underestimated. The organizations very clearly list on the numerous types of users which are capable to launch the insider threats; as well they also identify the vulnerabilities. Today the malicious insider attacks have become part of the real world and the destructing results are clearly identified.

Thus it can be concluded that the concern about the insider threats is increasing globally. But the time scale of detection of the insider threats is quite high; mostly in months. The need is to decrease the time in the detection of the insider attacks. Among the senior management respondents around nine out of ten (89%) gave the response that the vulnerability to the insider attacks is more as compared to the other attacks.

In CSA report 2010 V 1.0 the malicious insiders were identified as the top third threat but at that time no public example was available as per the report. But today in 2017 a numerous of public examples are available for the same. This fact clearly signifies that the malicious insider attacks are posing as a challenge to the organizations. Also in our earlier work we have identified the need of IDS for the cloud based environment [6]. While this paper presented a number of attacks against cloud authentication but the main aim is to highlight the malicious insider attacks concern because some of the issues are partially solved but these attacks requires further thought. Thus the future work is to provide mechanism to detect the malicious insider attacks in Cloud based environments with both the accuracy and timeliness.

REFERENCES

[1] Priya Oberoi and Sumit Mittal, "Review of CIDS and Techniques of Detection of Malicious Insiders in Cloud Based Environment", CSI - 50th Golden Jubilee Annual Convention, Publication in the Proceedings of the convention, Published by Springer under AISC Series in press

[2] Patil Madhubala R., "Survey on security concerns in Cloud computing," International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 1458-1462.

[3] Cloud security alliance ,"The Treacherous 12 - Cloud Computing Top hreats in 2016", https://cloudsecurity alliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016

[4] Cloud Security alliance guidance version 2.1, "Security guidance for critical areas of focus in cloud computing", http://www. Cloud security alliance .org/ guidance /csaguide.pdf,2009

[5] Cloud Security alliance guidance version 3.0 , "Security guidance for critical areas of focus in cloud computing" , http://www. Cloud security alliance .org /guidance /csaguide.pdf, 2011.

[6] Muhammad Kazim and Shao Ying Zhu, "A survey on top security threats in cloud computing", IJASCSA,International Journal of Advanced Computer Science and Application, vol 6, no.3, 2015.

[7] F. Fatemi Moghaddam, N. Khanezaei, S. Manavi, M. Eslami, and A. Samar, "UAA: User Authentication Agent for Managing User Identities in Cloud Computing Environments," in IEEE 5th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 2014, pp. 208–212.

[8] M. Ahmadi, M. Chizari, M. Eslami, M. J. Golkar and M. Vali, "Access control and user authentication concerns in cloud computing environments," 1st International Conference on Telematics and Future Generation Networks (TAFGEN), Kuala Lumpur, 2015, pp. 39-43

[9] Andrew Kellett ,"Vormetric insider threat report global edition",https://dtr.thalesesecurity.com/insider threat /2015

[10] "CybersecurityTrendsReport",https://www.Cyber security-insiders.com/portfolio /cyber security-trends-report, 2017

[11] Jon Oltsik, "The Ominous State of Insider Threats", https://www.vormetric.com/sites/default/files/ap_Vormetric Insider_Threat_ESG_Research_Brief.pdf

[12] Garrett Bekker, "2016 vormetric data threat report" , https://www.vormetric.com/campaigns/datathreat/ 2016

[13] "Data protection and insider threat", http:// www. veriato.com/lp/whitepapers/insider-threat-report , 2016

[14] "Defeating the Insider Threat and Shoring up the Data Security Lifecycle" , https://cloudsecurity alliance .org/download/defeating-insider-threat-survey/CSA , 2016

[15] H. G. Goldberg, W. T. Young, A. Memory and T. E. Senator, "Explaining and Aggregating Anomalies to Detect Insider Threats," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, 2016, pp. 2739-2748.

[16] A. Coden et al., "Uncovering insider threats from the digital footprints of individuals," in IBM Journal of Research and Development, vol. 60, no. 4, pp. 8:1-8:11, July-Aug. 2016

[17] T. Chen, T. Han, F. Kammueller, I. Nemli and C. W. Probst, "Model based analysis of insider threats," 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), London, 2016, pp. 1-3.

[18] Z. Abduljabbar, H. Jin, D. Zou, A. A. Yassin, Z. Hussien and M. A. Hussain, "An efficient and robust one-time message authentication code scheme using feature extraction of iris in cloud computing," Proceedings of 2014 International Conference on Cloud Computing and Internet of Things, Changchun, 2014, pp. 22-25.

[19] I. Khan; Z. Anwar; B. Bordbar; E. Ritter; H. u. Rehman, "A Protocol for Preventing Insider Attacks in Untrusted Infrastructure-as-a-Service Clouds.," in IEEE Transactions on Cloud Computing , vol.PP, no.99, pp.1-1

[20] S. Guha, S. S. Yau and A. B. Buduru, "Attack Detection in Cloud Infrastructures Using Artificial Neural Network with Genetic Feature Selection," 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/ CyberSciTech), Auckland, 2016, pp. 414-419.

[21] C. V. Neu, A. F. Zorzo, A. M. S. Orozco and R. A. Michelin, "An approach for detecting encrypted insider attacks on OpenFlow SDN Networks," 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, 2016, pp. 210-215.

[22] W. Meng, X. Luo, W. Li and Y. Li, "Design and Evaluation of Advanced Collusion Attacks on Collaborative Intrusion Detection Networks in Practice," 2016 IEEE Trustcom /BigDataSE/ISPA, Tianjin, China, 2016, pp. 1061-1068.

[23] J. Nikolai and Y. Wang, "A System for Detecting Malicious Insider Data Theft in IaaS Cloud Environments," 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, 2016, pp. 1-6.

[24] R. Gamble and S. AlQahtani, "Mitigating service impersonation attacks in clouds," 2016 Future Technologies Conference (FTC), San Francisco, CA, 2016, pp. 998-1007.

[25] K. Kourai and K. Juda, "Secure Offloading of Legacy IDSes Using Remote VM Introspection in Semi-trusted Clouds," 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2016, pp. 43-50.

[26] X. Feng, Z. Zheng, D. Cansever, A. Swami and P. Mohapatra, "Stealthy attacks with insider information: A game theoretic model with asymmetric feedback," MILCOM 2016 - 2016 IEEE Military Communications Conference, Baltimore, MD, 2016, pp. 277-282.

[27] I. Agrafiotis, A. Erola, J. Happa, M. Goldsmith and S. Creese, "Validating an Insider Threat Detection System: A Real Scenario Perspective," 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, 2016, pp. 286-295.