Perlustration on Recent Research into Multi Clouds integrated with Multi Party Computation

Parsi Kalpana

Abstract: Recent advances in multi cloud technologies and multi-party computations have improved State of art usage of Cloud computing in real time scenarios. Primary reason behind using any service offered by others is ease of use with lesser economics. Cloud Computing is technological advancement which is in usage for last two decades because of its Pay-per-Usage policy offering enormous benefits across the user community. In spite of its enormous benefits, single factor which is stepping it back from its wider adoption throughout the digital society is its Security. Tremendous research work was done across industry and academia in association with cloud security. This paper focuses on brief history, real time deployment of cloud, usage, benefits, risks associated and Surveys various studies done by national and international organizations related to cloud security concerns and dwell upon the advantages of integrating multi clouds and multi-party computation techniques and emphasizes on recent research done across multi cloud environment and give a short note of future work to enhance security paradigm.

Index Terms: Cloud Computing, Multi Clouds, Multi Party Computation, Risks, Security.

I. INTRODUCTION

Cloud Computing, metaphor for internet is an emerged technology which gives the user flexibility of placing everything and/or anything online, it may be data, applications, software or hardware with ease of use and thus offering everything as a service. It has gained widespread use and is playing a vital role in both industry and academia. As with any technological advancements, benefits and problems comes hand in hand the same is applicable for cloud environments. Major factor which contributed to its much demand is "Pay-per-Usage" model. Concept of Cloud Computing actually dates back to 1960's when John McCarthy at MIT had a vision that Computation will become public utility someday. In its current context for the first time it was used in 1997 by Prof. Ramnath K. Chellappa. He defined cloud computing as a new computing paradigm where boundaries will be determined by economic rationale rather than technical perspective [1]. NIST definition of cloud computing was been discussed in [2]. Contemporary enhancements of cloud computing have been originated from the Web technology which was basically designed to outfit to web applications.

Basically, transformation of cloud computing can be branched into three stages: Idea Stage – It is an inception stage where utility and grid computing are evolved. It came into existence in 1960's and lasted till pre-internet phase. Pre-cloud Stage – In this, Internet was pioneer to provide Application as Service, emerged in 1999 and was in existence till 2006. Cloud Stage – More delectable real cloud emerged in 2007 and services got streamlined as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [3].

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Parsi Kalpana*, Assistant Professor at Sr Francis College for Women, Hyderabad.

II. REAL TIME DEPLOYMENT OF CLOUD COMPUTING

Without the actual awareness of this technology, people are using it in the form of services like Gmail, Google, Facebook, YouTube etc. [4] which are provided by Internet. Also, TurboTax, Instagram and much used Google Drive all are applications which are cloud-based only. Hotmail is the first of its kind application based on this technology that gave the users compliance of storing their textual data and images at servers which are far away from user's proximity. Later, Amazon was the main vendor which started providing storage space, business functionality and all necessary computing resources in the form of Cloud Computing Model. The year 2006 saw emerging of EC2 (Elastic Compute Cloud) which gave the power to users and companies to lease their resources and computers and to run their own services and applications [5]. Salesforce pondered the idea of delivering enterprise applications as cloud-based services since 1999.

III. ANALYSIS OF CLOUD USAGE, BENEFITS AND RISKS ASSOCIATED

In this 21st century, there is an exponential increase in usage of data as the entire human kind and society is emphasizing on digitalization in every sphere of life and it is becoming more hazardous to preserve the vital and important data not only for individuals but also for organizations to keep very crucial and critical information, systems, programs running 24 hours a day all days through on in-house computer server because of which there is a transition of placing data and applications on cloud basing on the policy of pay per usage which is very beneficial for individuals and organizations too. For approximately two decades Cloud computing has been around.

As per International Data Group's study [6], most of the businesses are using cloud technology already, approximately around 69% in one way or other, and some businesses mentioned that they are too planning to implement cloud-computing solutions (around 18%). Also, as per report by Dell, companies that invest in cloud, big data, security enjoy up to 53% rapid growth in terms of economics compared to their competitors.

Basically, most of the organizations are using the cloud technology to increase their customer base, to run their business efficiently, to better serve their customers and increase overall profits. According to the estimates, 90% of the businesses in the United Kingdom are using a minimum of one cloud service [7].Cloud offers huge and tremendous benefits in terms of Cost Savings**,** pay structure, Flexibility, Competitive Edge, 24 by 7 Availability of Resources, Easily Manageable, Mobility, Speed to market**,** Increased Collaboration, Quality Control, Sustainability and Storage Options thus enhancing the productivity and minimizing upfront costs. Thus, Cloud adoption is increasing at a rapid phase as organizations are looking to diminish cost incurred by Information technology, to escalate business critical operations and to upsurge swiftness. However, major challenge which is acting as a barrier for its wider adoption is security of data and systems. Nine out of ten organizations are very or moderately concerned about public cloud security.

