ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 4, Issue 1, January 2018

Retreat in distributed computing utilization of action log for client Statistics assurance

Shekhar.R[1], Sridhar.T[2]

Assistant Professor, Department of Computer Science & Engineering, Alliance University, Bangalore, INDIA [1]

Professor, Electronics and Communication Engineering, Alliance University, Bangalore, INDIA [2]

Abstract: ***Cloud security incorporate under its umbrella extremely broad arrangement of administration level assertions (SLA's), systems which are utilized to secure client information, applications and assets that are associated by means of cloud. Be that as it may, in any case the customers are incapacitated with next to no help and learning about what really happens to their information after they have pushed it on to the cloud. Information possession is critical issue, particularly while managing a gigantic measure of information. This permits cloud gives to make their own terms and conditions, which on occasion may appear to be self-assertive. We proposed a novel approach which will keep up logging and observing for helping cloud purchasers to distinguish any strange movement and resolve the issues as needs be. However, logging has a wide application as well, hence it relies upon the client how and what he logs and screens. To help the purchasers all cloud specialist co-ops keep up logs and produce a tremendous measure of data, quite a bit of which is excess, clumsily designed, yet there are shrouded pieces of information that can help the customer to comprehend that they are having, or all the more vitally, going to have an issue. Utilizing these logs the work makes a device which parses these logs and gives client the adept measure of data and enables them to comprehend their exercises and occupation conduct on cloud. It causes them to report any irregularity in the utilization of their cloud occupation and foundation adequately.***

Keywords—***Cloud Computing, Cloud security, OpenStack, Server node log, logging and monitoring***

I. INTRODUCTION

Cloud computing has become one of the fast-growing area under upcoming technologies. On-demand resource allocation is one of the reason why cloud has become very high in demand technology in current era [3][4]. For any organization reducing capital and operation expenditure is core area, on which management exercises to reduce, and this is the main drive of cloud computing. A possible definition of cloud computing is given at [1]. The main concern is about the data stored on the remote servers in the cloud cluster, the user assumes that data is secure and there are no other persons in between to access or control his data assuming that his data is kept private. But there is chance that the owner of the remote server may comprise on the user data since he or the organization have direct control on it. This definitely rises concern on how secure is our data in cloud environment.

Having all the benefits of cloud not everyone avails effectively in terms of security and resource utilization, many situations user does not have control on where his data loaded and under whose control it is in the cloud, nothing is visible to the user apart of web interface. Assuming cloud providers are honest in securing the data, but still they have malevolent system administers who have provision to tamper the data and violate confidentiality and integrity. After all internal security concerns, cloud still have possible traditional attacks where user data is at risk.

Many attempts are made towards improving the security on clouds and realizing the various factors affecting it. The work details the existing characteristics of cloud and identifies the issues and states some earlier proposals to mitigate the security issues.

The work focuses mainly on the Openstack cloud services and it encompasses. Openstack allows users to monitor their activities and helps them in recognizing any abnormalities. But, with its various facilities comes a set of codes implementation that is required to be done by each user to activate such security mechanisms. OpenStack allows the consumer, to allocate their resources within configuration limits set by administrators. The cloud services provide every end user with:- *OpenStack dashboard*: - is an web-based GUI, where the consumer/ user can manage and create his own resources within the configuration limits he has. *OpenStack command-line clients*: - which enables the consumer/ user to run commands for viewing , creating, and managing resources in a cloud.

Though Openstack sounds to be an effective medium of providing all resources to cloud consumers, still there are consumers which feel handicapped due to various reasons like, Incapability to understand the illustrated log files available to them. Lack of knowledge about the alerting and monitoring tasks. Unavailability of support from the cloud service providers as the data ownership is always under question.

To aid to the above reasons, designing a tool that helps the consumers by alerting them with abnormalities, showing them the apt amount of information from the verbose of log files and warning them about a potential problem, is the aim of the work. The tool works with the swift log files, swift being the storage component of Openstack. The log files contains log with various headers that helps in identifying with the help of useful headers what abnormalities can happen.

