Cloud Computing Data Breach

Abdalla Alameen

Department of Computer Science, College of Arts and Sciences
Prince Sattam Bin Abdulaziz University,
Wadi AdDawser 11190, K.S.A.

Abstract - *Nowadays, Cloud Computing services extend to all businesses due to their benefits and easy usability. The most important issue of cloud is security. Due to their advantages, most business are now using these cloud computing applications, with data being stored and used through their cloud computing application. As these cloud services providers are resources for data, security is primary for maintaining their integrity and privacy. This paper has focused on issues related to the data breach. Data breach occurs because of various loopholes present in the entities of cloud computing. We have discussed issues which can help the researchers to apply new methodology to overcome the threats*

Keywords —*Cloud Computing, Data Breach, Virtual instances, API, DDoS.*

I. INTRODUCTION

Cloud computing is used as architecture for enterprise network because it enables clients to pool crucial resources such as network elements, central processing units, memory and network interface on their priorities (which is called resource elasticity); usage based pricing and standard architecture[1-4]. A major contribution of this technology is data that is being outsourced to the Cloud Service Provider (CSP). Thus, this type of service of storing data brings relief to the IT administrator and enterprises. It also avoids capital investments on software, hardware, and personnel. On the other hand, these types of services are executed in a much secured manner so as to keep the integrity and privacy of the remotely saved data [5-8]. Yet, there are some circumstances where remote data is compromised. There are some reports of CSP deleting unused data and also never went public about data loss (to keep good repo). However, remote data storage also brings risk apart from the benefits. CSP can use cloud auditing techniques to keep privacy and integrity of the remote data [9-16]. Cloud Auditing can perform audit of the remote stored data. However, it is not a service to avoid data loss. Cloud data loss can be result of loophole present in the framework of the Cloud data center [17-21].

IBM and Ponemon Institute have released a report on security breaches of Cloud Service Providers (CSP), which cost clients approximately $3.795 million in 2015. Furthermore, Data breach happens because of 92% of hackers, 17% of insiders, less than 1 % business partners and more than 17% of involvement of multiple parties [22]. Major percentages of hackers, breach the cloud data because various reasons. These threats are illustrated in Figure 1. Threat to the remotely stored data is from each and every entities of cloud itself. Hence in this survey we show existence of problems in various appliances of Cloud architecture.

Threats and data breaches have always been a concern for the CSP. There are many forms of threats for the CSP. These threats not only hamper cloud services but also cause the cloud to be considered an un-trustworthy platform for data storage [6-19]. The Cloud Security Alliance released an online magazine called The Notorious Nine regarding the threats faced by cloud providers. Data loss is considered to be the top ranked threat. Furthermore, it is also reported that data stored on a reliable cloud can also be in danger; it could eventually be lost for various reasons, including accidental deletion by the cloud provider. Natural calamities, such as earthquakes, fires and other disasters, could cause user data deletion from the cloud.

This research provides a systematic guide to the present state of the literature, in view of the comprehensive issues present in the Cloud computing architecture. This survey not only identifies and categorizes these threats, but also compares and analyzes their destructions to the cloud and its entities. For example, our research work lists weaknesses of the earlier work on cloud architecture, to enable researchers to design new methods and architecture in the future. Related topics, such as providing programming and approaches to the Cloud, are beyond the scope of this paper. Cloud data protection is a different concern and, therefore, needs obvious consideration.

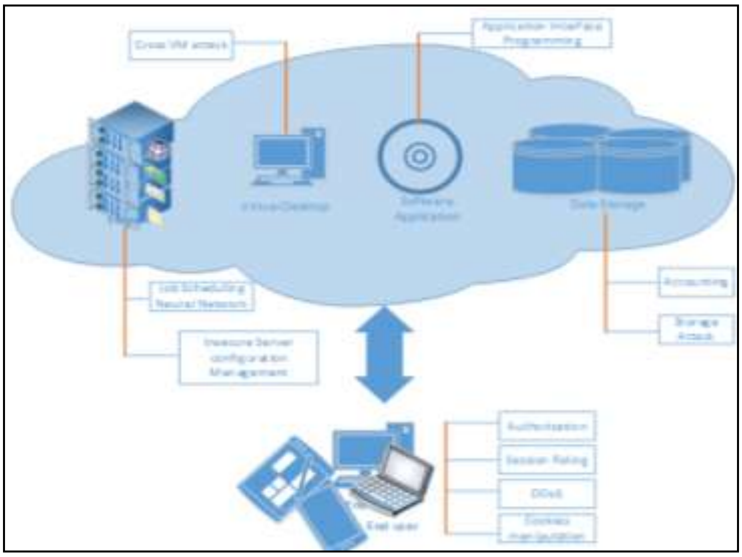

Figure 1: Cloud Data Threats

II. Data Breach

Control of remote data is ceased to the CSP once it uploaded to their cloud by the client. So hence, financial records, health records, social networking profiles, and corporate information are no longer private data. However, this kind of data storage is protected by various means of networking and internetworking tools. Very recently, breach incidents have been reported from organizations such as Sony Pictures, Home Depot, Adobe Systems, Drop Box, UC Berkeley and Top face. The main root causes for the data breach are classified as malicious, system failure and human factor (https://www4.symantec.com).