General security concerns at a rate of 43%, leakage and loss of data at 41% and loss of control at 31% act as top hurdles for cloud adoption as per report by Cloud Security Spotlight 2018 [8], among the cloud security concerns, access by unauthorized users at 63% plays a major role. Thus, the most prominent and effective approach to bridge this security gap is the capability to set and compel consistent cloud security policies. Encryption of data at rest and during transit ascend the list of most competent security measures for cloud data protection. As per McAfee study [9], 97% of organizations use public, private, or a mix of both cloud services, 83% store sensitive data in the public cloud and 1 in 4 organizations has experienced data theft from the public cloud. As per CSA Cloud Adoptions Practices and Priorities in the Chinese Financial Sector: Survey Report [10], the major two worries are data security and confidentiality, policies and regulations issues. Third in the list was Compatibility and interoperability with current system. Most users expressed that some kind of measures or controls are to be used to address these security concerns. More than 68% users said that they use encryption techniques. Around 73% of organizations expressed that they are using at least 1 application or a part of their computing infrastructure is in the cloud as per IDG Cloud Computing study 2018 [11], and around 17% mentioned that they are planning to do so within a year. Multi clouds strategy was been already used by 42% of organizations approximately. Main advantages of using multi-cloud mechanism are simple and rapid disaster recovery and expanded cloud options.

As per survey conducted by Netwrix Cloud Security [12], the major issue is security and privacy of sensitive data for both small and medium sized businesses. Most of the users are concerned about unauthorized access to their private assets. Second threat which was pondering upon was account hijacking. Other related issues were denial of service, malware infiltrations, insecure API and inside misuse.

As per Oracle and KPMG Cloud Threat report 2018[13], 90% of organizations categorize half or more of their cloud resident data as sensitive, 66% of companies suffered significant interruption of business operations in past 24 months and 38% mentions that cloud security is major challenge. As per CSA Cloud security report 2018 [14], 91% organizations are concerned about cloud security. Major three challenges are dealing with data leakage and data loss, confidentiality breach and data privacy.

In this data-driven age, it is essential and compulsory that companies and/or organizations protect and secure their workloads in the cloud. The most competent security mechanisms are encryption of data as well as encryption of network, then it is (SIEM) Security Information and Event Management at 52%.Thus, many organizations are interested to deploy their sensitive and crucial data into cloud but setting back only because of security concerns. Data of above analyzed reports was been summarized in the Table 1.

Name of Survey Report	Year	Top Concerns	Effective Measures
Cloud Security Spotlight Report [8]	2018	1) 90% focused on Security concerns 2) General security concerns (45%) 2) Data loss & leakage risks (41%) 3) Loss of control (31%). 4) Top Cloud Security concern is Unauthorized Access (63%)	1) 65% suggested Encryption at rest 2) 57% suggested Encryption in motion 3) 60% says Continuous protection is needed.
McAFee study [9]	2018	1) 97% of organizations use cloud services. 2) 83% store sensitive data in public cloud. 3) 1 in 4 organizations has experienced data theft from the public cloud.	1) Enhance the quality of code and decrease vulnerabilities and exploits 2) Combining quality assurance, security and development within the environment of application or operational unit.

CSA Cloud Adoptions Practices and Priorities in the Chinese Financial Sector: Survey Report [10]	2016	1) Security and confidentiality of data 2) Policies and regulations issues.	69% focus on Transmission Encryption
IDG Cloud Computing study [11]	2018	1) 73% of organizations use cloud services 2) 42% are using multi clouds.	
Netwrix Cloud Security Survey 2015 [12]	2015	1) 60% respondents concerned about security and privacy of data	1) String internal security policies 2) More investments in additional security mechanisms
Oracle and KPMG Cloud Threat report 2018[13]	2018	1) 90% of organizations categorize half or more of their cloud resident data as sensitive 2) 66% of companies suffered significant interruption of business operations in past 24 months 3) 38% mentions that cloud security is major challenge.	1) Securing Database with Defense-in-Depth approach 2) Encryption of structured data 3) Security automation
CSA Cloud security report 2018 [14]	2018	1) 91% organizations are concerned about cloud security. 2) 67% data loss and leakage protection 3) 61% data privacy threats 4) 53% confidentiality breaches.	1) 64% suggested Data encryption 2) 54% suggested Network encryption

Table I. Analysis of studies done by different standard national and international organizations regarding cloud concerns

Hence forth, focusing on cloud security is hour of need and much research is going on across the world to deal with security issue as it is playing an important role in cloud adoption everywhere.