II. RELATED WORK

The general cloud architecture which is named as cloud stack [2]. Configured upon hardware infrastructure, cloud services are offered in various ways from the top to bottom layer. In the cloud stack, each layer represents one service model. Fig. 1 shows the architecture of a cloud environment.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 4, Issue 1, January 2018

Infrastructure-as-a-Service (IaaS) is offered in the bottom layer, where resources are aggregated and managed

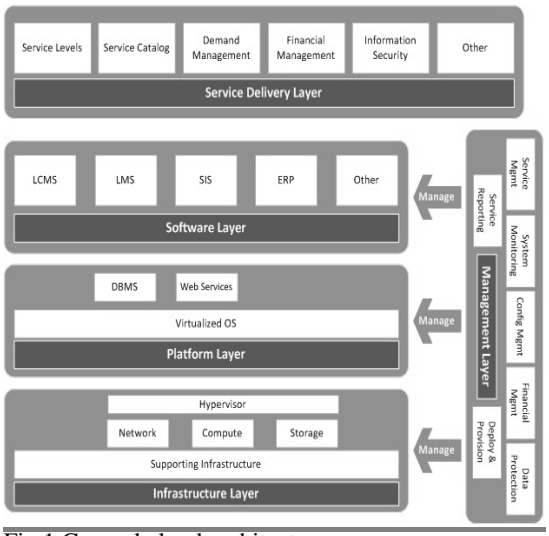

Fig.1 General cloud architecture.

physically (e.g., Emulab) or virtually (e.g., Amazon EC2), and services are delivered in forms of storage (e.g., GoogleFS), network (e.g., Openflow), or computational capability (e.g., Hadoop MapReduce). The middle layer delivers Platform-as-a-Service (PaaS), in which services are provided as an environment for programming (e.g., Django) or software execution (e.g., Google App Engine). Software as a Service (SaaS) locates in the top layer, in which a cloud provider further confines client flexibility by merely offering software applications as a service. Apart from the service provisioning, the cloud provider maintains a suite of management tools and facilities (e.g., metering and billing, dynamic configuration) [5]. The base delivery models for cloud environment are SaaS, PaaS and IaaS. There exists other delivery models such as IDaaS, CaaS, DaaS and ect. ; Cloud deployment models are Private cloud, Community cloud, Public cloud and Hybrid cloud; management models (trust and tenancy issues) -Self-managed and 3rd party managed (e.g. public clouds and VPC)

a. Cloud Characteristics

There are five essential characteristics of cloud, first one is *on-demand self-service* – consumer may raise a request for resource at any time depending upon his requirement, at this situation the resource has to be allocated to the consumer without alarming cloud provider. *Broad network access* – consumer can access his services via web based mechanism through heterogeneous network tools. *Resource pooling* – Cloud provider virtually pools unutilized resources such as storage, CPU time and network bandwidth from various sources and forms a virtual cluster. These resources are dynamically pooled and released to the source whenever required to make sure that the source resource provider do not face deadlock. *Rapid elasticity* – the capacity of resource requirement is variable form the consumer side, ie. Whenever the consumer need a resource it should allocated to him, at this situation all the resources maintained by the provider should be elastic in nature. *Measured service* – resources used ny the consumer are metered for the further billing purpose.