CSP can use cloud auditing techniques, to keep privacy and integrity of the remote data [6-19]. Cloud auditing requires two to three entities to perform data auditing. These entities are classified as user/client, auditor, and server (where the data is stored). Users issue request to the auditor to perform auditing, then auditor issues challenge to the server, in turn server releases the proof for the challenge. Finally, the verification is performed for the block of data. All these cloud auditing techniques use cryptographic methods and classified as Message Authentication Code (MAC), Homomorphic authentication and Boneh-Lynn-Shachan.

CSP and data privacy and data integrity is at stake and it has opened innovative door for research opportunities. Hence, to cope up with threats, CSP and Cloud users should prepare in advance to act against threats before they hit the CSP and Cloud users [23]. They also suggested of preparing a strategy document about risk management and this document should be reviewed by stakeholders. Furthermore, we should mount continuous pressure on the threat actors and also keep watch on the privacy and security issues arose from the changes in the policies [24]. This is also a opportunity for researchers for applying new scientific methods to overcome cloud data breach issues caused by the threat actors.

A survey paper [25] has come out to following few guidelines to avoid data breach issue such as gaining the confidentiality of customers (Demographic questions), user habits, & frequency of internet usage, developing security issues, collecting the feedbacks of customers frequently.

Researchers of [26] have come up with certain solutions like users must be aware of current systems, governmental policies to be developed, educating the users in terms of security and so on. Sometimes users often face the problem of data storage over various clouds irrelevant to localization. To overcome this issue, paper [26] had a good approach of verification of distributed databases, updating, deletion, viewing of data on demand with restrictions by issuing the tokens.

Scientific only solutions might not to protect remote data against breach and privacy and integrity of cloud data. However, humanities and social science contributors can also render expertise on these issues [27]. Following sections, under data breach, we have categorized various threats entities related to the cloud described. Figure 2 shows all the categories mentioned in our research paper [20].

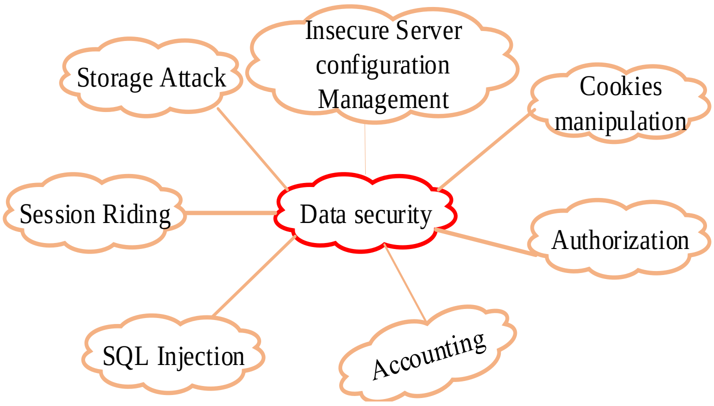

Figure 2: Cloud Data Threats

a. *Insecure Server Configuration Management*

Cloud servers are rented out as pay per basis by using virtual instances. Virtualization is software sits between physical network and cloud users. It is the fundamental technology that empowers cloud computing. Virtualization allows cloud service provider to run multiple servers using Virtual Machine (VM) over a single hardware system. To run these multiple high end server, administrator requires programming the configuration files to suit with Cloud client’s requirement. Misconfiguration of Web server’s files, application server’s files, and network service configuration files will be vulnerable to threats. These configuration files are responsible to invoke remote applications using request-reply sessions between server and clients. These request-reply primitives are required by the cloud computing services to store data, directory services, email services and more. Hence, erroneous configuration files leads to variety of security concerns. However following measure can be taken to avoid security threats:

- Alerts on logins
- Unused services should be off
- Proper usage of service by security mechanisms
- Access controls
- Vertical Heterogeneity (mobile devices).

