PA2554: RESEARCH METHODOLOGY IN SOFTWARE ENGINEERING AND COMPUTER SCIENCE

SECURITY CHALLENGES AND THREATS IN CLOUD COMPUTING

Student Name	**P-number**	**Mail Id**	**Contribution (25% each if both contributed equally)**
Kola RamyaSree	9510241509	rako17@student.bth.se	25%
Vadrevu Surya Veera Anantha Sai Sudheer	9506081356	vasu17@student.bth.se	25%
Sai Nidhin, Kanminipaty	9708315495	kasd17@student.bth.se	25%
Venkata Manoj Kumar Mandalaneni	9611042517	mbvq17@student.bth.se	25%

TABLE OF CONTENTS **Page no.**

Abstract:

Cloud computing Security involves various technologies and security measures to provide security to the cloud services like data storing, providing Infrastructure /platform / Software as services. Our main aim is to identify and gather knowledge about threats and issues in Cloud Computing security and identifying the various mitigation strategies that can be used.We reviewed 21 papers that contain both issues and solutions in it and we also used survey research methodology to identify the barriers , headaches that cloud stakeholders face while using the services.we formulated a report combining these issues and provided them solutions.Research methods like Systematic Literature review, Survey were used to identify present security issues with cloud computing.

Introduction:

Based on NIST[1] "Cloud Computing is a model which is convenient, on-demand network access to the shared pool of Configurable Computing Resources which can be rapidly provisioned and released with Minimal Management Effort". Cloud computing is an approach to expand the capacity or capabilities dynamically without putting Resources into new frame work, training new faculty or licensing new programming. In the most recent couple of years, cloud computing has developed from being a promising business idea to one of the quickly developing fragments of the IT Business. As more data on people and organizations are set in the cloud concerns are starting to develop how safe an environment it is. Security is one of the real issues which decreases the development of cloud computing and confusions with information protection and information assurance continue to plague the market.

The Cloud provides several advantages like fast deployment, pay for use, lower cost, scalability, rapid provisioning, network access,greater resiliency, hypervisor protection against network attacks low cost disaster recovery and data storage solutions. As per the recent IDCI Survey, 74% of the IT Executives and CIO's cited security as a top challenge preventing their adoption of Cloud Service Model. Analyst assumes that in the coming five years worldwide market for cloud computing will rapidly increase to $95 Billion. And 12 percent of the overall software sector will move to the cloud during that period.

Presently, there are 3 Services in the cloud they were

1.Infrastructure as a service(IaaS)

2.Platform as a service(PaaS)

3.Software as a service(SaaS)

Infrastructure as a service:

This service basically delivers Virtual Machine Images as a service and the machine can contain whatever the developer wants. Instead of purchasing Servers, Software, Data Center Resources, Network Equipment, and expertise to operate them, customers can buy these Resources as an Outsourced Service,delivered through the Network Cloud. The consumer can automatically grow or shrink the number of Virtual Machines running at a given time to accommodate the changes in their requirement. For example, host firewall.

Platform as a Service:

It is another application delivery model. PaaS lets the consumer to deploy their applications on the providers cloud infrastructure using programming languages and tools supported by the provider. The consumer does not have to manage the underlying cloud infrastructure but has control over the deployed application. A recent example is the Google App Engine, a service that lets developer to right programs to run them on Google's infrastructure.

Software as a Service:

This service provides capabilities to the service subscribers to access provider's software applications running on a cloud infrastructure. The service providers manage and control the application. Customer doesn't have to own the software but instead only pay to use it through a web API.

A Cloud deployment model represents a specific type of cloud environment that is mostly focused on ownership, size and access. These deployment models again are classified into four different types public cloud, private cloud, community cloud, hybrid cloud. The origin of cloud computing was basically, formulated to reduce managing cost of hardware and software resources and also cloud computing can be accessed from anywhere. The main concern of cloud computing is security as cloud computing is never 100 percent secure as experts say this is the only reason where some people hesitate to adapt cloud computing.

Aim & Objectives:

The main aim of our study is

- To identify security challenges and threats that are prevalent in the cloud environment which form as barriers for adopting cloud computing from real world.
- Identifying the challenges and provide having mitigation strategies-Collecting solutions, guidelines from organizations for a challenge gathering with references.
- Identifying existing cloud computing security challenges, those are expected in future.

