Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July 2021: 5219-5228

An Investigation of Cloud Computing Security issue using Prototype Model

Anita Rani[1], Mr. Parveen Rathi [2], Dr. Pawan Kumar [3], Dr. Deepak Goyal [4], Dr. Pankaj Gupta[5]

[1]M.Tech Scholar, Department of Electronics and Communication Engineering, Vaish College of Engineering, Rohtak, anitaluthrapawar@gmail.com

[2]Assistant Professor, Department of Electronics and Communication Engineering, Vaish College of Engineering, Rohtak, parveenrathivce@gmail.com

[3]Assistant Professor, Department of Electronics and Communication Engineering, Vaish College of Engineering, Rohtak, pawankr8732@gmail.com

[4]Professor, Department of Computer Science Engineering, Vaish College of Engineering, Rohtak, deepakgoyal.vce@gmail.com

[5]Professor, Department of Computer Science Engineering, Vaish College of Engineering, Rohtak,

pankajgupta.vce@gmail.com

Abstract

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. There are many problems related with cloud computing traffic, security and resource management. We can provide security in cloud by many ways like on data, network and storage. I propose homomorphic encryption to provide security on cloud. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data. This method provides more security on data because provider is not involving in key management. I use proxy re-encryption technique that prevents ciphertext from chosen cipher text attack. This system is more secure than existing system.

Keywords: *Cloud Computing, Security, Encryption, Decryption, Cipher Text*

1. Introduction

Cloud Computing is an organization-based technology that utilizes the web and distant workers which centers around sharing calculations or assets for keeping up with data and applications. Cloud Computing functions as "Pay-as-you-go‖ model is most engaging element. The cancellation and generating of virtual machines running on actual equipment and being constrained by hypervisors is an expense proficient and adaptable computing worldview. What's more, the reconciliation and far and wide accessibility of a lot of sanitized information in various areas, for example, wellbeing area can be of enormous advantage to scientists and experts. Cloud Computing is very wealthy in highlights yet fundamental fates of Cloud Computing are as per the following:

- Use of internet-based services to support business process
- Rent IT-services on a utility-like basis
- Cloud Vendors

The Cloud Computing Technology chips away at three diverse SPI (Software Platform Infrastructure) models

- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- SaaS (Software as a Service)

Besides this there are four organization (public, private, half breed, and local area) models. According to the use or prerequisite shopper can utilize the service(s) of the cloud and convey the cloud.

- Public Cloud
- On-site Private Cloud/Outsourced Private Cloud
- Hybrid Cloud
- On-site Community Cloud/ Outsourced Community Cloud

2. Problem Statement and Objective

2.1 Problem Satement

The term Cloud Computing which portrays the transformative advancement of many existing innovations and ways to deal with computing at its generally essential, isolates information and application assets from the central foundation and component used to convey them with the expansion of designation of assets with utility model and versatility. Cloud Computing intensify coordinated effort, scale, accessibility, nimbleness and gives the possibility to cost decrease for the shoppers and organizations. At the end of the day, Cloud Computing portrays the utilization of an assortment of uses, information and foundation, network, information and capacity assets and finally appropriated administrations. These parts can be immediately coordinated, prepared, carried out and destroyed utilizing a utility model for designation and de-portion and utilization.

2.2 Objectives of The Study

There are various objectives for our research which are listed below:

- To examination cloud network assaults and propose counteraction/relief techniques against oneof them.
- The cloud network security draws out the scientific classification of various kinds of cloud assaults that have happened in ongoing past and their related dangers. Under Cloud network security, we would break down classifications of the assaults, which are more conspicuous on cloud networks.
- To investigate Data Security assaults in the Cloud network, propose anticipation/moderation

techniques

- To explore reason(s) for hesitance in selection of Cloud Computing by buyers regarding security and danger.
- For upgrading the selection of cloud technology, it is obligatory to know the reasons for hesitance to appropriation of cloud technology in India at various levels (little, center, and huge size) of ventures.

3. Methodology

Strategy comprises of the entire periods of a specific report that stay critical towards specific exploration directed proficiently. This investigation utilizes spellbinding, factual techniques while breaking down the data gathered. This part contains various undertakings which study generally speaking issues, theories, how the speculations are deciphered, data assortment just as techniques concerning planning and completing fundamental explores that guide researcher on what, why and how to gather and assess data, just as systems for drafting results towards driving end in research.