However, cloud architecture provides the complete configuration of web server files, to offer best services still there is a big issue comes to configure or update these server files as discussed in paper [28]. An appropriate approach has been discussed in paper [29] that is file monitoring techniques over the cloud by virtual machines or users. As we are aware that there is interconnection of one cloud with millions of cloud servers, so it will become very difficult to monitor and configure each file by means of virtual users. Further because of mobile devices, that are connected to a cloud for supporting heterogeneity and it is named as mobile cloud computing. In such ad-hoc environment virtual machine should be configured to support interoperability, portability, and integration among mobile devices. Because mobile devices are built using various operating systems, however to unify them on the Cloud environment, administrator and developer have to be aware of configuration through XML languages, or any suitable configuration files [30-31].

b. Storage Attack

Cloud data storage system stores sensitive information, either in a database or Google cloud's Bitable and Microsoft's Azure blob. This service is ideal for the web based applications, mobile applications and Internet of Things. These storage systems are developed and usually integrated with Apache's HBASE and Hadoop. This combination requires configurations files to be synchronized with region server and cluster, which are geographically distributed. A few configuration mistakes are commonly made that includes:

- Improper storage settings
- Storage Correctness Guarantee
- Privacy Preserving Guarantee
- Security Guarantee for Cloud Data Auditing
- Poor choice of encryption methods and security methods.

Storing large amounts of data in the cloud computing environment raises many concerns about data protection [32-35]. Data integrity and privacy can be lost because of the physical movement of data by the cloud administrator from one place to another, malware, dishonest cloud providers, application programming Interface (APIs) and other malicious users who may distort the data. However, there are instances of accidental data deletion and data removal from the cloud [33-34]. Data auditing is an age-old process to verify saved or preserved data. Cloud data auditing enable CSP to keep client data in a secure place but also to maintain its privacy and integrity [9] as shown in the Fig 3. Hence, it becomes obligatory to verify saved data corrections at regular intervals. Now, with the help of cryptography, the verification process is performed for remote data by delegating a third party auditor [TPA] [9]. This research focuses on the cloud data auditing algorithms and the issues (Integrity and privacy) faced by these algorithms while performing cloud data auditing.

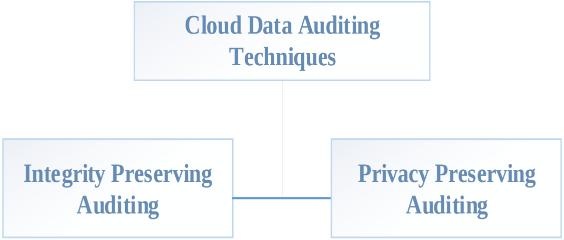
Cloud Data Auditing Techniques
Integrity Preserving Auditing
Privacy Preserving Auditing

Figure 3: Cloud Data Auditing Techniques

c. Session Riding

A malicious user creates malicious web addresses and disseminates them through website or by email, expecting users to navigate through link and run the malicious code. If this code successful by passes the firewall, the actions that are enveloped inside the link will be executed under the privilege of user level. With respect to Cloud computing, few options are available for cloud client to interact with the Cloud server or provider. These tools are Web-browser and programmed graphical user interface. Web-browsers usually keeps frequently accessed data in their buffer which is called cookies. Whenever user visits the same page, it enables faster access to session by means of cookies. These sessions of Web transaction use HTTP protocol, by nature it is a stateless session. However, these technologies require session state is required for session handling. These sessions create room for the session hijacking and session riding for the threat actors. Hence, Cloud computing is also cannot eradicate session riding issue of web technology.

Steeling of the session keys or cookies is possible to the third party as mentioned in the reference, because of insecure cryptography, data protection & portability, ease of using the web services, in secure data transmission & user interfaces, shared public & private keys, data loss or breach, lack of user awareness to use the web applications and lack of improving Artificial Intelligence (A.I.) techniques.

Causes of session riding according to [36]:

- Illegal admittance to GUI.
- IP protocol weaknesses.
- Backup Weakness.
- Cloud Policy of usage(pay per basis and billing)

d. SQL Injection Attacks

SQL stands for Structured Query Language mainly used to frame the queries to retrieve the data from the database. This language widely used for many challenges and cloud computing is one among them. SQL injections are a method of injecting the SQL commands or statements to databases for data driven applications. SQL injection attacks are the latest threats which are being affected to CSP, confidentiality to the data being stored, integrity, auditing algorithms and so on. SQL injections change the meaning of SQL statements to steel the data. These Injection codes will be executed at

Application layer. When the client wants to access any data, he submits the request which will be encoded into SQL query and submitted to the database for verification if it is valid then the client is allowed to access the data else then he fails to access. CSP may stores the data in many data bases from where the data can be retrieved by various stakeholders like customers, clients, servers and many more. It is very difficult to predict what kind of data being driven by the stakeholders to meet his applications then how to provide the complete SQL statements with its parameters is very serious issue. Protecting all the cloud applications & its infrastructure against SQL injection attacks became a major issue for any organization. Though many applications or development had done in this area, still protection of cloud architecture & its applications stands to be more severe problem. Few issues which are commonly encountered below related to cloud computing.