Our initial target is to differentiate the different data security difficulties and also alleviation measures which We have focused on the effect level of the Security challenges like Security.

Security:

Security in cloud computing means to a wide range to a wide range of technologies. It is established which controls to protect company's information, applications and related infrastructures to cloud computing. In fact in IT industry the important factor to secure the success of a system is the security of information. Cloud computing in the area of IT industry can't be excluded from this fact. Here in which the users do not have control over where and why there information being saved, The role of security providing is more important and it decreased the amount of trust towards services. All security risks in internet are present in clouds too because of service providing by internet, consequently security data in clouds is a burdensome and difficult tasks. Cloud systems also use routine protocols and security frameworks in internet (like security and data encryption protocols) but they are not context oriented, so they need a powerful set of security and policy protocols to transfer data satisfactorily and safely. Some of the key protocols prevalent in the present day cloud industry are :Data security,Network security, Data integrity,Data access,Authentication and authorization, Data breaches, Virtualization vulnerability, Availability, Backup, Identitymanagement and sign-on process.

In PaaS services the client can put the purchased applications under the cloud infrastructure. Again the client does not manage the cloud infrastructure by controlling the application on net, servers, storage space. But it can be able to control or manage the applications. Any security under application level such as host and avoiding net penetration is in the domain providers and control, so the provider provides strong guarantees for inaccessibility of data in the applications in question. Another quality of security to propose is the entitlements presented by the PaaS platform. Regarding to the cost advantages of PaaS, there are efficiencies to be obtained when considering PaaS as a resolution to enforce usual entitlements across all applications in an enterprise or organizations.

In IaaS, the improvers can have effective control over security as long as there is no security hole in virtualization management. Moreover in the virtual machines theory it is possible to show these problems but in reality there are lots of security problems.

Related Work:

With the literature we researched for this project, Some key factors were noticed within the existing real world cloud environment.

One literature work mentions that there are four security problems such as XML signature element wrapping, browser security, cloud malware injection attack and flooding attacks and their reactions. The authors of this work believe that these security systems need deep and comprehensive analysis because of attacks may use different vulnerable points which can cause unauthorized access to data by hackers or the invaders may put a damaging service on the cloud systems for special purpose and this can amount to loss for users or even the system itself. L. Ertaul et al. [19] the following challenges mentioned are losing control over data, data integrity, risk of seizure,incompatibility issues and failures in provider's security, cloud provider goes down. To gain total acceptance from all potential users, including individuals,small business to fortune 500 firms and government, cloud computing require standardization in the security environment and third-party certification to ensure that standards discussed about the data security challenges such as Data Segregation and Protection, Data Leakage Prevention and proposed a feasible solution to those challenges.The security issues related to the cloud environment. He also examined about the existing security approaches to secure the cloud infrastructure and their disadvantages.

In another literature work, Jon Bordkin [22] according to Gartner there are seven challenges in cloud that every customer should raise about these challenges before selecting a cloud vendor:

- ***Privileged user access.*** Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs
- ***Regulatory compliance***. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider.

- ***Data location.*** When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in.
- ***Recovery***. Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster.
- ***Long-term viability.*** Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event.
- ***Data Segregation***
- ***Investigative support.***

Understanding these challenges addressed in [21] ,made us gain knowledge about the cloud service vendors can expect their customers to ask upfront . This also encouraged us to do further more research by questioning ourselves how actually a service vendor can come up this possible mitigation strategies for the stated challenges.

Another study ,D. Zissis and D. Lekkas, "Addressing cloud computing security issues,"[13] , provided a categorization of cloud security threats to Multi tenancy issues, access control, malicious insiders, Data control, management console security.

A better study of these categorization helped in understanding the actual problems faced in the real time cloud scenarios.

Knowledge Gap:

The main gap in our knowledge and research comes when we consider the definition of Cloud Computing as per NIST i.e. "Cloud Computing is a model for convenient, on-demand network access to the shared pool of configurable computing resources that can be rapidly provisioned and released with Minimal Management Effort". This statement, although adequate, does not mention the Security aspect of Cloud Computing. Security is such an important aspect of this phenomena that there is no provision completely given for it without any drawbacks.

