Improving quality of an existing Cloud framework for Security issues in data security model

Chandrahas Raju
940302-3774
chara16@student.bth.se

Madhukar Enugurthi
950607-7537
maen16@student.bth.se

Abstract—**Cloud Computing has become an area of importance with increased applications in many software companies by offering many benefits in terms of low cost and data accessibility. However, there are still many challenges in solving these security issues in handling data. Therefore, security issues still remain the primary inhibitor to adoption of Cloud Computing services. The main objective of our research is to improve the quality of an existing framework in data security model. In this article, we strive to achieve the above goals with the help of a survey. On conducting a survey, We identified the hypothesis behind these issues and provide support for future research on Data security issue in cloud computing.**

I. GROUP MEMBERS PARTICIPATION

The group members participated in the idea creation and report writing with the amount of involvment displayed in table I.

Group member	Idea creation	Report writing
Chandrahas Raju	50%	50%
Madhukar Enugurthi	50%	50%

Table I
WORK REPARTITION

II. INTRODUCTION

Cloud Computing is one of the best emerging parameter in IT industry i.e. Cloud Computing is the latest trend in IT market. Users access their files and applications by accessing internet through cloud storage. This enable the user to utilize the set of resources of the server over the network. Cloud involves accessing the software applications. Cloud Computing also provides data storage and processing power over the Internet. Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. The term cloud has been used historically as a metaphor for the Internet. This usage was originally Derived from its common depiction in network diagrams as an outline of a cloud, used to represent the transport of data across carrier backbones (which owned the cloud) to an endpoint location on the other side of the cloud. There are three types of service layered models in Cloud Computing. Software as a service(SaaS), Platform as a Service(PaaS) and Infrastructure as a Service(IaaS). Customer obtain the facility to access use an application or service that is hosted in the cloud for example Microsoft provides software as a service in Microsoft Office web application are accessible to office volume licensing customer and office web application is called SaaS. Customer obtain access to the platform by enabling them to organize their own software and application on cloud environment and control their application but they can't manage servers and storage. It shares platform for customer software application configuration, testing and development of application this is called PaaS. The facility provided to the customer is to leave processing storage and other fundamental computing resources.

The customer does not manage or control the basic cloud infrastructure but has control over Operating System, storage, deployed application is called IaaS.

A. Background

The main concern in Cloud Computing is the security issue, even though many researchers have been focused in this area they have not found the perfect solution yet. The impact of cloud services on the business sector is tremendous. With the increase in the end-users, there is an increasing growth in the number of Cloud Service Providers (CSP) as well. The CSP is a third party that maintains and manages information about another entity [3]. To know the security aspects and frameworks that are mitigating the issue which are present in current literature, we studied few Systematic Literature Review (SLR) and articles about security issues to gain knowledge in the present literature As we studied about few SLR's and articles regarding security issues in Cloud Computing, we gained some knowledge about what are the issues Cloud Computing is facing in security. By analyzing all the SLR's we have found that the effective framework is missing to mitigate the data security model issues. So our purpose of this research is to provide improvement in quality of existing framework related to data security in Cloud Computing.

B. Objectives

The main aim of these research is to improve the quality of the data security in cloud. That is how the data is going to be secured from malicious prosecution. The main focus of this research is to make the readers gain the knowledge about quality improvement in data security.

C. Structure

The report is structured in the following way: Section III gives the motivation and background of this report. Section IV shows how the plan in conducting the research is done. Section V gives deals with how the research have been performed. Data extraction, analysis of data and interpretation of the results were discussed in Section VI. Previous knowledge with important novelties and their threats to validity in research is discussed in Section VII. Conclusion and summary of our work is explained in the final or last section.

III. BACKGROUND AND MOTIVATION

The focus on cloud computing was a obtained when the search was made related to latest technologies. Many of the results shown to us was related to Cloud Computing and effects of security in cloud. Later we gained some knowledge in Cloud Computing and found that security was the major problem in the cloud then our focus was shifted to how to save the data in cloud. Then we have studied about the security models in the Cloud Computing.

a) : Initially a reviews was assist to know importance of am ligating Cloud and security, then later we have planned to target on improvement in the security. Cloud is having a feature called parallel computing which allows to store lager amount of data. Cloud is basically on the remote servers which can have large measure of data for which the security issues are more.

b) : The Author of (Data security issues) has conducted a survey on problems that the cloud is facing in the security and privacy which helps the future developers in building a better security system. The previous Authors said that use of cloud has rapidly increased, even though it has a wide range of market there is a lack in providing the security. Customers does not want to lose their private information as a result of malicious insider in the cloud. The purpose of this survey is to research on the security issues to eradicated the data lose in Cloud.