IV. PARADIGM SHIFT FROM SINGLE TO MULTI-CLOUDS AND USAGE OF MULTI PARTY COMPUTATION

As analyzed, the major problem with cloud computing archetype is shielded deployment of private and delicate data inherently. Thus, cloud users must be attentive of the actuality that all their private and intimate data leaves the own control and protection sphere once cloud services are used.

Henceforth, state of art cloud security mechanisms has their own constraints. There is no standard viable way to achieve any specific type of data dependent operations and methods without penetrating into confidentiality and integrity. Because of this nature of cloud, it is very much prerequisite and necessitous to have a strong fraternity amongst the cloud user and its service provider. Earlier scenario of having sole cloud provider for all services has become least accepted because of existence of issues like availability of service, malignant conspirator within the cloud. Current decade has enriched a major transition to regime of multi clouds rather than just emphasizing on single cloud. The seed idea behind multi clouds was first introduced by Vukolic [15]. Here, we emphasis on revolutionary shift to multi clouds from single cloud in order to safeguard and insure the armor of the user's important data. The contemporary exploration articulated on the multi-cloud habitat [16],[17],[18],[19] where several clouds were used to overwhelm the issues inherent in individual cloud form.Multi-party computation is a sub field of Cryptography where a finite number of users can compute some procedures or functions on their inputs without conceding any information on their individual data. Formally, Secure Multiparty Computation (SMC) problem is defined as a scenario where multiple users or parties having private inputs I_1, $I_{2,}$ I_3……, I_n want to figure out the value of the public function p = $f(I_1, I_{2,} I_3…, I_n)$ in a way where by no user or party will be aware of other's input or data except the common result. Yao introduced the SMC problem in [20]. Both empirically and analytically, it was demonstrated that Yao's protocol is secure [21]. First of its kind large scale implementation of multiparty computation succeeded practically in 2008 at Denmark [22].Thus, multi-party computation can be performed by using the concept of multi clouds which can be constructive for assuring the solitude of individual data or organization. In this scenario, multi-party computation will work as depicted: by using a secret sharing scheme such as Shamir's [23], user will compute shares of his/her data and distribute the shares to the multi clouds. By using these shares, the user can reconstruct the result, where by an intruder cannot plodder the data even he/she penetrate into one or more clouds, thus confidentiality of user's data can be warranted unless the cloud providers collude among themselves.

V. RELATED WORK ON MULTI CLOUD ENVIRONMENT

Meiko Jensen et al [24] discussed about achieving security by using multiple clouds at the same time. They mentioned that usage of multi clouds is already existing but focus was on load balancing and not on security. Also, as per their knowledge, their work is first attempt to acquaint with convention of multiple clouds to fabricate security. They proposed three distinct architectural patterns namely replication of application, partition of application system into tiers and partition of application tiers into fragments in which they focused on the usage of multi-party computation and discussed that security can be provided by using these architectural patterns.

Nikhar Maheshwari et al [25] proposed SMCC architecture by using SMC protocols. In the proposed architecture, they emphasized on trusted third party which is generated randomly where cloud was introduced and the computations are done on the cloud. Also, they used anonymizer layer whose task is to delegate the data received from parties to cloud, which is purely inactive with zero intelligence and it allows only one-way communication. Authors mentioned that by using trusted third party and anonymizer layer, security can be guaranteed in Cloud environment.Mohammed A. AlZain et al [26] briefs Contempo research related to single and multi-cloud security and focused on issued related to data security. Authors discussed about usage of HAIL, RACS, DepSky Systems to deal with issues like Data integrity, Availability, Confidentiality and Vendor Lock-in.Jens Matthias Bohli et al [27] provide survey on achieving security merits by using multiple distinct clouds simultaneously. They emphasized by using different case studies how usage of multiple distinct clouds is beneficial. As per their observations, major improvements suggested are: a single technical approach should be designed to deal with each type of security problem by combining the approaches presented i.e, using n clouds with sound data encryption may be designed. Samiksha Shukla et al [28] focused on using SMC Protocol based on ideal dishonest majority to deal with Data confidentiality, privacy and security.Kiran Baby et al [29] surveyed on usage of multi cloud architecture to assure better security and performance. They focused on usage of cryptographic data splitting combined with homomorphic encryption to ensure security.Abdul Razaque et al [30] aims at providing data security by incorporating multi clouds. They focused on data sharing across multiple clouds and reconstructing it and mentioned that even though fusion of data sharing and multi-clouds is promising it has uncertainties and difficulties in practical implementation.Because of enormous benefits associated with multi clouds and multi-party computations, surveyed the recent work associated with multi clouds integrated with Shamir secret sharing which is one of the very important algorithms under the multi-party computational mechanisms and analysis was depicted in below Table II.