3.1 Research Methods

The strategy for research utilized in this investigation contains subjective method that include the utilization of electronic mail polls (email), distributed survey over subsequent meet-ups, mobile phone, skype, WhatsApp and one on one meeting communications. Associations and client were chosen dependent on their particular involvement in cloud computing, security and protection angle in cloud, cloud administration, organization just as innovations to follow the fundamental point of the exploration concentrate in discovering an answer for the security issues related to cloud computing. For the initial segment of the overview surveys were sent to cloud clients. The polls were thoroughly examined to empower respondents to concur whether to be conveyed, at whatever point needed for whichever extra information. PDA/skype/WhatsApp and one on one meeting cooperation's directed with many cloud clients too. The meeting connections are semi-organized towards permitting the interviewee respondents free communication of their perspectives.

Watchfulness is continued in data examination, while suitable semi-organized meetings and questions are intended to discover extra theoretical issues and to help with getting free missteps, question in various responses to review questions and meeting. Respondents are given affirmation by the scientist on classification of all that they contributed in the exploration study.

3.2 Research Approach

As expressed before, an examination study to be led in an exploration field of information technology and computing might be best done utilizing subjective methodology. Due to the idea of the investigation that reports the recent concerns were specialist's perception, basic investigation of applicable examination, exact meeting and utilization of records are expected to answer parcel of the exploration study questions. These make it simpler for the investigation to receive deductive/inductive and subjective/quantitative approaches likewise. Subsequently, the researcher utilizes a portion of the strategies expressed, to totally accomplish study goals by giving proper proposals to end and various techniques for handling cloud security issue and dangers issues.

3.3 Research Design

Exploration configuration considered being approaches, systems just as strategies utilized while directing a specific report, distinct ideas are created, inspect in an unmistakable methodology. Illustrative methodology which is now and again examines as explorative examination are utilized in this investigation for investigating beneficial thoughts and purposeful entirely on the need to sort various techniques; cloud computing security issues will be radically diminished and annihilated to foster associations execution with suggestions of expected various methodologies and model improvement toward the finish of exploration study discoveries.

3.4 Research Process

Despite the fact that, there exist disparate systems in leading exploration, every one of the strategies include in a progression of achievements that produce research measures with incredible dependence coordinated. The occasions in research technique don't continually screen a similar guidance.Thusly, the examination followed certain systems to successfully give a commendable report. The interaction in research contains: portraying the issue as depicted in presentation part, improvement the exploration plan and inspecting through assessment, gathering and amassing the vital data for the investigation (overviews and meetings), dealing with and looking at the data gathered from both essential, optional wellsprings of data assortment methodology, then, at that point at long last articulating surmisings and revelation fundamentally to closing the examination. By and by, the suppositions of study conventionally produce imaginative ideas for planned examination. Hence, making the whole cycles in research rehashed normally, the beneath figure elaborate more on this.

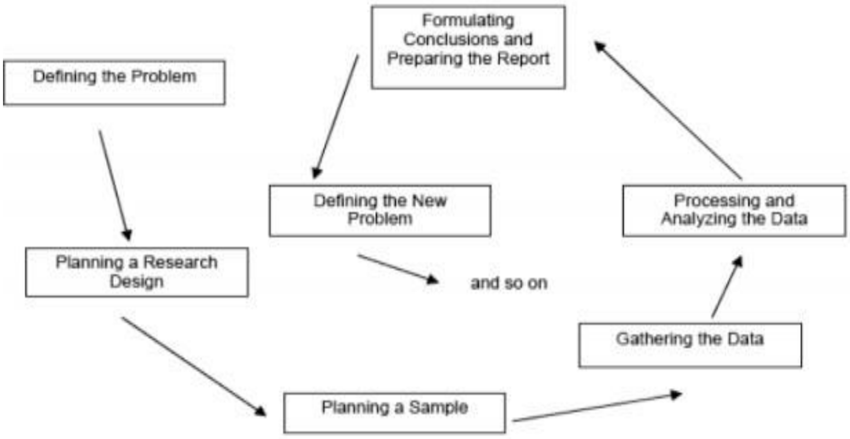

Formulating Conclusions and Preparing the Report
Defining the Problem
Defining the New Problem
Processing and Analyzing the Data
Planning a Research Design
and so on
Gathering the Data
Planning a Sample

Fig.1: Research Process. [**Source:** Adopted in Ahmad Sobhani, 2008]

4. Classification and Method of Data Collection

A decent report is pondered to be unique, reliable, critical, practical and very much expressed with adequate data. The data must be made by implies out of bases which are commonly ordered via essential/optional secretly [39] this examination utilizes both data however accentuation are fundamentally on the data accumulated basically. Since, this help researcher in accomplishing powerful, reliable and proper choices which can be utilized in working on the revelations of the examination concerning security issues in SPI administration models, sending models, the advances and cloud computing as a rule.