b. Cloud Security Challenges

With all its characteristics still consumer is rethinking on usage of cloud environment coz of its security issues. As stated earlier the main challenges for security on cloud is categorized as, Loss *of control* – leasing the third party environment will surely bring down the expenditure of an organization, but however this means the consumer/ organization is losing the control on his data and other acts. This is has become high concern for the consumer to rethink in security [7] and privacy of their data and other acts on cloud environment. *Multi-tenancy* – this means the data of multiple cloud consumers stored on same virtually pooled resource. When it is virtually pooled environment data of different consumers are placed on the same physical machine. In this case if one cloud consumer compromise on data access mechanism, there is a high chance that other legitimate cloud consumer's data is at risk. *Massive data and intense computation* – cloud is very capable of handling heavy data storage and task execution. The traditional security mechanisms are not sufficient for this type of environment. Although the self-managed clouds have some security issues the above mentioned ones exist mainly in third-party management models. A threat model helps in understanding a security problem, strategies in design and asses solutions. The steps in building the model focus on, Identifying attackers, assets, threats and other components, Ranking the threats, Choosing mitigation strategies, Building solutions based on the strategies. The threat may be from the insider or the outsider, the insider goals of attack are, *client* - Learn passwords/authentication information, and Gain control of the VMs, *cloud provider* -Log client communication, can read unencrypted data, can possibly peek into VMs, or make copies of VMs and can monitor network communication. The outsider goals of attack are, intrusion, network analysis, man in the middle and cartography.

c. Macro Level Security and Privacy Issues

The security and privacy issues on macro level can be expressed under following heads

Infrastructure Security- This is again divided into three sub heads i.e infrastructure level, user level and application level. *Data Security and Storage*- Numerous aspects of data security includes, Data-in-transit: Confidentiality + integrity using secured protocol, Confidentiality with non-secured protocol and encryption, Data-at-rest - Generally, not encrypted, since data is commingled with other users' data. Encryption if it is not associated with applications? But how about indexing and searching? Then homomorphic encryption vs. predicate encryption? Processing of data, including multitenancy, Identity and Access Management (IAM) and Privacy.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 4, Issue 1, January 2018

d. *Cloud Threats and Vulnerabilities*

Threats to Cloud Confidentiality are Cross-VM attack via Side Channels and Malicious SysAdmin. Threats to Cloud Integrity are data loss/manipulation and dishonest computation in remote servers. Threats to cloud availability are Flooding Attack and Fraudulent Resource Consumption attack. Threats to Cloud Accountability are SLA violation, Dishonest MapReduce, Hidden Identity of Adversaries and Inaccurate Billing of Resource Consumption.

VM co-residence: in cloud environment co-residence means, multiple cloud consumers stored their data on virtually pooled resource which may be physically same machine. This kind of environment has raised security issues, such as Cross-VM attack and Malicious Sys Admin. *Loss of Physical Control:* consumers have their data on third-party cloud servers, this means owners have lost their direct control on the data. Loss of control means the consumers are unable to face certain attacks. For example, data or software may be altered, lost, or even deleted; in addition, it is hard and unrealistic to guarantee data/computation integrity and confidentiality with traditional methods. *Bandwidth Under-provisioning:* A customary DOS/DDOS attack still exist in cloud computing with relative solutions in prior researches. Specific to cloud computing, there is a new type of DOS attack that takes advantage of the current under-provisioned cloud-computing infrastructure. *Cloud Pricing Model:* Cloud computing adheres to the pay-as-you-go pricing model that determines the cost of services in terms of metrics such as server hours, bandwidth, storage, etc. Since all cloud customers are financially responsible for the services they use, attackers always have incentives to harass the billing process by exploiting the pricing model. For example, Economic Denial of Sustainability (EDoS) attack manipulates the utility pricing model and causes unmanageable costs for cloud customers.

III. BUILDING THE TOOL

The tool is designed with the aim of giving user a helping hand in carrying out their activities on the cloud network. The tool provides a user to log into the dashboard of openstack directly thereby giving a hand to the level of security. Horizon itself provides a secure authenticated login to the end user. Every user of Openstack has its dashboard by default, which is accessible only by authenticated username and password provided to each individual end user. Once the end user logs into the horizon through the tool authentication page, the tool gives the authenticated user access to the log files with a click of a button. This then takes user to the filtered log file which contains information about the date and time the user logged in, the amount of bytes the user sent and received and the status of the users request. The user when finds any unidentified log entry is directed to raise a complaint for registering the anomaly with the cloud service provider. This helps the consumer by having a valid proof to raise the complaint and ask the service providers for the accountability.*TOOL Specification:* The tool is developed on NETBEANS 7.0 version as a Java Swing application. The tool runs on all platforms and as it is developed on netbeans 7.0 version with JDK 6. It requires the user to be an authentic cloud user with valid username and password. As the tool requires authentication every time the authentication is done using user's HORIZON credentials. This makes it mandatory that the user has Openstack to access the cloud on the system. Tool gets integrated with Openstack and then fetches the required data for an individual user from his account upon valid access.