RESEARCH QUESTIONS:

With the view of achieving the goals and objectives, we tried to formulate the research questions to explain the following things. Identifying and analysing the existing security issues like challenges, threats, vulnerabilities in the present-day cloud computing. Provide the mitigation strategies for the prevailing security issues and threats.

To be able to cover these areas and with the analysis of research problems in the selected articles We formulated the following research questions,

Research Question 1:

From the Cloud stakeholders view, What are the critical security threats and vulnerabilities that are forming as barriers to adapt cloud computing applications in the present day?

Research Question 2:

What are the mitigation strategies to use by the cloud computing users to handle these existing challenges?

Research Question 3:

How would be the trends in the future security issues in cloud computing?

Importance of these research questions:

With the proper apprehension of the related work, It is intuitive that, there is no complete solution to provide for the existing cloud security challenges, also there are not any mentioned ideals in the application of the counter measures.In order to formulate the mitigation strategies for security issues, the problems prevalent are needed to be understood in detail, For this purpose we formulated the RQ1.Then the major part of concern is to provide the mitigation strategies/ application guidelines to address the actual risks.Which we try to focus on using RQ2.It is evident that that the applications to mitigate the cloud security challenges will not be completely effective like to eliminate security issues in cloud, we tried to address the future trends in cloud security issues using RQ3.

The importance of these RQs can further be comprehended with these factors. In research methodology formulating the research questions should be done carefully. For a good research question, it should be - relevant, clear and simple, manageable/feasible.

Relevance :

The research questions should be within the scope of problem being addressed. It should not be in such way to elaborate everything beyond the scope of the problem definition. As the current problem being addressed is to identify and analyse the cloud computing security issues, we formulated the RQ1 to identify the security problems existent and then we formulated the RQ2 to be able to provide the mitigation strategies to be used in order to solve the challenges. We tried to identify the future trends in the cloud computing security with the notion of using this report for further research in the future.

Clear and Simple:

The research questions should be clear without leading to any confusion. Further it should not be too simple or too complicated. The complexity of a research question can often hide the major concerns of the problem definition. We formulated all the three research questions to answer the major concerns in the problem area of the research articles and papers we reviewed. Also, there will be no ambiguity when referring to the scope of answer for these questions, as they are clear and thought - through.

Manageable/Feasible :

The research questions must be realistic and they should not carry the research topic out of scope and scale of the project. Keeping the time and resource constraints in the mind, the research questions are to be formulated. We formulated the aforementioned research questions, within the limitations of time data access, not stretching too much. RQ1 tries to address the major security issues present day. For this, we planned to make extensive literature review identifies the threats, challenges and vulnerabilities. From the review of the selected articles, which used survey methodology to gather data from cloud computing expertise and common stakeholders RQ2 can be addressed. With reference to the further.

Research Methodology:

There are two research methods selected for this study, as we felt multiple research methods result in better outcome.The research methods selected are Literature Review and Survey.Systematic Literature review would help to sort out the required literature and survey would let us know the real time scenario.Reasons for selecting these research methods based on cloud computing security are as follows,

- To collect the knowledge to summarize the existing cloud security issues.
- Through Systematic review the advantages and defects of each work can be enumerated. Then, investigate tendencies of the researchers to design a new strategy or select existing strategies.

Literature Review makes or allows to establish our theoretical framework and methodological focus. Literature Review , holds the basic meaning of understanding the context of the considered scholarly papers which yields the current knowledge, enough to have a foundation and advance further with the substantial findings of the research work.We chose this method as as to target all the three RQs.This literature review covers detailed understanding and extracting the initial knowledge for the articles stated in the References section.With this, we can review and do evaluation of each source , we gathered up research evidence regarding the existing cloud scenario and its various threats. The reason behind to choose this method is to summarize the vulnerabilities and threats concerning this topic that are defined by the previous researchers in their works and also to identify the current state and most important security issues for Cloud computing .Through the review the advantages and defects of each work can be calculated.

Survey is an exhaustive research technique for gathering data to describe, compare or clarify knowledge, attitudes and conduct. To efficiently gather data from a huge population to look for the data in the information and sum up to the wider population.We chose this as our main research method and by targeting RQ2,RQ1 and also RQ3 with less priority.