Cloud Computing Adoption Framework (CCAF) is responsible for multil-layered security but enables to prvide completley. Problems which may araise like predicting and writing the privileged Sql queries to be returned from the database by the server on the stakeholders request. A problem which may arise due to SQL Injections like Validating the SQL statements with proper parameters is very difficult issue. Returning the SQL error messages helps the malicious user to predict the queries. Validating of databases tables' width their names is another main issue [37]. To protect from the malicious attacks on the cloud it has been recommended to maintain web server log file which maintains table of malicious users' with their relevant links with referred to [38] but it is very difficult to maintain the log table for all malicious users with their relevant links as they are in millions. Maintaining the web server log file may increase the issues like identification of GET and POST methods of database connectivity for different queries are more difficult. Generation of dynamic nested queries across CSP for various databases has to be identified. Encoding & decoding of different cryptographic algorithms to be used by auditor is more complicated. Basic communication or connectivity to the cloud is password and user name, hence, these mechanism are week due to [36] unprotected user behavior (weak passwords, frequently changing passwords), and Also, the verification application has flaws, permit interference, and replay over cloud applications.

e. Authorization

Security of authorization is also very burning issue in the area of cloud computing and online applications. Authorization means of providing confidentiality, integrity, & availability to all cloud applications. As seen in the figure 1 at core level like cloud infrastructure which includes storage areas, servers, networks (internet, intranet, inter cloud) and so on while coming to application level we have auditors who will resolve the issues at client, server, third parties and so on. Authorization is to be provided for managing the risks at each level from core level to application level. Much advancement has done in the security authorization still we need to accomplish the challenges in the areas like API & Cloud Computing.

To provide the proper authentication, paper [39] proposes Kerberos are used for reliable authentication over insecure Cloud between the users. In [40-41] the cloud computing environment allows the third party to access the computing resources like networks, servers, storage, applications, and services. In order to avoid the misuse of these resources, cloud management system should provide & prepare a Service Legal Agreement (S.L.A.) to all the users who access the cloud. However to maintaining the S.L.A of all the users is another issue [42]. The cloud architecture should provide the authorization in terms of mainly three services as discussed in paper [2] they are firstly Cloud Software as a service (SaaS) : (these are the services or user interfaces built by the vendor which are distributed over cloud), secondly Cloud Platform as a Service (PaaS) (These gives the platform for the clients & servers to deploy their applications) at last but not the least Infrastructure as a Service (IaaS) (It gives facilities for client & servers to store, process networks, and other fundamental computing resources). The unique identification of users over cloud is very much essential, to resolve this issue paper [42] focus on Digital signature based authentication scheme which can be implemented by distributed key management. Using Digital Signature may have the issues like generation of private keys & its confidentiality, verification of both public & private keys which requires powerful authentication or cryptographic algorithms, keys expiry, maintaining certificates, compatibility. To provide strong authentication over cloud paper [43] proposes Role-Based Access Control in Cloud Computing which works by identifying user agents over the cloud, defining their roles, providing permissions, protecting objects. As we know cloud, it is an interconnection of millions of other storage servers, so identification of agents is not a simple task. In [44], authorization model has proposed for cloud computing which provides systematic role-based access control.

f. Cookies Manipulation

When users visit any website, cookies will be created to keep a tack of movements performed on the website by the user. Cookies will help the protocol in accessing where he left off. For example if we login in a web page it store the login credentials, so that if we try to log on for the next time it gives the login credentials automatically. Cookies can also be defined as memory of browsers which keeps the accessing history. Main advantage of cookies is faster execution; keep history of accessing, identification of user with server and many more. Managing cookies can be differently for different browsers like Netscape navigator, google chrome, internet explorer, fire fox, safari, and opera and so on. Some of the issues related to cookies needs much advancement in cloud computing is confidentiality to maintain browsing history of each user, integrity constraints of cookies, session expiry of cookies, compatibility with various operating systems & electronic gadgets. Furthermore, cookies play a major role for subsequent communication across HTTP (hypertext transfer protocol) connection. Hence, cloud computing architecture needs secure way of keeping cookies free from threat actors. Cloud computing servers, they identify who visited them. For example, if a cloud client visits the cloud website, client's records such as names, financial records and credit card numbers, site uses cookies to store all these information. However, by storing these data in cookies will exposes client records to the threat actors. Hence, in [45], researchers have proposed to store such information in a simple customer ID number. Authors [46] have proposed to use cryptography to secure the cookies. Message authentication code (MAC) and HMAC (Hash based MAC) can be a good choice for cookie-issuing server for creating security keys and these keys are kept in Seal_cookey it's a variable for private key.