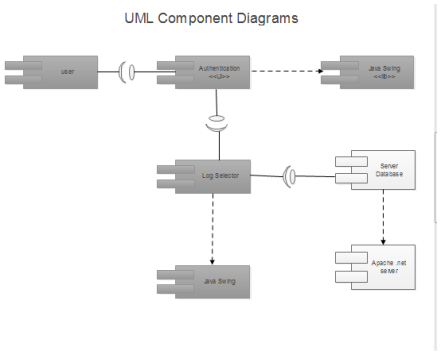

Fig 2. Component Diagram of the tool

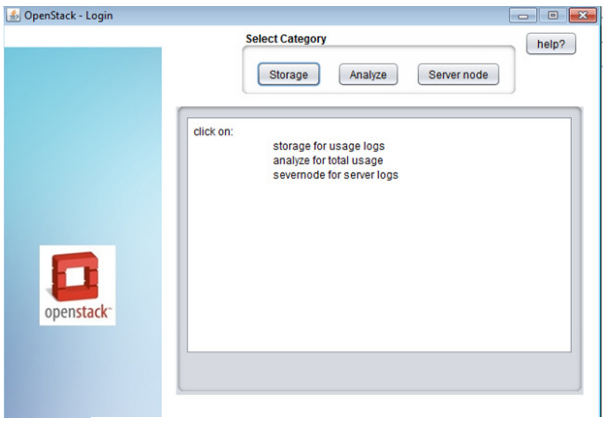

Fig 3. Screenshot of the selection Page

Fig 3 includes Authentication and Log selector as two UI components, Java Swing being the library component needed for both the UI components. The user component is connected to the Authentication component which acts as the entry point for the user into the software to access his logs. The authentication is dependent on the Java swing libraries to perform the assigned function and is then linked to the log selector which is linked with the server database from where the stored logs are fetched. The tool is comprised of two sections, AUTHENTICATION and LOG VIEWING. The authentication page after the successful login directs the user to the next page which allows user to view the logs on a button's click. *Login Page:* Following is the login page of the tool where the user enters his user name and password to login to his account.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 4, Issue 1, January 2018

The authentication method involves mapping of the username and password from the authentication page to the HORIZON authentication page which opens in the web browser. This helps user by saving from double login, once for the tool and once for horizon. The advantage of using this technique is that by this the security element can be inherited from the Openstack horizon itself. On successful authentication the following pop up message appears. The technique of web crawler is used in order to login the authentic user into his account. By using the web crawler one gets the HTML element of the web page, as HORIZON is web based we get the elements of HORIZON to fill in the fields of username and password. *Log Display :* This window helps the user by displaying the apt amount of information from the log files filled with the verbose. The headers fetched include the date and time stamp the status as well as the bytes sent and bytes received by the user. The user can configure what information or headers he wants to fetch from the logs and retrieve them.

The selection page contains three categories Storage, Analyze, Server node. The STORAGE button helps user to get the usage logs parsed, the SERVER NODE button helps in retrieving the server logs and ANALYZE button helps in analyzing the amount of data transferred.