4.1 Primary Data

The strategy received by the researcher to accumulate data is review techniques. Questions are planned and disseminated to numerous respondents chose from various clients and master of cloud technology. Around 200 surveys were appropriated however 178 reactions were gotten. Lamentably, some were return as invalid, not filled effectively and some filled in blunder.

Thusly, 100 Questionnaires that are filled accurately where haphazardly picked, utilized in the exploration cycles to determine and to discover answer for the examination questions and achieved research objective.

4.2 Secondary Data

The secondary kinds of data embraced in this examination were unequivocally the library assets like: diaries, web, course readings, magazines, meetings and understudy papers were gone to acquire knowledge as a matter-of-fact researcher in cloud computing and security angle. Thus, the material had contributed hugely in enlarging plausibility in the examination study and the researcher's ability in thinking about completely the exploration study region. The papers, distributed diaries, course and meeting papers are cautiously examining where overwhelming and huge articles on information framework technology, information security extricated. Papers of different region utilized, including of measurable data, were altogether concentrated to gather the applicable data needed for the investigation.

4.3 Prototype Model

A section from the procedure and techniques portrays over, a Prototype Model will likewise be utilized after the examination of the discoveries as an exploration plan to foster a security model that will help in lessening the degree of security hazards related with cloud computing. In the model a solitary emphasis of the prototyping model will be utilized in exhibiting practical capacities of created framework/model. The model considers alteration and correction of a framework lastly unloading the entire framework and fostering a fresher one that fits the exploration study discoveries. This will likewise be addressed utilizing an UML Use Case Diagram to show the capacities in the model. Agreeing prototyping model includes of four phase measures model. These model stages incorporate the accompanying: making destinations of model, portray model functionalities, creating and assessing model which is considered as fundamental critical cycles.

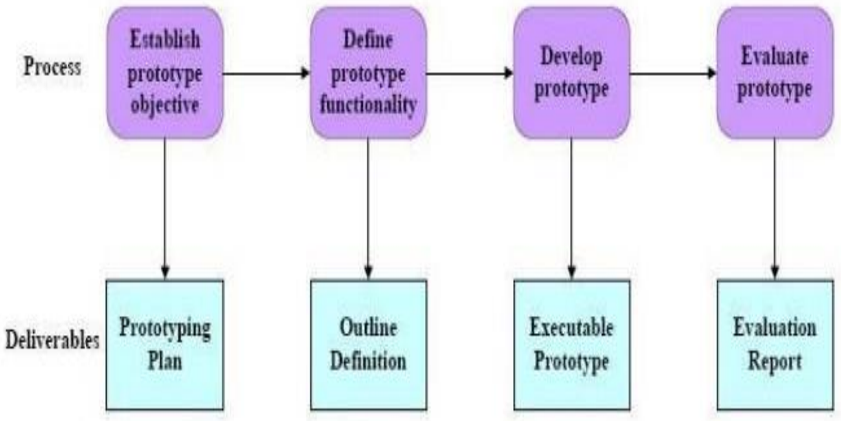


Fig.2 : Stages in Prototype Model. Adapted from [41] Sommerville (2007).

The model executes an expendable model strategy. This is as the assurance of the model is to build up and test the very much planned capacities to represent the dangerous region distinguished. Besides, model was utilized to examine the forces and deficiency of the all-around planned capacities of the model created.