III. Application Programming Interface (API)

Figure 4, illustrates API communication between server and end-user application. API's are sets of routines, agreements, and tools for building software applications. API sends requests and receives responses among different software's in terms of commands, program, function, routine, parameters and so on. API's is defined as set of routines, agreements, tools for building software applications on platforms like windows and Linux. APIs are well known in providing infrastructure in terms of software for hosting services of both client & servers. API's may meet the wide variety of applications form development techniques to business applications. It plays a major role in developing the Graphical User Interface (G.U.I) by the programmers to meet the demands or applications for its stake holders. This API's communication not only intended with software routines but also hardware devices like sending prints from different application editors to printer, sharing the files between different systems and many more. The API's have its applications in the areas like Global Information systems (GIS), Databases, developing web services, virtual environment for the users to develop any real time or business applications and security based services running over Cloud computing. However, Cloud application executions are likely to fail because of unresponsiveness, return errors, unexpected output or no output at all [47]. Regarding data breaches, API failures may be invoked when a client machine becomes unresponsive for a certain period of time or an indefinite period of time. There are plethora of research work is carried out on the latency issues of API.

Research on system operations has focused on reducing errors and repair time rather than investigating latency issues [48-49]. But, cloud clients have very limited access to the cloud infrastructure by means of API. Therefore, API's operation depends on API call reliability [47]. According to [47], they have classified errors in the API as contents are missing and wrong content fetched. This may become a major issue regarding their use in the cloud. During APIs unresponsive, hackers can use this communication channel for their own interests. Collectively, it can be concluded that APIs should be standardized for the cloud computing environment so that return errors and other important non-communication channel failure errors on unresponsive systems can be debugged properly to arrive to a viable solution to this security issue.

As discussed earlier API are very much needed to service the needs of clients & servers. With reference to scalability is the most important factor in development of API which takes cares of growing amount of work by the client and server queries [1]. To improve these API Cloud architecture very much needs to develop few network protocols to make connection between various clients accessing to same server one at a time. In [19], they have suggested a Cloud resource interfaces that keeps APIs away from useful resources usage.

Cloud client uses their own interfaces to interact each other which raise the issue of insecure interfaces whose impact may be malicious activities, unauthorized access, week authentications, and data tampering and so on. To overcome this impact it's very much needed to design and implement the interfaces which work on virtual systems. We also suggest to develop some encryption techniques to handle insecure interfaces [2, 5]. In order to minimize the effort of programmers for building the user interfaces, much software components needs to be developed by using API which brings all the programmers to build their own applications on cloud and deploy them as referred in [3]. One of the important concern in the area of cloud is Service Legal Agreements(S.L.A.) which ensures about the Quality of Service QoS i.e. functionality to be provided to its users but after some time they are unable to provide it as mentioned in the S.L.A's [4]. There is a much need of improving the QoS parameters while making S.L.A's. As cloud computing became vast area, much advancements has been carried in the last decades it has been found that cloud has good Service Oriented Architecture (S.0.A.) This consists of much hardware and software resources. Due to some reasons these resources may have problems like fault tolerance, reliability, software components managements, optimization of scheduling algorithms, monitoring and providing proper sequence of Graphical User Interface (G.U.I) is still lagging and needs much advancements as discussed in [6].

