Survey in data security of public cloud

Priya S. Patel[1], Nirav Shah[2]
[1]Student of Master of Engineering, Silver Oak College of Engineering, Ahmedabad, India
2Assistant Professor, dept. of IT, Silver Oak College of Engineering, Ahmedabad, India

Abstract- **Now a days, Cloud computing is a type of online based computing. Which gives shared computer dealing out resources and data to the computers? It is very challenging part to maintain the safety of all stored data which many users want to use in many applications. The stored data in cloud is so important that the users make ensure either the data is corrupted or lost. This work studies the problem of ensuring the mitigation and prevention of data storage in Cloud Computing. This paper, proposes to collect the data and store data in the cloud. The methodology followed is, when any user attempt any wrong password for three times the system take them as an unauthorized user and block the IP address. So, In future they cannot access applications from that IP address and if they are not unauthorized user then they have to send a mail to client so they will unblock the user.**

Index Terms- data security, cloud computing, cloud data storage

I. INTRODUCTION

Cloud computing is the combination of many preexisting technologies that have matured at different rates and in different contexts. The goal of cloud computing is to allow users to take benefit from all these technologies. Many organizations are moving into cloud because it allows the users to store their data on clouds and can access at anytime from anywhere. Data breaching is possible in cloud environment, since data from various users and business organizations lie together in cloud. By sending the data to the cloud, the data owners transfer the control of their data to a third person that may raise security problems. Sometimes the Cloud Service Provider (CSP) itself will use/corrupt the data illegally [1].

Security and privacy stands as major obstacle on cloud computing i.e. preserving confidentiality, integrity and availability of data. A simple solution is to encrypt the data before uploading it onto the cloud. This approach ensures that the data are not visible to external users and cloud administrators but has the limitation that plain text based searching algorithm are not applicable. In this paper, we discuss how to more secure data storage on public cloud [1]

II. LITERATURE REVIEW

1) Research on the Model of Big Data Serve Security in Cloud Environment. [1]
Year: 2016
Author: Hai-ting Cui Shandong Sports University Jinan, Shandong, China
In this paper the author uses a model of massive knowledge Security Service is recommend for big information suppliers, consumers and cloud service suppliers, so as to realize shared services of reliable knowledge security. Safety of technology framework is established from four levels together with an outsized resource set for looking, matching and packaging knowledge, massive knowledge resources decomposition modelling designing, trust analysis and improvement, and large knowledge rule, on the facet of privilege security mechanism, knowledge security, network broadcast safety and cloud storage security to guard massive knowledge.
Anyone doesn't have authorization to switch management log and record, only view. Cloud services and management of academics are common for managing cloud platform along with completely different authorizations; users embody college management, academics and students.

2) Research of Cloud Computing Data Security Technology. [2]
Year: 2012
Author: College of Information Science and Engineering, Henan University of Technology, Zhengzhou, China.
In this paper the author uses cloud computing applications and analysis reception and abroad still

advance cloud computing stage for consumers and knowledge exchange between the larger the quantity of consumer information broadcast and storing a security threat, a cloud computing safety is a crucial problem to be resolved. During this paper, all with state of encoding technology presents a cloud computing knowledge safety solutions, each to make sure safe broadcast of information to guarantee the safety of static information. The consumer must offer knowledge associated with cloud services (such as queries), the connected content also will be encoded before broadcast to the cloud; the utilization of all homomorphic encoding options, the appliance by the cloud of cipher text operations directly associated with the performance, then the consequence back to the top user. During this approach, each within the channel or medium, transmission or operation of all encoded knowledge, whetherornotpurloined, can't derive the initial knowledge or different helpful info. The program uses associate uneven encoding formula; you'll handover knowledge between multi-consumer securities.