4.4 Prototype Development

An investigation by acknowledged three systems that can be utilized for UI in prototyping; visual programming language, web-based prototyping and content driven prototyping. The content driven prototyping was carried out in making visual rudiments for clients to interrelate with framework towards playing out its tasks or functionalities. Thusly the apparatuses and language to be use in creating model in the examination are:

- Wordpress
- Adobe Fireworks
- CSS
- Ajax
- PHP
- MySQL

UML: Use Case, Sequence and Class Diagrams

Bound together Modeling Language curtailed as UML it is the capacity for showing use case charts Use case outlines are generally utilized all through the investigation phase of a specific examination concentrate to arrange framework functionalities. Accordingly, the specialist utilizes the utilization case in isolating the framework intrigued by entertainers and use case. The entertainers imply characters played by clients of a framework. In addition, the utilization case chart is the straightforward procedure to address client's relationship with the framework that shows the relationship between the client and the diverse use cases in which the client is included.

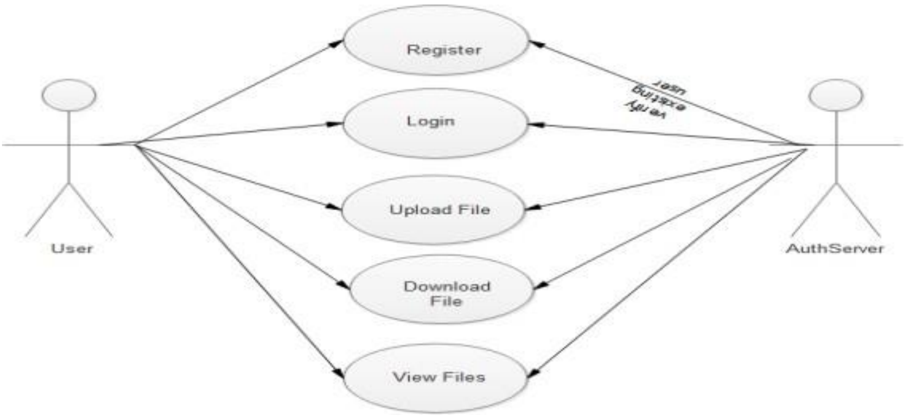


Fig.3 Use Case Diagram for Prototype [Source: Adopted in survey 2018]

5. Data Analysis Outcome

The overview led with the guide of survey instrument been dispersed for revelations to a few respondents with knowledge of cloud computing, data are formed to permit the researcher concoct sensible examination and answers to the investigation questions. The issues are commonly concerning the protection and security issues with respect to selection, administrations, arrangement and innovations of cloud computing. The examination of the investigation results had been dissected through a basic illustrative investigation using various questions.

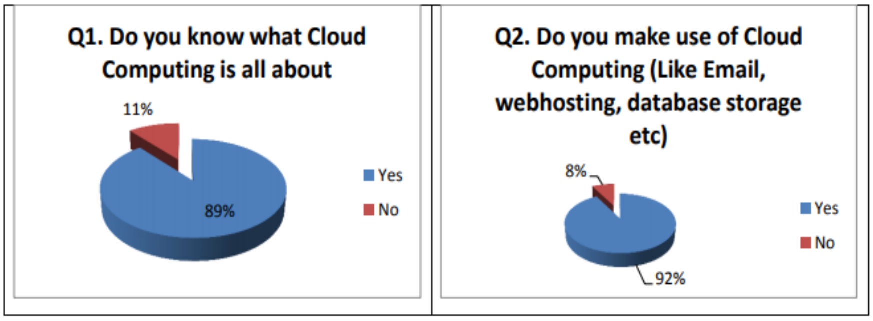


Fig.4 Usefulness of Cloud Computing

Question 4 of the overview survey discussed various sorts of cloud computing in which clients can have one of admittance to cloud computing technology through any of the models.

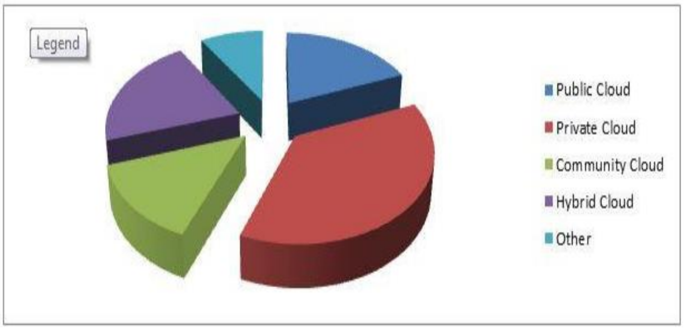


Fig.5 Cloud Deployment Models (Q4)

Result in the underneath figure showed that 43% concurred Cloud Computing further develop execution in business, unequivocally concurred had 21% as those with the assertion as per result, Neutral had 31%, emphatically differ had 2%, though differ had 3%.