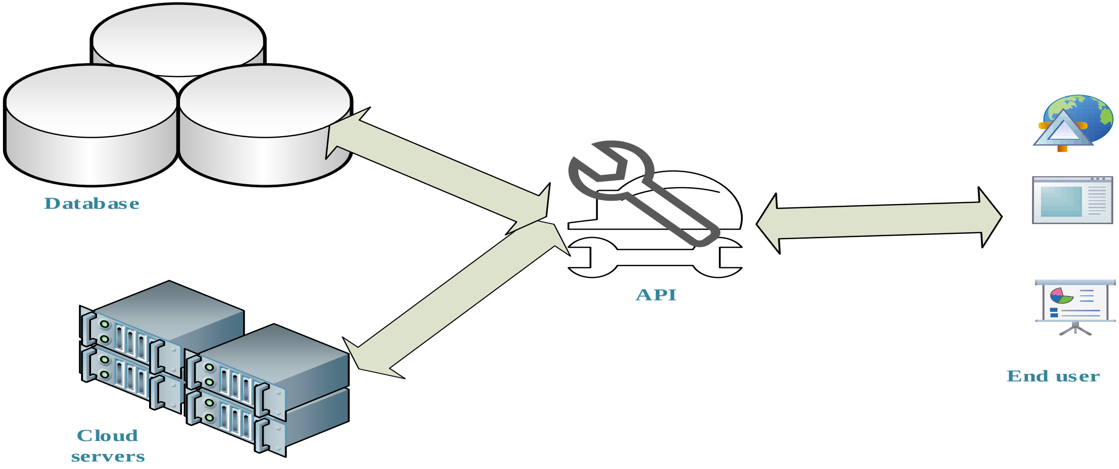

Figure 4: Application programming Interface (API)

IV. DENIAL OF SERVICE OR DISTRIBUTED DENIAL OF SERVICE

This is the most common form of threat faced by CSPs. In a Denial of Service (Do's) attack, intruders attack the cloud infrastructure to disable it or to cause the cloud service to become unavailable [55]. It is a systematically planned attack wherein the attacker floods the cloud network to prevent the cloud provider from offering services. There are many planned attacks that can be initiated on the cloud infrastructure, such an ICMP flood, a SYN flood, teardrop attacks, peer to peer attacks, cloud resource utilization attacks, application-level attacks, nukes, HTTP post attacks, and UDP and NTP attacks. There are also many cloud service based attacks, such as through VoIP cloud services, multimedia, and cloud storage. There are many DDoS attacks that are also specifically planned for cloud service providers, including network and transport level flooding. This attack consumes bandwidth and resources in the CPU, memory, disks or databases; hence, it defeats the idea of cloud elasticity. Attackers carry out their attacks on cloud providers to achieve financial gain, seek revenge, intellectually challenge themselves, or participate in cyber warfare [55]. There are many solutions offered to protect against DoS/DDoS attacks, but the offered solutions might be unable to differentiate between legitimate clients and victims because of the nature of DDoS attacks [42]. Some researchers have suggested the use of Random Early Detection methods to prevent DoS and DDoS attacks, but these threats are still flourishing on the infrastructure [42]. There are some solutions that have specifically been designed to prevent DoS and DDoS, such as intrusion prevention and intrusion detection systems.

The major attacks on cloud computing due to DDoS attacks according to paper [34] major reasons are broad network access, excess in pool of resources, on demand self-service and so on. Ultimate solution to come up with a proper Service Legal Agreement (S.L.A.).Few remedies recommended in paper [56] to avoid DDoS attacks are prevention, monitoring, detection, and mitigation.

As previously mentioned, cloud security issues can somewhat be controlled and prevented. Malicious insiders, on the other hand, cannot be completely prevented from disrupting services; they are often difficult to identify while sharing secret data with untrusted people. This is the most popular type of attack for which a solution is difficult to find because the attacker typically operates within the system. The CERT Coordination Center at

Carnegie-Mellon University, USA, has started a training program regarding insider threats. Awareness is the key to avoid this threat; as experience with insider threats grows, more threats can be analyzed and avoided. Hence, CERT has a database of insider threats, and this database, the control, and the indicators can be derived from insider threats to the cloud infrastructure. Furthermore, a case-by-case analysis would be helpful to understand the psychological and mental movements for this particular threat. Organizations and human resources can increase their efforts to bring awareness to and inform employees of the consequences of this type of personal or corporate data breach. It is also reported that many insider threats originate with employees who left an organization and joined a competitor or with employees who were not compensated for services that they rendered a company for greater profits. These issues can also be avoided by enforcing guidelines for the sharing of personal information with colleagues, engaging in appraisals, routinely training employees, and publicly praising employees in front of other team members. In-house training on psychological behavior and mental health is also a key ingredient to mitigating this type of threat.

V. CONCLUSIONS

This paper systematically studies the issues present in the Cloud architecture. Future work on this architecture and new methods of communication services should be suggested. This review article will help the research community to develop a more secure way to protect cloud data.

REFERENCES

[1] Abdalla Alameen , 2015, Building a Robust Client-Side Protection Against Cross Site Request Forgery, International Journal of Advanced Computer Science and Applications(IJACSA), 6(6): 64-70.

[2] Mell, P. , & Grance, T. 2011. The NIST definition of Cloud Computing, The National Institute of Standards & Technology, U.S. Department of Commerce.