3) Toward a Big Data Architecture for Security Events Analytic. [3]
Year: 2016
Author: Laila Fetjah, Karim Benzidane, Hassan El Alloussi, Othman El Warrak, Said Jai-Andaloussi and Abderrahim Sekkaki Computer Science Department Laboratory of research and Innovation in Computer Science University Hassan II, Faculty of Sciences Ain Chock Casablanca.
CloudComputing did come back up with such a big amount of engaging blessings like quantifiability, flexibility, accessibility, speedy application readying, and user self-service. But in discernment, Cloud Computing makes making certain security among these environments such a lot difficult. So ancient security mechanisms like firewalls and antivirus software's have well-tried lean and incapable of addressing the sheer quantity of knowledge and events generated among Cloud infrastructure. Herein, we have a tendency to gift an extremely ascendible module primarily based system that depends upon massive information techniques and tools providing a comprehensive resolution to method and analyses relevant events (packets flow, logs files) so as to come up with AN informative selections that may be handled consequently and fleetly. The objective of our work is to develop a whole answer for counterintelligence, named Advanced Persistent Security Insights System (APSIS), that depends on taking advantage of the standard capabilities of a SIEM system; that are information aggregation, correlation, alerting, dashboards, compliance, retention and rhetorical analysis, then exposing it to massive information with the appliance of counterintelligence so as to own additional correct read on what's happing on the infrastructure.

4) Big Data Analytics: Security and Privacy Challenges[4]
Year: 2016
Author: Youssef Gahi, Mouhcine Guennoun, Hussein T. Mouftah School of Electrical Engineering and Computer Science, University of Ottawa, 800 King Edward Ave., Ottawa, ON, Canada
Big information is employed by several organizations to extract valuable info either to require promoting choices, track specific behaviours or discover threat attacks. The process of such information is formed attainable by victimization multiple techniques, referred to as huge information Analytics. We highlight the advantages of huge information Analytics then we tend to review challenges of security and privacy in big data environments. Moreover, we tend to gift some offered protection techniques and propose some attainable tracks that change security and privacy in a very malicious huge information context. Big information is an honest basis for several organizations and governments in several sectors that shall mechanically method and extract valuable insights so as to assist call makes. However, the actual fact to gather and figure all potential and varied information could lead on to several security and privacy violations. Furthermore, we have a tendency to bestow some potential solutions and techniques that might facilitate securing this distributed surrounding

III. PROBLEM STATEMENT AND DEFINITION OF WORK

Increasing in users can lead in increase of hackers too. In such situation the admin has got to block several hacker information processing and also he has got to manage the resource allocation for brand spanking new users. Thus admin potency step by step decreases by failing to dam hackers and to assign needed resources to users. It had been ascertained once there's increase in variety of users, Admin fail to manage the method flow or doing applicable work. In a while Admin realize as a tedious job to handle with.so all the modules were properly extra to system to boost the system performance.

IV.PROPOSED SYSTEM

According to the analysis of different papers, Data security is major problem in current time. The cloud system is created then the server is infrastructure. The files are converted in the encryption and also store in the encryption format. The log is generated on the server how many times the consumer is visiting the application up to that the event and log generated for server. Identified the IP address on the network and analysis the events and manage the events. On the basis on log generation we can identified how many times the consumer are visited the application and if they are attempt the wrong password for more than three times then the alarm event is generated and represent unsuccessful event. If any user attempt the wrong password for more than three times the IP address for that network Is blocked.

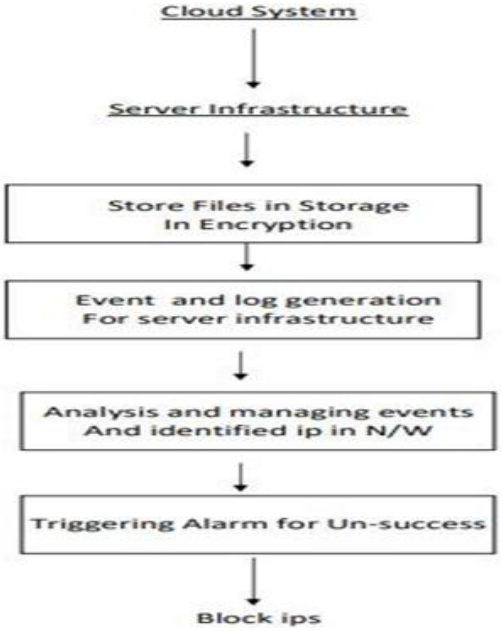
Cloud System
Server Infrastructure
Store Files in Storage In Encryption
Event and log generation For server infrastructure
Analysis and managing events And identified ip in N/W
Triggering Alarm for Un-success
Block ips