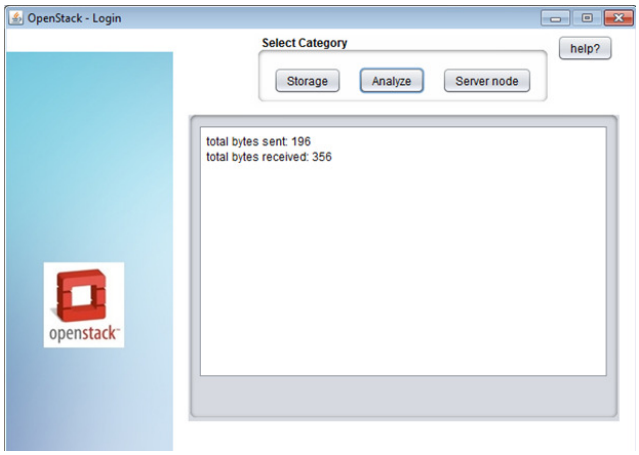

Fig 4: Screenshot of the page displaying the analysis made on the logs

Fig 4. Shows the storage log, shows the headers of bytes received bytes sent and timestamp from the storage logs. also shows the total bytes sent and received that is shown by the analyze button window.

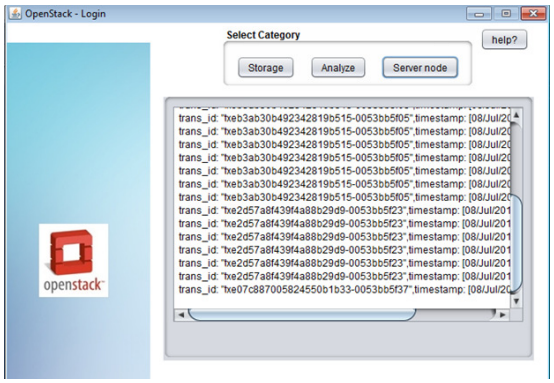

Fig 5: Screenshot of the page displaying server node logs

The above Fig 5 is server node logs containing all the nodes namely, Container, Object and account. The log analysis and parsing is based on simple pattern matching

Jul 8 03:00:28 saio swift_proxy: 192.168.56.1 192.168.56.1 08/Jul/2014/03/00/28 GET /auth/v1.0 HTTP/1.0 200 - curl/7.30.0 - 32 64 - tx0d3187a020bc4905bb497-0053bb5ecc - 0.0164 - - 1404788428.607697964 1404788428.624054909
Jul 8 03:00:34 saio swift_proxy: User: test uses token AUTH_tkb0bd609d7ab8423e951784f70b4e6208 (trans_id tx543e426000a4495fa729a-0053bb5ed2)
Jul 8 03:00:34 saio swift_proxy: User test:tester has admin authorizing. (txn: tx543e426000a4495fa729a-0053bb5ed2) (client_ip: 192.168.56.1)
Jul 8 03:00:34 saio account-server: 127.0.0.1 - - [08/Jul/2014:03:00:34 +0000] "GET /d2/710/AUTH_test" 404 - "GET http://saio:8080/v1/AUTH_test/" "tx543e426000a4495fa729a-0053bb5ed2" "proxy-server 1569" 0.0013 "-" 1568
Jul 8 03:00:34 saio account-server: 127.0.0.1 - - [08/Jul/2014:03:00:34 +0000] "GET /d3/710/AUTH_test" 404 - "GET http://saio:8080/v1/AUTH_test/"

using java. The logs are stored as static file which is fetched and then parsed in order to retrieve the needful information. The log files contain both server node logs and usage logs together with their own headers and structures. In order to gain the information from the files we have two configuration files as well which helps in getting the needed headers by each individual user.

Sample Log

The sample logs are from swift, they have three different types of log entries Storage Logs, Proxy Logs and Authentication requests. The proxy logs contain the log entries for bytes sent and bytes received whereas the storage node logs contains the information about the request method, request time and transaction Id. The above logs have entries for authentication requests which contains entries under the headers

a. Configuration Files

There are two configuration files used in order to select which headers are needed to be displayed. *Configuration File For Storage Log* - This file contains the headers from the storage logs and following is an example having few headers which are displayed using this configuration file.bytes_recvd request_start_time datetime client_ip bytes_sent