In programming field the most generally utilized research techniques are experimentation, case study and survey. An experiment is not suitable for our research since we are not dealing with a few conditions and end product relationship. Also, a case study investigates required information under controlled people in a specific time period. But our survey needs information from the impression of large number of population in a collective sense. So, we have chosen to perform a survey as the most suitable research method for our study.We have done literature study also and found few mitigation measures and then we performed survey and prepared questionnaire based on the mitigation measures from the literature study. Such that from the survey we will get much better results efficiently.

Sampling of our study:

The subjects of our survey are the people who are experienced in cloud, such as students, industrial experts(extensive cloud services users), and also the sample population of our survey will range between 20-30 of selected subjects. Our focus is a population who has experience in cloud computing. A questionnaire will be prepared through google forms and will be published to the population to obtain the required data. The feedback from the survey will be analyzed and based on the analysis the mitigation measures for the challenges will be identified.

Population:

The population for our research study are cloud users, students,employees, testers.

Population categorization:

Users	Students/ Employees	IT Employee	Professors
Age	19 - 30	46 - 50	Above 50
Experience (years)	8 - 10/naive	10 - 15	Above 17
Profession	Students	Testers	others
Background	Software Engineering /CS	Computer Science Engineering	Computer science Engineering

Knowledge level	Medium	High	High

Preparing online Question for survey -Gathering Inputs

For this survey method, we tried to define the following survey question in order to get the most of the cloud stakeholders and vendors.Following are the research questions.

1) What is your profession?

(a) Employee

(b) Professor

(c) Student

(d) Other

2)What do you Prefer for Data storage services ?

(a) Cloud Storage

(b) Legacy storage systems

(c) Others

3) What are your critical cloud security concerns while using the cloud services and how can they be addressed? (More like a subjective descriptive answer)

4)What are the biggest barriers for cloud services adoption ?(More like a subjective descriptive answer)

And then based on the majority of concerns we have understood from the existing researches, we phrased the following questions.

5). Is your data stored in the cloud was encrypted or not?

(a) Yes

(b) No

(c)Don’t know

6). Does the providers take responsibility for any loss of the particular data in the cloud?

(a) Yes

(b) No

(c)Don’t know

7). Do you believe that cloud providers establish efficient frameworks for data security controls?

(a) Yes

(b) No

(c)Don’t know

8).Does the presence of Malicious Insiders affect the efficiency of the cloud?

(a) Yes

(b) No

(c)Don’t know

9). Do you think security aspects like authorization and authentication are fulfilled by cloud providers?

(a) Yes

(b) No

(c)Don’t know

10). “Cloud Computing do not have vulnerabilities associated with the internet applications.”

(a) True

(b) False

11). Does backup and recovery services are provided in cloud computing?

(a) Yes

(b) No

(c)Don’t know

12). Does cloud service provider provide factors like customer specific data masking and ensures data integrity?

(a) Yes

(b) No

(c)Don’t know

13). How does the future security challenges going to be like in cloud industry(Answered as subjective descriptions)