Fig: Flow Diagram

V.PROPOSED METHODOLOGY

Step-1: initialize AWS server

Step-2: setup python AWS cloud watch agent

Step-3: if file is empty, it isn't listed.

Execute "echo "month date time message" >> /var/log/myapp/request.log"

Step-4: define log analysis matric pattern

Step-5: define alarm for cloud watch log trigger

Step-6: define sns notification email (sns-simple notification service)

Step -7: setup subscription email

Step 8: setup goto3

Step 9: define input value A

A = ec2.send_command (Instance IDs)

Step 10: setup IAM auth

Response ec2.client.associate_iam_instance_profile

Step 11: if response == 3 add value in E1 E1 = file of IP collect.

Step 12: using IAM json policy denied

VI. CONCLUSION

Cloud computing provide the facility to store the confidential data but the security is important of data. Here we are providing the security, when any user attempts any incorrect password of login page for three times. The IP address of that user will automatically block and then after any user cannot login from that IP Address and we are also using the encryption and decryption for providing the more security.

REFERENCES

[1] Cong Wang, Qian Wang, and Kui Ren,” Ensuring Data Storage Security in Cloud Computing”, US National Science Foundation,2015, pp 1-4

[2] Raj Kumar, “Research on Cloud Computing Security Threats using Data Transmission” International Journal of Advanced Research in Computer Science and Software Engineering, India Volume 5, Issue 1, January 2015, pp. 399-402.

[3] Youssef Gahi, Mouhcine Guennoun, Hussein T. Mouftah, “Big Data Analytics: Security and Privacy Challenges”, IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, June 2016, pp 15-17.

[4] Laila Fetjah, Karim Benzidane, Hassan El Alloussi, Othman El Warrak, Said Jai-Andaloussi,” Toward a Big Data Architecture for

Security Events Analytic”, IEEE 3rd International Conference on Cyber Security and Cloud Computing , Beijing, China,2016,pp 1-7.

[5] Natalia Miloslavskaya and Aida Makhmudova, “Survey of Big Data Information Security”, 4th International Conference on Future Internet of Things and Cloud Workshops, Vienna, Austria, Aug 2016,pp 4-9.

[6] Suliman A. Alsuhibany,” A Space-and-Time Efficient Technique for Big Data Security Analytics”, vol. 46, no. 2, Riyadh, Saudi Arabia, pp.241-284, 2016.

[7] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik,“Scalable and Efficient Provable Data Possession,” Istanbul, Turkey Proc. of SecureComm ’08, pp. 1–10, 2008.

[8] Saakshi Narula,” Cloud computing security: amazon web service”, Fifth International Conference on Advanced Computing & Communication Technologies, Haryana, India, Feb 2015,pp 699-703

[9] I.Somerville, Software engineering, 9th edition, vol.ISBN 9780 1370 35151.Adison Wisley publishing company, 2010.

[10] Manikandan Shanmugam , Prof. Monisha Singh “A Comparitive Study Traditonal Healthcare System and Present Healthcare System Using Cloud Computing and Big data”, International Conference on Signal Processing and (INDIACom), pp.2108-2112, 2016.

[11] Lalitha V.P ,Sagar M.Y,Shranaappa S,Shredar Hanji,Swarup R,”Data Security In Public Cloud “International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017)