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 4, Issue 1, January 2018

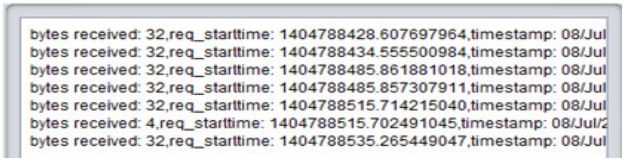

Fig 6. Configuration File for Storage Log

Configuration File For Server Node Log This file contains the headers from the Server node logs and following is an example having few headers which are displayed using this

client_ip remote_addr datetime request_method request_path protocol.
status_int referer user_agent auth_token bytes_recvd bytes_sent
client_etag transaction_id headers request_time source log_info
request_start_time request_end_time policy_index

configuration file. transaction_id datetime status_int.

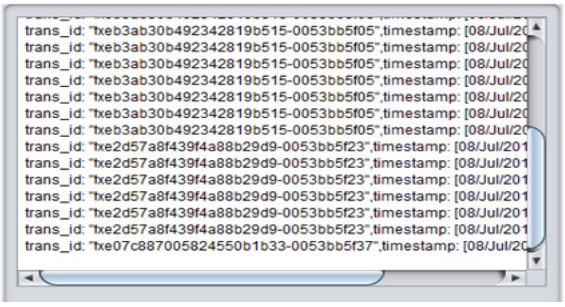

Fig 7. Configuration File For Server Node Log

IV. CONCLUSION

The work focuses on bringing out the threats on cloud security and various aspects of security issues which make the wide number of consumers reluctant to avail the benefits of cloud computing. Cloud computing is a huge umbrella encapsulating large amounts of applications and implementations. The advantages of it are pleasing but the threats and unreliability has made it a myth whether to believe in it or not. The consumer on the other hand suffers a lot because of the lack of trust as well as lack of control because of which building the trust is not only difficult but also an unachievable task as of now. Though service providers ensure the security at times but no solid steps are available with the user to account for. The project work tries bringing out the reasons and security issues therefore trying to enlighten the path for development of a more secured environment for all and consumers at priority.

The project defines the path of logging and monitoring as the way of knowing any threat or abnormality happening on the cloud with the user's data. The technique of log monitoring requires a set of commands to be written by each user and processed further. Not every user is aware of it and doesn't really possess the understanding of the verbose of log files thereby having a disadvantage in terms of monitoring and affecting his own security. The idea of a tool which sorts out the huge amount of information in the log files to display the apt amount of information for a user to judge whether or not there exist some threat to his data on cloud seemed helpful in the present situation. There is always a scope of improvement where the tool marks the step for a way to improve security and resolve the issue of data ownership on cloud.

REFERENCE

1. Nikos Antonopoulos, Lee Gillam, "Cloud Computing: Principles, Systems and Applications", Published by Springer.
2. Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," in IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843-859, Second Quarter 2013. doi: 10.1109/SURV.2012.060912.00182
3. Anand Darne1 , Rushikesh Longadge, "A Result Analysis on Secured Encryption in Cloud Computing using Symmetric Cryptography", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.7, July- 2014, pg. 680-688.
4. 'Resource Provisioning Methodologies: An Approach of Producer and Consumer Favorable In Cloud Environment', in the International Journal of Emerging Technology and Advanced Engineering, Volume 3, pp.8-13, Special Issue 4, October 2013 (ISSN 2250 – 2459 (Online), An ISO 9001:2008 Certified Journal) with Srinivasan R and Elijah Blessing Rajsingh.
5. Sagar B Patil, Pooja A Vhatkar, Jaya Gajwani, "Towards Secure and Dependable Storage Services in Cloud Computing",International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163, Volume 1 Issue 9 (October 2014)
6. L. M. Kaufman, "Can Public-Cloud Security Meet Its Unique Challenges?," in *IEEE Security & Privacy*, vol. 8, no. 4, pp. 55-57, July-Aug. 2010. doi: 10.1109/MSP.2010.120
7. A. Tripathi and A. Mishra, "Cloud computing security considerations," 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, 2011, pp. 1-5. doi: 10.1109/ICSPCC.2011.6061557
8. R. K. L. Ko, P. Jagadpramana and B. S. Lee, "Flogger: A File-Centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments," 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, 2011, pp. 765-771.
9. I. Ray, K. Belyaev, M. Strizhov, D. Mulamba and M. Rajaram, "Secure Logging as a Service—Delegating Log Management to the Cloud," in IEEE Systems Journal, vol. 7, no. 2, pp. 323-334, June 2013.doi: 10.1109/JSYST.2012.2221958