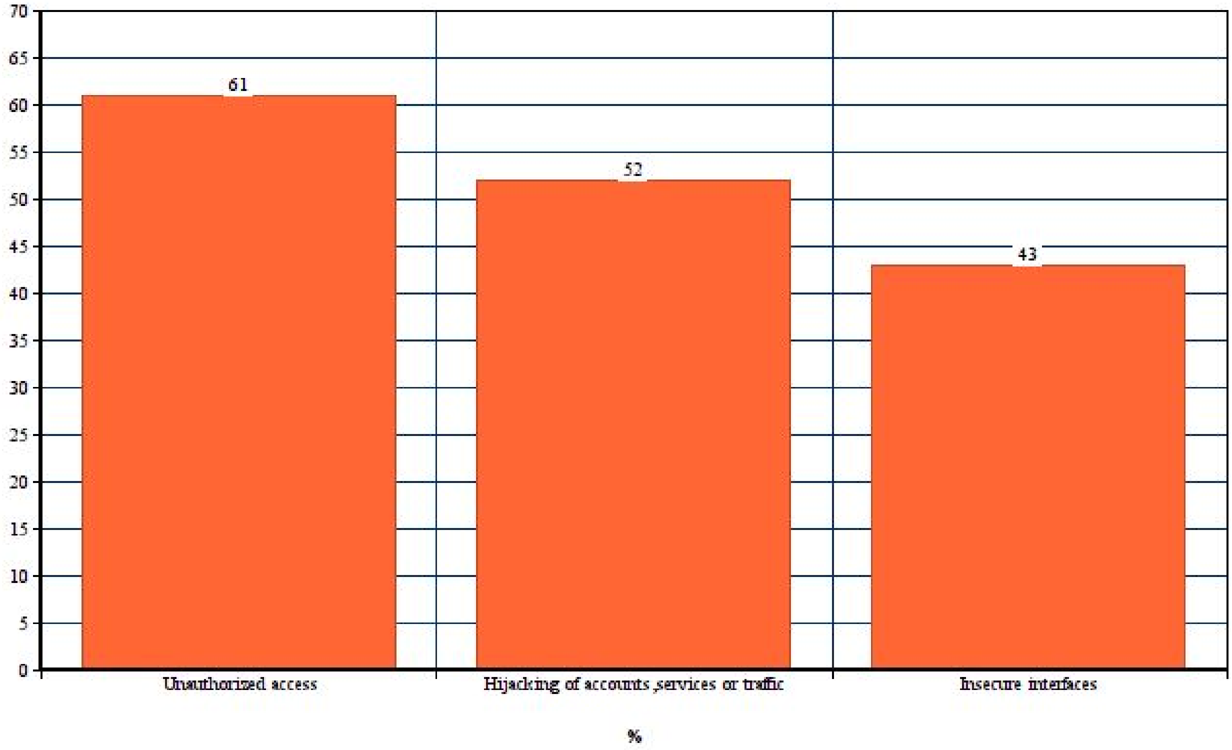
Data Collection:

The questionnaire is prepared using google forms to get the required data. These google forms were posted in the social media sites and also the student groups and google groups with our peers. We requested all our peers to forward the questionnaire as much as possible in order get a better data to analyse.All the acquired data was examined and analyzed to answer our research questions.

Data Analysis

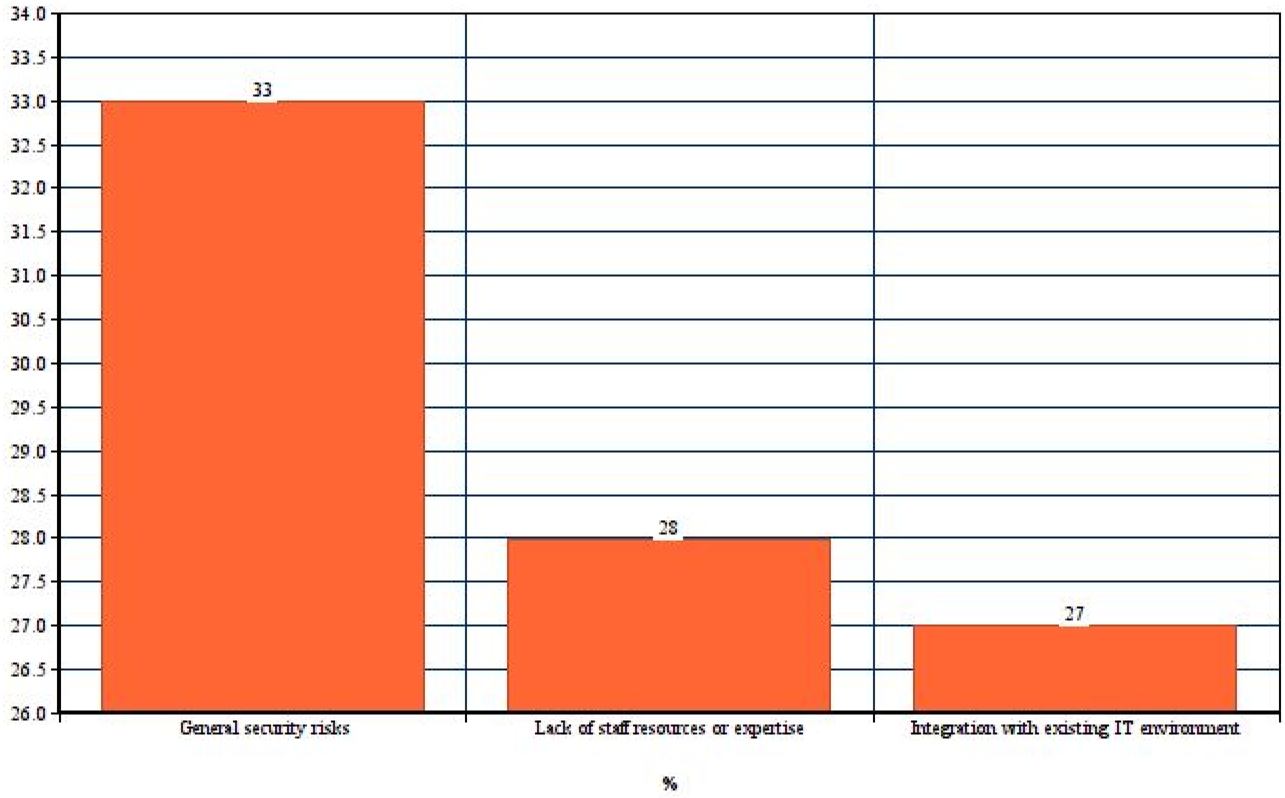
From the above survey we collected the answers responded from the population.