Reference	Problems identified & overcomed	Architecture proposed	Approach used	Platform & Dataset used	Experiment/Evaluation	Analysis & Limitations (if any)	Future Work
[31]	Data Privacy in DAAS	NetDB2-MS	Multi-service providers & Secret sharing algorithm	Simulated using Java and used Numeric data	Comparative evaluation of Blowfish encryption and Secret sharing approach (Data storing & Retrieval)	Complexity increased but with increased level of Security	Considering non-numeric data and larger data size

[32]	Service availability, Data intrusion, Data integrity.	MCDB model	Multi cloud service providers & Shamir secret sharing	Simulated using Java and used Numeric data	Compared with Amazon cloud service and Evaluation of queries like exact matching, range and aggregate queries.	Complexity increased but with increased level of Security	To compare with other existing cloud service provider's models.
[33]	Confidentiality Availability & Integrity of data	Comparative study	Comparison of Shamir's secret sharing and Rabin's IDA	Private cloud setup using Open Stack cloud framework & used Employees sample database which consists of 6 tables and total of 4 million records.	Comparative study of Shamir's secret sharing & Rabin's IDA.	Secret sharing methods are computationally inexpensive when compared with traditional encryption techniques. Also, no need to focus on secure storage of encryption keys.	-
[34]	Privacy and Security of data	Multi clouds database model	Multi cloud service providers & Secret sharing approach	-	Divided the data into multiple parts and stored on different service providers using shamir's secret sharing approach	Usage of multi sharing techniques is considered novel	-
[35]	Data integrity & Confidentiality	MCDB model to protect Multimedia	Google drive, OwnCloud and Dropbox are used as Multi cloud databases & Shamir secret sharing	Simulated using PHP	Designed and implemented prototype system of UMIT Momento application	Improved data availability, confidentiality and integrity.	-
[36]	Security and availability of user data	Secure storage & Sharing scheme in multicloud environment	Proxy reencyrption and Shamir's secret sharing approach	Simulated in Java & used 100 sets of data each with 1MB size and different content.	Analysis in terms of Security and Time cost.	Scheme proved to be highly secure	Increase the interaction and connection with existing commercial clouds to make it more practical

Table II. Analysis of Multi Clouds integrated with Shamir Secret Sharing Approach

VI. CONCLUSION/ FUTURE WORK

Deploying multi cloud environment and integrating it with multi-party computation mechanism was very much beneficial in reducing the risk of data intrusion, service availability and to ensure data integrity and overcoming vendor lock-in issues. But these advantages evidently route with assured expenditure. Also, adoption of multiple clouds proportionally increases the amount incurred. Yet, if one of the current approaches are deployed skillfully, overall amount might still be less than amount incurred by running the service in-house. As in [27], strong encryption technique combined with secret sharing approach on multi clouds will be a viable solution to enhance the security in cloud environment. Future work is to analyze different data encryption mechanisms and to come up with an integrated approach which is fusion of multi-party computation and strong encryption mechanism to strengthen the much-deliberated security concern and to provide a feasible solution for supervision of data security in cloud environments.

REFERENCES

1. https://cloudtweaks.com/2011/02/a-history-of-cloud-computing/
2. P. Mell and T. Grance, “The NIST Definition of Cloud Computing”, Computer Society, Sep 2011.
3. https://www.engineersgarage.com/articles/what-is-cloud-computing-article
4. Zaigham Mahmood, “Data Location and Security Issues in Cloud Computing”, International Conference on Emerging Intelligent Data and Web Technologies”, IEEE, 2011.
5. "Announcing Amazon Elastic Compute Cloud (Amazon EC2) – beta". 24 August 2006. Retrieved 31 May 2014.
6. https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/
7. https://www.idexcel.com/blog/top-10-advantages-of-cloud-computing/
8. https://media.scmagazine.com/documents/114/cloud-security-spotlight-repor_28381.pdf
9. https://www.businesswire.com/news/home/20180415005135/en/McAfee-Study-Reveals-1-in-4-Organizations-Public-Cloud
10. https://downloads.cloudsecurityalliance.org/assets/survey/FSI_China_Report_25Oct.pdf
11. https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/
12. https://www.netwrix.com/download/documents/netwrix_report_cloud_security_2015.pdf
13. https://assets.kpmg/content/dam/kpmg/kz/pdf/Oracle-and-KPMG-Cloud-Threat-Report_2018_Limited.pdf
14. https://pages.cloudpassage.com/rs/857-FXQ-213/images/2018-Cloud-Security-Report%20%281%29.pdf