IV. RESEARCH DEFINITION

A. Research Objectives

The main objectives of these research is to provide improvements in the quality to an existing framework in data security. To identify basic structure for the framework related to data security in Cloud. Further analyzing of data in literature review for identifying the existing framework related to data security.

B. Research Questions

The research questions are:

- RQ1 What is the state of art for the framework related to data security?
- RQ2 How can the selected framework will increase the quality to mitigate the security issues relates to data security model?
- RQ3 What are the mitigation factors faced by the cloud regarding data security?

C. Research Method

When we have referred to selected empirical method using preliminary guidelines Kitchenham the ambiguity in selection of research method was solved. The above reference which we have given consist information related to selected empirical research method. There are five methods of research according to them which is relevant to software engineering are research by survey, case study, controlled experiments, action research and ethnography.

a) : The study on security models in cloud computing helps us answering RQ1. RQ2 and RQ3 are answered by conducting literature review to gain more knowledge about security issues in cloud. Data extraction from literature review is analyzed and we gain knowledge about framework related to Data security, by this we can answer RQ2 and further we provide enhancement to an existing framework which mitigates Data security model in Cloud Computing. On providing these improvements in quality to an existing framework we can answer RQ3.

b) : To answer all these research questions, we have selected quantitative method for data collection. The quantitative method is practitioner survey. We have selected this survey based on our research questions. This research questions can be answered by our targeted audience. The data collection is analyzed using grounded theory approach and that data is used to answer our research questions.

D. Unit of Analysis

The unit of analysis we have chosen after the research method was audience who are professional in our particular subject/topic. We have prepared a questionnaire and it is kept openly in the LinkedIn site. All the individuals who are answering that questionnaire are selected. After the selection, judgment sampling is done to those selected people. We have got few responses for our questionnaire. By this judgment sampling out RQ's got answered.

E. Data Collection

We have conducted an online survey through a questionnaire where the data is collected. In our questionnaire there are questions which are taken from our research questions. We have selected our responses from the highly professional people. By asking them the questions like their age of experience, where did they train in that particular topic etc. We got few responses and selected few responses which we felt as the best ones.

F. Data analysis

After the data extraction process is done from the resources, we started analyzing that data. We have divided the work between our team mates. We have chosen partitioning method sampling method. The data collected from different users are partitioned according to their age, experience and all. Then we have divide our work and analyzed the data individually and peer reviewed others work after the analysis and concluded the answers.

V. RESEARCH OPERATION

We started our research with a team of two people. We searched for what are the issues that Cloud Computing is facing. By searching this we have found that security is the major issue that the cloud has. A systematic literature review has been conducted for our topic in which we have referred to many of the papers related to our topic and found some gaps in that references. After finding the gaps in that research we have formulated the research questions as seen in the research definition and planning section (Research questions). The research questions are analyzed to select method for conducting a survey. Analysis is done by taking all the responses into consideration. The responses were taken into consideration in such a way that the people who are professional in Cloud Computing. The whole research process took 29 days.

a) : After the targeted professionals are identified we have prepared a questionnaire using google forms. The questions were related data security issues in cloud. It took 15days to get all the responses from the professionals. All the responses are compared and drawn a conclusion from it.

A. Quality Assurance

While doing an online survey there is a risk of user's bias. To overcome such kind of things we have framed questionnaire in such a way that user can answer questions without any preferences. All the answers came from the audience may not be correct, this may effect the quality of the research. To over come such kind of quality problems results from research websites are given more preference than the direct answers.

VI. Data Analysis and Interpretation

A. Data Analysis

The data analysis is discussed in this section based on our survey and literature review. Questionnaire is used in finding the data. Totally we got 14 responses from the different professionals. In all the 14 responses we found 5 responses suits our research questions.

a) : The response all we got are from the people who are working on cloud computing, software professionals, senior program managers, developers.