- For the first question , we got the answers dependant on the roles of the participants.Most of the participants are former computer science/software students who now are working in cloud industry.Other Group of participants are current students, software testers, general cloud service users.
- For the second question, nearly 70% of the participants came up with the answer that, they are comfortable using cloud services rather than legacy storage services.
- For the third question, we got more subjective answers from the participants and we encouraged them to give a description in support of their answer, so we can understand better.And the following demonstration describes the participants biggests concerns :



Participants Critical Concerns in Cloud services Applications

- For the next question also we got more subjective answers from the participants and we encouraged them to give a description in support of their answer. And the demonstration looks as follows:P



- Participants Biggest barriers to adapt cloud services

- All the remaining questions are yes/no questions that can be used to gather the participants inclination in various cloud scenarios.The response to these questions made it clear that the cloud service vendors strive to provide various efficient methods for secure cloud services, the cloud stakeholders still feel the headache of factors like transparency of cloud infrastructure (which rises the challenge of malicious insiders), cloud vulnerabilities that come up with internet applications.

From the above analysis, we can get into an idea about the present situation and also the majority challenges that are present in the modern life.As we know this survey is also helpful for even further developments that can be made to maintain security for the data.Therefore, this will be considered as a general and open trust in cloud computing. To ensure protection in cloud computing we likewise propose strict control and decides that they are prepare and reject by states alongside continuous and strict checking to achieve the perfect point. Moreover, an organization for security as a medium between provider and user should be built to secure data transfer security in clouds aiming safe data transformation so that no one expect the organization itself have information about the transformation and mechanisms and handled algorithms of data transformation and the user can see input or make it ready to transfer in cloud space by a decoder which the provider provides for him [6]. So trust in cloud frameworks will be upgraded and the clients enthusiasm to utilize this technology will be increased. In addition, the providers concerns about security will be answered and they will do their best to improve security and so there is any need to provide security by them.

Result - Expected Outcomes:

The complete cloud Services context presents an added risk on the services as the cloud users data is often outsourced to a third party involved.In our research, with the considered research methodologies, the aforementioned research questions are addressed in brief and the possible outcomes for each of those RQs are formulated as follows:

1. ***RQ 1: From the Cloud stakeholders view, What are the critical security threats and vulnerabilities that are forming as barriers to adapt cloud computing applications in the present day?***

- With the studied literature, we analyzed the risks and threats. After analysing the existing vulnerabilities in cloud computing ,the authors of the various research works concluded that 'Data Storage' and 'Virtualization' are the most critical vulnerabilities and an attack to them can do the most harm. Analysing the threats that are related to the cloud services technology used, it is indicated that cloud service models are exposed to these threats and identified the threats that are associated with data being stored and processed remotely, sharing resources and the usage of virtualization.