15. M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp. 105-111.
16.H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10: Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.
17.A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11: Proc. 6thConf. On Computer systems, 2011, pp. 31-46.
18.K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp. 187-198.
19.C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.
20.A.C. Yao, “Protocols for secure computations,” Proc. 23rd IEEE Symposium on the Foundation of Computer Science (FOCS), IEEE 1982, pp. 160-164.
21.I. Ioannidis and A. Grama , “An efficient protocol for Yao’s Millionaires Problem,” Proc. 36th Hawaii International Conference n System Sciences,HICSS’03, 6-9 Jan 2003, IEEE Press, pp. 6-11.
22.https://www.researchgate.net/publication/220796917_Secure_Multiparty_Computation_Goes_Live
23.A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, pp. 612–613, 1979.
24.Meiko Jensen, J¨org Schwenk, Jens-Matthias Bohli, Nils Gruschka, Luigi Lo Iacono, “Security Prospects through Cloud Computing by Adopting Multiple Clouds”, IEEE 4th International Conference on Cloud Computing, 2011.
25.Nikhar Maheshwari, Krati Kiyawat, “Structural Framing of Protocol for Secure Multiparty Cloud Computation”, 2011 Fifth Asia Modelling Symposium, 2011.
26.Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, “Cloud Computing Security: From Single to Multi-Clouds”, 45th Hawaii International Conference on System Sciences, 2012.
27.Jens Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo lacono, Ninja Marnau, “Security and Privacy-Enhancing Multicloud Architectures”, IEEE Transactions on Dependable and Secure Computing”, Vol 10, No 4, July/Aug 2013.
28.Samiksha Shukla, Dr.G.Sadashivappa, “Secure Multi-Party Computation Protocol Using Asymmetric Encryption”, 2014 International Conference on Computing for Sustainable Global Development (INDIACom).
29.Kiran Baby, Anupriya Vysala, “Multicloud Architecture for Augmenting Security in Clouds”, IEEE Proceedings of 2015 Global Conference on Communication Technologies (GCCT 2015).
30.Abdul Razaque, Saty Siva Varma Nadimpalli,Suharsha Vommina, Dinesh Kumar Atukuri,Dammannagari Nayani Reddy, Poojitha Anne, Divya Vegi, Vamsee Sai Malllapu, “Secure Data Sharing in Multi-Clouds”, IEEE International Conference on Electrical, Electronics and Optimization Techniques (ICEEOT) 2016.
31.Mohammed A. AlZain, Eric Pardede, ” Using Multi Shares for Ensuring Privacy in Database-as-a-Service”, Proceedings of the 44th Hawaii International Conference on System Sciences, 2011.
32.Mohammed A. AlZain, Ben Soh, Eric Pardede, “MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing”, Ninth IEEE International Conference on Dependable, Autonomic and Secure, 2011.
33.S.Jaya Nirmala, S.Mary Saira Bhanu, Ahtesham Akhtar Patel, “A Comparative Study of the Secret Sharing Algorithms for Secure data in the Cloud”, International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.4, August 2012.
34.Ion Morozan, “Multi-Clouds Database: A New Model to Provide Security in Cloud Computing”, 2014. https://www.researchgate.net/publication/273136522_Multi_Clouds_Database_A_New_Model_to_Provide_Security_in_Cloud_Computing.
35.Sumedh N. Pundkar, Dr. Narendra Shekokar, ” Cloud Computing Security in Multi-clouds using Shamir’s Secret Sharing Scheme, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016.
36.Kaiying Feng, Junxing Zhang, “Improving Availability and Confidentiality of Shared Data under the Multi-cloud Environment”, 2nd IEEE International Conference on Cloud Computing and Big Data Analysis, 2017.

Authors Profile

Parsi Kalpana is currently working as Assistant Professor at Sr Francis College for Women, Hyderabad. She is pursuing PhD in Computer Science Engineering from Osmania University and holds 2 Masters Degrees, M. Tech in Computer Science & Engineering from JNTUH and Master of Computer Applications from OU. She possesses more than 16 years of teaching experience and has published 10 papers in various International Journals and Conferences. Her area of interest is Cloud Computing and its security mechanisms.