- RQ1 Solution: The different set of solutions for secure storing of the data in Cloud Computing are through homomorphic encryption, multi party computation and anonymity.
- RQ2 Solution: Data centric is one of the way in increasing the security in the Cloud Computing. If the data has gone into a public cloud, data security and governance control is transferred in a whole cloud provider. The best way of protecting the data in Cloud is by keeping the sensitive data secure using the data centric and file level encryption which works for both private and public Cloud Computing environment.
- RQ3 Solution: The mitigating factors faced by the Cloud during the data security is water

hole attack, compliance with data privacy laws in multiple geographies and so on. Coming to water hole attack done to Cloud during the security, this attack has 3 stages firstly the attacker does some reconnaissance and research on its target, in which employees of the targeted company who visits regularly. The second stage is insert an exploit into trusted sites. And finally takes advantage of their system vulnerabilities. The other method is Cloud environment is key and you must understand the respective data storage regulations. Most regulations include EU's very restrictive regulations accept that this a good solution. These are the mitigating factors faced by the cloud during the data security.

VII. Discussion

A. Contribution

This research provides to explore the improvement in security in cloud computing. Initially our focus was on Cloud Computing after gaining detailed knowledge in Cloud Computing we have found that the security is the major drawback in the cloud, so we have decided to work on the particular area that is about data security issue in cloud. So we have started our research on this topic. After the survey has done, different professionals have given their opinion on our questions we asked. RQ1 is based on the state of art framework related to data security, Our RQ2 is about the improvement in the quality of the data security and finally our RQ3 is about what is the mitigating factor facing regarding the data security by cloud.

B. Threats to validity

- Construct validity: In our questionnaire the respondents may misinterpret some terms so this causes construct validity. To avoid this, we kept our questionnaire simple.
- Internal validity: There is a problem of drawing a wrong interface from the data collection this lead to chance in internal validity. To avoid this, we used multiple methods of drawing the answers.

- External validity: As we kept a survey on this there is a problem of getting less number of response this cause external validity threat. To avoid this, we just increased the targeted population
- Conclusion validity: Our conclusion may cause the conclusion validity due to ambiguous drawing in the answers.
  To avoid this, we have spent enough time to draw the conclusions.

VIII. Summary and Conclusions

Cloud storage is one of the popular services provided by the cloud providers to store the customer data in a remote server. Even though the Cloud providers advertise that the stored information will be secure and intact, there are security attacks which lead to loss of data. To overcome the loss of data, the data security principles are implemented in different ways to protect the data [5]. It is a vital to take security and privacy into account when designing and using cloud computing services [6].

a) : After this research we can conclude that improving the security issue in data can be done by data security method. Our results show the data security can be eradicated using the data centric protection. In further we can eradicate this type of security issues by CIA model also.

b) : Due to limited amount of time we have collected only limited data that is only from 3 companies. In the future research we are planning to conduct more research on the methods which we are choosing.

References

[1] M. Sugumaran, B. B. Murugan, and D. Kamalraj. An architecture for data security in cloud computing. In *Computing and Communication Technologies (WC-CCT), 2014 World Congress on*, pages 252–255, Feb 2014.

[2] P. K. Tiwari and S. Joshi. A review of data security and privacy issues over saas. In *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*, pages 1–6, Dec 2014.

[3] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom. Cloud computing security: From single to multi-clouds. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 5490–5499, Jan 2012.

[4] D. Chen and H. Zhao. Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, volume 1, pages 647–651, March 2012.

[5] P. Dinadayalan, S. Jegadeeswari, and D. Gnanambigai. Data security issues in cloud environment and solutions. In *Computing and Communication Technologies (WCCCT), 2014 World Congress on*, pages 88–91, Feb 2014.

[6] M. Z. Meetei and A. Goel. Security issues in cloud computing. In *Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on*, pages 1321–1325, Oct 2012.

[7] S. D. Choubey and M. K. Namdeo. Study of data security and privacy preserving solutions in cloud computing. In *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*, pages 1101–1106, Oct 2015.

[8] Z. Tang, X. Wang, L. Jia, X. Zhang, and W. Man. Study on data security of cloud computing. In *Engineering and Technology (S-CET), 2012 Spring Congress on*, pages 1–3, May 2012.