- In the survey research method, When asked about the biggest barriers to overcome in order to provide integral secure services, we collected the following barriers -

  - General Security Risks

  - Lack of staff resources or expertise

  - Integration with existing IT environment

- We also tried to provide the possible outcomes for the RQ1, from the cloud stakeholders point of view. We aggregated some of the data collected from the Survey research method to identify the security threats and vulnerabilities .The critical cloud security threats are -

  - *Unauthorized access*:Specifically unauthorized access through mis usage of employee credentials(can be third party or other vendor side employees) and misleading access controls

  - *Hijacking of accounts, services or traffic* :Mis usage of the traffic often by the third parties collaborated with the cloud vendors.Stolen identity by the hijackers to conduct malicious and unauthorized activities.

- *Insecure interfaces / APIs.* Cloud service vendors provide a set of interfaces /APIs for the their customers to manage their cloud services.These interfaces /APIs often result in API dependencies and logging restrictions.

2. ***RQ 2: What are the mitigation strategies to use by the cloud computing users to handle these existing challenges?***

- From the literature review method , we summarized the potential mitigation strategies shall be- build up user trust by limiting the access rights, keeping track of user transactions and enhancing the privacy preserving protocols.Also following the strategies like use of central global transaction manager, following electronic communication privacy act, re-evaluating security models enhances the security mechanism.Some of these strategies like access rights restriction,enhancing the privacy preserving protocols, following electronic communication privacy act, re-evaluating models can truly restrict the security threats to a huge extent, on the downside in the order of providing security there are mitigation strategies like use of central global transaction manager and keeping track of user transactions will make the users compromise on their confidentiality to some level.
- Through the data collected from the participant response in the survey, following are the key strategies :
  - By robust cloud security controls to provide deep visibility,
  - Multi factor authentication for the users.
  - Policy automation for verifiable and comprehensible security management.
- Also,there is a gap prevalent between the traditional security systems and the security requirements for present day cloud scenarios. Traditional security tools are not designed for cloud environments.. The need to secure cloud access from anywhere across highly dynamic, virtual cloud environments simply breaks the traditional network perimeter defense approach designed for the purpose of traditional data systems security.The survey results confirmed that traditional methods are woefully inadequate in securing the cloud. The gap is primarily in controlling and verifying security policies into cloud infrastructure security

3. ***RQ 3: How would be the trends in the future security issues in cloud computing?***

From the both survey and literature review methods, we summarized the potential security issues in future of cloud industry.The security challenges expected to be faced in future are as follows:

- Threats like Hypervisor viruses, Malicious insiders, Abuse and nefarious use of Cloud Computing
- Vulnerabilities like Shared technology vulnerabilities, Service and traffic hijacking , Risk of multiple Cloud tenants, Insecure application programming interfaces
- Virtual machine security
- Smartphone data slinging

TRENDS:

As the cloud service providing companies are using multiple security tools like Data loss prevention softwares, Security information and event management(SIEMs) antivirus software, these result in humongous data which will be hard to manage alert on the critical signs for security threats.To gain better view of the data , the organizations adapting for advance data management practices like User and Entity Behaviour Analytics(UEBA) will be one of the trending aspects of the future cloud industry

In our research, we mainly concentrated on the different measures which to improve the data security challenges. By this survey, effective and the required data which were used to overcome the security challenges in the cloud computing is obtained. Also, based on our analysis various measures to improve the cloud computing is explored. Through our review, we expect that the after effects of our study could be utilized as a part of future research and ongoing applications. The identification of security challenges and mitigation techniques in cloud computing is challenged by considering the large number of services.most of the responses from the survey ,noted that cloud computing will place the dominant and expandable information transactions.

- Regarding critical security threats and vulnerabilities that are recurring present day cloud computing applications and for the cloud stakeholders
- The mitigation strategies that are to be used by the cloud computing users to handle the existing challenges.
- To know various trends for future security issues in cloud computing.
- To provide high security for the data from looting, like only particular user authentication.