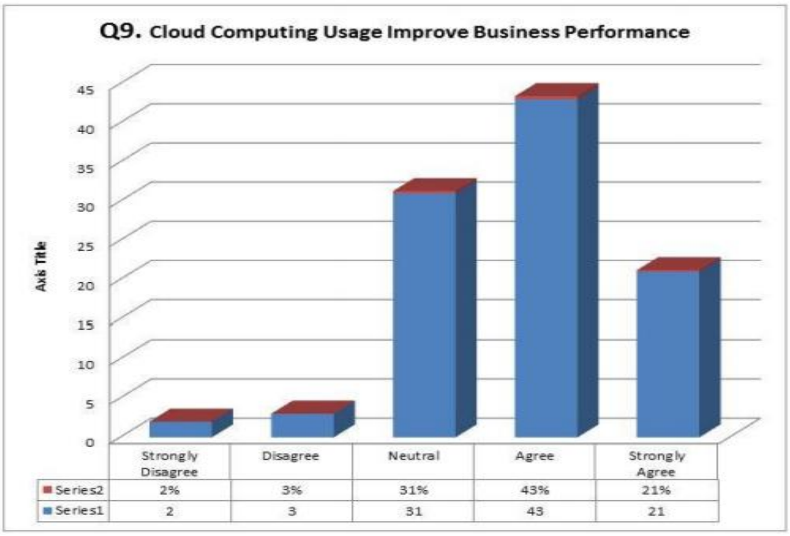


Fig.6 Cloud Computing Usage Improves Business Performance

The Issue of Adherence to Data Security Control: On the Issue of Adherence to Data Security Control as concurred in Services Level Agreements (SLA) the reactions from respondents is that 16% said Yes, 49% said No and 35% of the respondent addressed Maybe, that is to say they don't know on whether the Cloud Service Provider comply to such understanding rigorously or not.

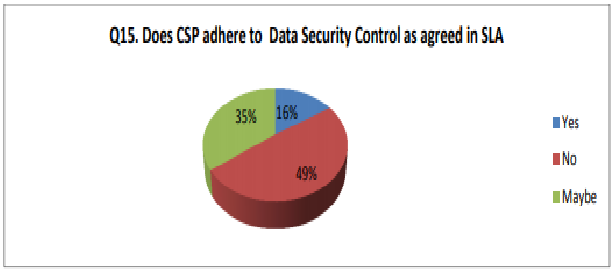


Fig.7 CSP adherence to Data Security Control as agreed in SLA

Cloud Service Providers (CSP) Perspective and Users Perspective: On the security worries with respect to relationship from Cloud Service Providers (CSP) Perspective and Users Perspective, both the suppliers and clients are having related worries as far as Data and Information Storage. Most particular the protection and security issues, so reactions are introduced after investigation of the Question from the Survey structure which shows 62% of the reacted consider there is solid direct relationship from the two players and 38% are of the assessment of in a roundabout way related as displayed in the figure beneath