[3] Rochwerger, B., Breitgand, D., Levy, E., Galis, A.,Nagin, K., Llorente, I.M., Montero, R., Wolfsthal, Y., Elmroth, E., Caceres, J., &, Ben-Yehuda, M. 2009. The reservoir model and architecture for open federated cloud computing, IBM Journal of Research and Development. 53(4): 535-545.

[4] Pallis, G. 2010. Cloud computing: the new frontier of internet computing, IEEE Internet Computing, 1(5):70-3.

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

[6] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. 2011. Enabling public auditability and data dynamics for storage security in cloud computing, IEE Transactions on Parallel and Distributed Systems, 22(5):847-59.

[7] Chen, Z., Dong, W., Li, H., Zhang, P., Chen, X., & Cao, J. 2014. Collaborative network security in multi-tenant data center for cloud computing. Tsinghua Science and Technology, 19(1): 82-94.

[8] Tari, Z., Yi, X., Premarathne, U.S., Bertok, P., & Khalil, I. 2015. Security and Privacy in Cloud Computing: Vision, Trends, and Challenges, IEEE Journal of Cloud Computing (2):30-38.

[9] Wang, C., Wang, Q., Ren, K., & Lou, W. 2010. Privacy-preserving public auditing for data storage security in cloud computing. In INFOCOM-2010, Proceedings of 29th conference on Information Communications, 525-533.

[10] Wang, C., Ren, K., Lou, W., & Li, J. 2010. Toward publicly auditable secure cloud data storage services. IEEE Network, 24(4):19-24.

[11] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. 2011. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 22(5):847-59.

[12] Yang, K., & Jia, X. 2012. Data storage auditing service in cloud computing: challenges, methods, and opportunities, World Wide Web, 15(4):409-428.

[13] Wang, B., Li, B., & Li, H. 2012. Oruta: Privacy-preserving public auditing for shared data in the cloud. In Proceedings of IEEE 5th International Conference on Cloud Computing (CLOUD), 295-302.

[14] Yang, K., & Jia, X. 2013. An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 24(9):1717-26.

[15] Wang, B., Li, B., & Li, H. 2012. Knox: privacy- preserving auditing for shared data with large groups in the cloud, Applied Cryptography and Network Security, 507-525).

[16] Wang, Q., Wang, C., Li, J., Ren, K., & Lou, W. 2009. Enabling public verifiability and data dynamics for storage security in cloud computing. In Proceedings of 14th European Conference on research in computer security, France, 355-370.

[17] Xiao, Z., & Xiao, Y. 2013. Security and privacy in cloud computing. IEEE Communications Surveys & Tutorials, 15(2):843-59.

[18] Takabi, H., Joshi, J.B., & Ahn, G.J. 2010. Security and privacy challenges in cloud computing environments, IEEE Security & Privacy, 1(6):24-31.

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

[20] Subashini, S., & Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing, Journal of network and computer applications,34(1):1-1.

[21] Pearson, S. 2009.Taking account of privacy when designing cloud computing services.In Proceedings of the 2009 ICSE Workshop on Software Engineering and Challenges of Cloud Computing, 44-52.

[22] Verizon. 2014. Data Breach Investigations Report.

[23] Choo, K.K. 2014. A cloud security risk-management strategy. IEEE Cloud Computing, 1(2):52-6.

[24] Choo, K.K. 2014. Legal issues in the cloud. IEEE Cloud Computing, 1(1):94-6.

[25] Horvath, A.S., & Agrawal, R. 2015. Trust in cloud computing. In Southeast Con 2015, 1-8.

[26] Rathi, A., & Parmar, N. 2015. Secure Cloud Data Computing with Third Party Auditor Control. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), 145-152).

[27] Kobsa, A., Knijnenburg, B.P., & Livshits, B. 2014. Let's do it at my place instead?: Attitudinal and behavioral study of privacy in client-side personalization. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, (81-90).

[28] Otsuka, H., Watanabe, Y., & Matsumoto, Y. 2015. Learning from Before and After Recovery to Detect Latent Misconfiguration. In 39th annual IEEE Computer Software and Applications Conference (COMPSAC), 3:141-148.

[29] Gupta, S., Kumar, P., & Abraham, A. A Resource Efficient Integrity Monitoring and Response Approach for Cloud Computing Environment, In Pattern Analysis,Intelligent Security and the Internet of Things, 335-349.

[30] Sanaei, Z., Abolfazli, S., Gani, A., & Buyya, R. 2014. Heterogeneity in mobile cloud computing: taxonomy and open challenges. IEEE Communications Surveys & tutorials, 16(1):369-92.

[31] Khan, A.R., Othman, M., Madani, S.A., & Khan, S.U. 2014. A survey of mobile cloud computing application models. IEEE Communications Surveys & Tutorials, 6(1):393-413.