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 4, Issue 1, January 2018

10. J. H. Lee, M. W. Park, J. H. Eom and T. M. Chung, "Multi-level Intrusion Detection System and log management in Cloud Computing," 13th International Conference on Advanced Communication Technology (ICACT2011), Seoul, 2011, pp. 552-555
11. Nurul Hidayah Ab Rahman, Kim-Kwang Raymond Choo, A survey of information security incident handling in the cloud, Computers & Security, Volume 49, March 2015, Pages 45-69, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2014.11.006.
12. R. Vaarandi and M. Pihelgas, "Using Security Logs for Collecting and Reporting Technical Security Metrics," 2014 IEEE Military Communications Conference, Baltimore, MD, 2014, pp. 294-299.doi: 10.1109/MILCOM.2014.53
13. Suleman Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Muhammad Shiraz, Samee U. Khan, Rajkumar Buyya, and Albert Y. Zomaya. 2016. Cloud Log Forensics: Foundations, State of the Art, and Future Directions. ACM Comput. Surv. 49, 1, Article 7 (May 2016), 42 pages. DOI: https://doi.org/10.1145/2906149
14. S. Muthurajkumar, S. Ganapathy, M. Vijayalakshmi, A. Kannan, Secured Temporal Log Management Techniques for Cloud, Procedia Computer Science, Volume 46, 2015, Pages 589-595, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2015.02.098.(http://www.sciencedirect.com/science/article/pii/S1877050915001623)
15. Yi S., Qin Z., Li Q. (2015) Security and Privacy Issues of Fog Computing: A Survey. In: Xu K., Zhu H. (eds) Wireless Algorithms, Systems, and Applications. WASA 2015. Lecture Notes in Computer Science, vol 9204. Springer, Cham
16. W. K. Daniel, "Challenges on privacy and reliability in cloud computing security," 2014 International Conference on Information Science, Electronics and Electrical Engineering, Sapporo, 2014, pp. 1181-1187. doi: 10.1109/InfoSEEE.2014.6947857

Prof. Shekhar R has vast experience in teaching subjects related to Computer Science & Engineering. He has a post-graduate degree in Computer Networks and is Completed studies at the Manonmaniam Sundaranar University, Tirunelveli. He is serving as an editorial member of IJITCS, an international journal and has been a reviewer for several national and international journals. He is also a sitting member of different national and international associations in the field of Computer Science. His publications appear in many journals of national and international repute. His research interests include data mining-image mining, image processing, computer networks and artificial intelligence. He is currently working as Assistant Professor and Dy. HOD in the Department of Computer Science & Engineering at ACED, Alliance University.

Prof. Sridhar T is a dedicated academician with 28 years of teaching experience in the field of Electronics and Communication Engineering. Prof. Sridhar completed his Master's degree from UVCE, Bangalore and obtained his Bachelor's degree in Engineering from Andhra University, Visakhapatnam and is now pursuing a doctoral degree in the field of Low Power VLSI design from Visveswaraya Technological University (VTU), Belgaum. Prof. Sridhar is a life member in ISTE chapter and holds a diploma in Training & Development form ISTD New Delhi. He has received the CISCO certification in CCNA (Cisco Certified Network Associate) from CISCO Systems. He was a resource person for various guest lectures. He has also organized various technical FDP's, workshops conducted and hands-on training. He is currently working as Professor and Dy. HOD in the Department of Electronics and Communication Engineering at ACED, Alliance University.