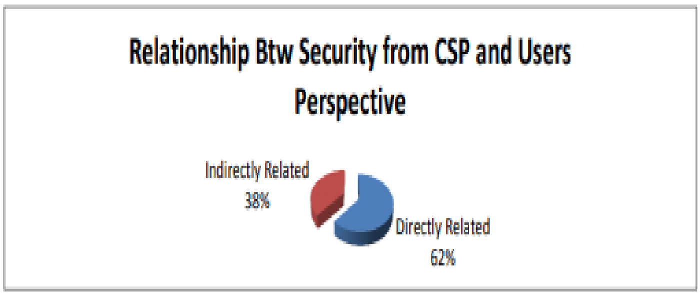
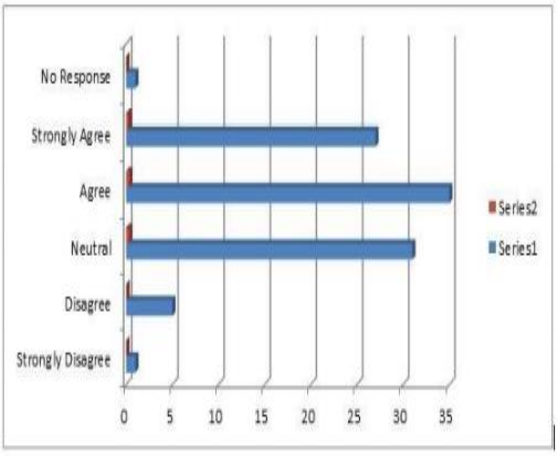
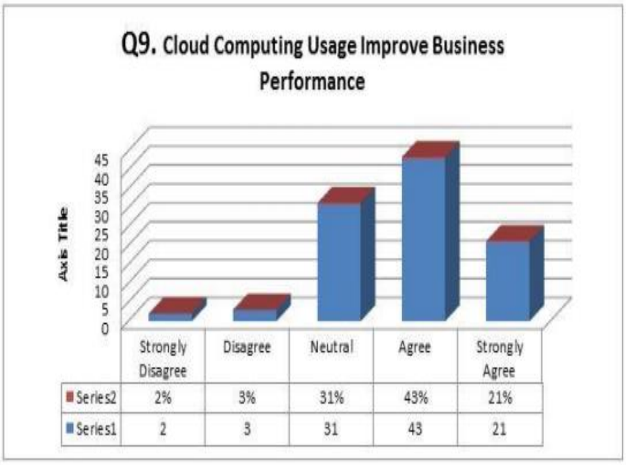


Fig.8 Relationship between security from CSP and User Perspective

Statistical Result of the Hypothesis and Correlation Analysis: Question 7, 9 and 10 were used in describing the hypotheses 1, 2 and 3 respectively.





	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Series2	2%	3%	31%	43%	21%
Series1	2	3	31	43	21

Fig.9 Question 7 for Hypothesis 1

Fig.10 Question 9 for Hypothesis 2

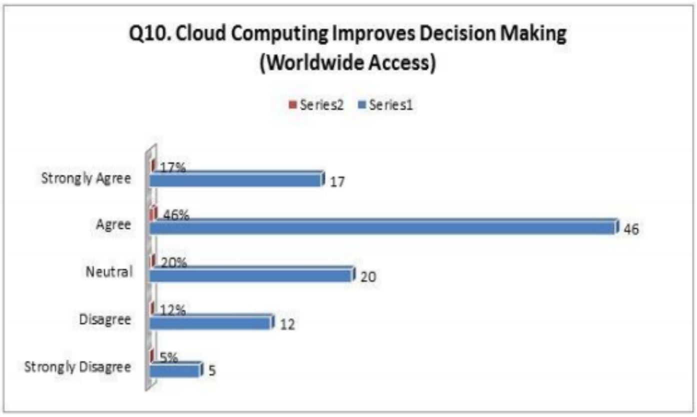


Fig.11 Question 10 for Hypothesis 3

6. Conclusions and Future Scope

Cloud computing gives various benefits to client yet at the same time because of security issues numerous clients wonder whether or not to embrace it too the specialist co-op may have an issue about un approved admittance. Along these lines, to settle issue identified with both client and specialist co-op, we fostered another structure by proposing mix of encryption and jumbling strategy together. Prior to sending data on Cloud encryption, it gives security to the data which is on change in the network by which client guarantees the privacy of his data. We have proposed a safe stockpiling cut off which monitor client keys too hash of the archive transferred on the worker. For the Cloud suppliers, productive obscurity strategy is proposed by which the privileged data of Client like secret key, contact subtleties and so forth are not tempered by outsider. The means for calculation are likewise sorted out which guarantee the productive working of activities. We have additionally given itemized examination about the result created by the carried-out model by considering vital boundaries like time and security. From the examination between the model with and without confusion we should say that even the obscurity may build modest quantity of time however for the Cloud supplier this time become unimportant thinking about the security of client's data. Rather than utilizing encryption measure on worker which is proposed in some model, we should say jumbling diminishes the weight of worker concerning execution cost and thusly client can improve administrations from Providers. By utilizing Group strategy, we can say that the weight of Cloud suppliers towards dealing with singular inquiries is decreased.

Future Work: The previous area has uncovered the ends drawn from the exploration completed. From the knowledge acquired in the examination, the specialist could recognize conceivable future extent of the exploration. Bearings for equivalent to follows.