[32] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., & Brandic, I. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation computer systems, 25(6):599-616.

[33] Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. 2010. Security and privacy in cloud computing: A survey. In IEEE 6th International conference on Semantics Knowledge and Grid, 105-112.

[34] Yang, K., & Jia, X. 2012. Data storage auditing service in cloud computing: challenges, methods and opportunities, World Wide Web, 15(4):409-28.

[35] Kallahalla, M., Riedel, E., Swaminathan, R., Wang, Q., & Fu, K. Plutus: Scalable Secure File Sharing on Untrusted Storage. InFast 2003, 3: 29-42.

[36] Grobauer, B., Walloschek, T., & Stöcker, E. 2011. Understanding cloud computingvulnerabilities. IEEE Security & privacy, 9(2):50-7.

[37] Chang, V., Kuo, Y. H., & Ramachandran, M. 2016. Cloud computing adoptionframework: A security framework for business clouds, Future Generation Computer Systems, 57:24-41.

[38] Han, E.E. 2015. Detection of Web Application Attacks with Request Length Module and Regex Pattern Analysis. In Proceedings of International conference on Genetic and Evolutionary Computing, 157-165.

[39] Li, H., Wang, S., Tian, X., Wei, W., & Sun, C. 2015. A Survey of Extended Role- Based Access Control in Cloud Computing. In Proceedings of the 4th International Conference on Computer Engineering and Networks, 821-831).

[40] Shyam, G.K., & Manvi, S.S. 2015. Resource allocation in cloud computing using agents. In IEEE Interantional conference on Advance Computing (IACC), 458-463).

[41] Sowmiya, M., & Adimoolam, M. 2014. Secure cloud storage model with hidden policy attribute based access control. In IEEE International conference on Recent Trends in Information Technology (ICRTIT), (1-6).

[42] Kolhar, M., Abualhaj, M.M., & Rizwan, F. 2016. QoS Design Consideration for Enterprise and Provider's Network at Ingress and Egress Router for VoIP protocols,International Journal of Electrical and Computer Engineering (IJECE), 6(1):21-26.

[43] Li, H., Wang, S., Tian, X., Wei, W., & Sun, C. A Survey of Extended Role-Based Access Control in Cloud Computing. In Proceedings of the 4th International Conference on Computer Engineering and Networks, 821-831.

[44] Kamoun, M., Labidi, W., & Sarkiss, M. 2015. Joint resource allocation and offloading strategies in cloud Communications(ICC), 5529-5534.

[45] Park, J.S., Sandhu, R. Secure cookies on the Web. IEEE internet computing. 2000 Jul 1(4):36-44.

[46] Bellare M, Canetti, R., & Krawczyk, H. 1996. Keying hash functions for message authentication. In Advances in Cryptology—CRYPTO'96, 1-15).

[47] Lu, Q., Xu, X., Bass, L., Zhu, L., & Zhang, W. 2015. A Tail-Tolerant Cloud API Wrapper. IEEE Software, 32(1):76-82.

[48] Yuan, D., Park, S., Huang, P., Liu, Y., Lee, M.M., Tang, X., Zhou, Y., & Savage, S.2012. Be Conservative: Enhancing Failure Diagnosis with Proactive Logging. In OSDI, 12: 293-306.

[49] Tan, V., Groth, P., Miles, S., Jiang, S., Munroe, S., a SOA-based provenance system. In Provenance and Annotation of Data, 203-211).

[50] Xing, X., Liu, B., & Ling, D. Neural Network PID Control based Scheduling.Mechanism for Cloud Computing, Appl. Math, 9(2):789-96.

[51] Ahuja, M.S., Kaur, R., & Kumar, D. 2015. Trend Towards the Use of Complex Networks in Cloud Computing Environment. International Journal of Hybrid Information Technology, 8(3): 31-40.

[52] Sandhu, R., Sood, S.K. 2015. Scheduling of big data applications on distributed cloud based on QoS parameters, Cluster Computing, 18(2):817-28.

[53] Ranjan, R., Benatallah, B., Dustdar, S., & Papazoglou, M.P. 2015. Cloud Resource Orchestration Programming: Overview, Issues, and Directions, IEEEJournal of Internet Computing, 19(5):46-56.

[54] Shyam, G.K., & Manvi, S.S. 2015. Resource allocation in cloud computing using agents. In IEEE International conference on Advance Computing (IACC), 458-463.

[55] Zargar, S.T., Joshi, J., & Tipper, D. 2013. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, IEEE Communications Surveys Tutorials, 2046-69.