- The planned lightweight encryption plot is assessed to learn its benefits with regards to voluminous data. Further investigation is required with Map Reduce programming worldview with enormous data.
- In the setting of Internet of Things (IoT) as one of the wellsprings of enormous data with asset obliged associated gadgets, it is fascinating to approve the proposed instruments in the IoT incorporated use cases like shrewd home, brilliant city and savvy transportation.

References

1. NIST National Institute of Standard and Technology, U.S Department of Commerce. Guidelines on Security and Privacy in Public Cloud Computing. Special Publication [Home Page on the Internet] 2011. [Cited on 15th December, 2016] Available from http://csrc.nist/specialpublication/nistpubs/800-144.pdf
2. Bharat Bhargava (2012), Security and Privacy Issues in Distributed System and Cloud Computing. Seminar Lecturer, Computer Science Department, Purdue University, West Lafayette, Indiana, USA. 2012, [Cited on 15th December, 2016] Available from www.cs.purdue.edu/homes/bb
3. Rabi P. P, Manas R P, Suresh Chandra S. Cloud Computing: Security Issues and Resaerch Challenges, 2011. Published in IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol.1, No.2, December 2011.
4. Usman Ahmad U., Shah Shoib F. and Mavera U. Security and Privacy issues in Cloud Computing and Providing Platform for E-learning, 2014 Published in International Jounal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 5
5. Shilpashree S., David Q. L., Athanasios V. et al. Security and Privacy in Cloud Computing: A Survey. Parallel & Cloud Computing, 2013. 2 (4), 126-149. New York, NY: American V-King Scientific Publishing, LTD. [Cited on 2nd January, 2017] Available from http://opus.ipfw.edu/compsci_facpubs/44
6. Sapna M., MM Chaturvedi. Privacy and Security in Mobile Cloud Computing: Review, 2013. Published by International Journal of Computer Applications (0975-8887) Volume 80-No11, October 2013.
7. Ms. Rupali R. K., Ms Rinkle C. P. Data Security and Privacy Protection Issues in Cloud Computing, 2015. Published in International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 2, pp:(1130-1134), Month: April-June 2015, [Cited on 23rd January 2017] Available from www.researchpublish.com
8. Shufen Z., Hongcan Y., Xuebin C. Research on Key Technologies of Cloud Computing. 2012 International Conference on Medical Physics and Biomedical Engineering. Physics Procedia 33 (2012) pp:1791 - 1797. [Cited on 1st February, 2017] Available from www.sciencedirect.com
9. Sean C., Kevin C. Cloud Computing Technologies, 2012. Published in International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No2, June 2012, pp. 59-65 ISSN: 2089-3337.
10. Shrinivas A. An Overview of Cloud Deployment Models and Security Issues in Cloud, 2016. Published in International Journal of Computer Application (2250- 1797) Volume Six (6), No. Four (4), July – August 2016. [Cited on 8th February, 2017]
11. Nikita G. and Toshi S. Cloud Computing – SPI Framework, Deployment Models and Challenges, 2014. Published by International Journal of Emerging Technology and Advanced Engineering, Volume 4, Special Issue 1, February 2014, International Conference on Advanced Development in Engineering and Technology (ICADET-14), India. [Cited on 28th February] Available from www.ijetae.com
12. Al-Muslim W. and Li C. User Privacy and Security issues in Cloud computing, 2016. Published by Internation Journal of Security and Applications Vol. 10, No 2, (2016) pp 341-352.
13. Awodele O. et al. Big Data and Cloud Computing Issues, 2016. Published in International Journal of Computer applications (0975-8887) volume 133 – No. 12, January 2016. [Cited on 3rd March, 2017]
14. Nancy J., and Sakshi C. Overview of Virtualization in Cloud Computing, 2016. Published by IEEE, in Colossal Data Analysis and Networking (CDAN), Symposium on 18-19 March 2016. [Cited 2nd May, 2017]
15. Chakradhara R., Mogasala L., and Ramesh K.Cloud: Computing Services and Deployment Models, 2013. Published in International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 2 Issue 12, Dec. 2013 Page No.3389-3392 [Cited 2nd May, 2017] Available online from www.ijecs.in
16. Shrinivas A. An Overview on Cloud Deployment Models and Security issues in Cloud, 2016. Published by International Journal of Computer Application (2250-1797) Volume 6 – No. 4 July – August 2016. [Cited 7th May, 2017]