Time and activity plan:

1. Discussion of the topic: jan25th - feb1st

2. Selection of topic: feb1st - feb3th

3. Work on proposal: feb3rd - feb8th

4. Submission of research proposal: feb8th

5. Action plan discussion: feb12th - feb16th

6. Selecting research methods: feb16th - feb23rd

7. Implementation of research methods: feb23rd - mar3rd

8. Discussion of controlled experiment: mar5th - mar8th

9. Participants in survey: mar8th - mar13th

10. Detailed study design: mar13th - mar18th

11.Re-discussion on failures: may10th-may15th

12.Necessary improvements: may16th-22nd

13)Final resubmission: 29th may

Work Breakdown Structure:

• Research Proposal

• Literature Review

• Research Questions

• Research Method

• Risk Management

• Survey

- Sampling of our study

- Population
- Population categorization

• Preparing online Question for survey -Gathering Inputs
• Forwarding the Questionnaire
• Data Collection
• Data Analysis
• Result - Expected Outcomes

Risk management:

1)some of the risks that are to be managed in cloud computing are data integrity, privacy and also data recovery which are not in our control. It implies there is risk regarding data.
2)sometimes malicious threats are occurred regarding data in cloud.
3)Risks regarding unauthorized access to business and even customer data.
4)As it is based on internet there are more chances for hack attacks.

Mitigation strategies of risk management:

1)By providing authorized access like maintaining strengthen passwords.
2)Performing effective and careful effort while doing research on a cloud service provider.
3)we can also implement end-to-end encryption and also secured communication protocol
4)By using also up to date systems it means not use outdated operating systems.

Conclusion:

In this project, the introduction to the cloud computing, its security is given.We then pointed the context of the scenario we are currently working on.We defined the related work we reviewed for this research and knowledge gained through that work.We then defined the aims and objectives of the report, formulated the research questions and discussed the importance of the formulated research questions and relevance.We then discussed in detail about the research methodologies we chose, their importance in our context of research and the process of it in detail.We provided the data collection and data analysis we did by one of the research methodologies i.e, Survey method.

References:

[1]NIST -National Institute of Standards and Technology

[2]Clavister. Security in the cloud, Clavister White Paper /http://www.it-wire.nu/ members/cla69/ attachments/CLA_WP_SECURITY_IN_THE_CLOUD.pdfS [accessed on: 21[2] October 2009]

[3] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

[4] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, Mar. 2012

[5] Gharehchopogh, Farhad Soleimanian, and Sajjad Hashemi. "Security challenges in cloud computing with more emphasis on trust and privacy."International Journal of Scientific & Technology Research 1.6 (2012): 2277-8616.

[6] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[7] K, Sachdeva, Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis, University of Texas, Austin, 2011.

[8] Winkler, Vic JR. Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier, 2011.

[9] Gajek, Sebastian, Lijun Liao, and Jörg Schwenk. "Breaking and fixing the inline approach." Proceedings of the 2007 ACM workshop on Secure web services. ACM, 2007.

[10] Descher, Marco, et al. "Retaining data control to the client in infrastructure clouds." Availability, Reliability and Security, 2009. ARES'09. International Conference on. IEEE, 2009.

[11]. Ahmed S, Raja M. (2010) 'Tackling Cloud security issues and forensics model', High Capacity Optical Networks and Enabling technologies (HONET) , 19-21 Dec, pp. 190-195.

[12]. Gabriel Antoniu. Autonomic cloud storage: challenges at stake. In Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on, pages 481–481,

2010.9. F. Ogigau-Neamtiu, “CLOUD COMPUTING SECURITY ISSUES,” Journal of Defense Resources Management, vol. 3, no. 2, pp. 141–148, Jan. 2012.

[13] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, Mar. 2012.

[14]. S. Bulusu and K. Sudia, A Study on Cloud Computing Security Challenges. 2013.

[15]. M. D. Ryan, “Cloud computing security: The scientific challenge, and a survey of solutions,” Journal of Systems and Software, vol. 86, no. 9, pp. 2263–2268, Sep. 2013.

[16].“Security in cloud computing,” Int. J. Inf. Secur., vol. 13, no. 2, pp. 95–96, Apr. 2014.

[17]. S. Pandey and M. Farik, “Cloud Computing Security Latest Issues amp Countermeasures,” International Journal of Scientific & Technology Research, vol. 4, no. 8, pp. 27–30, Aug. 2015.

[18]. D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science and Technology, Vol. 3 No. 4, 2011, p. 2672- 2676.

[19]. L. Ertaul, Levent, Sarika Singhal, and Gökay Saldamli. "Security Challenges in Cloud Computing." Security and Management. 2010.

[20]. Rao, R. Velumadhava, and K. Selvamani. "Data security challenges and its solutions in cloud computing." Procedia Computer Science 48 (2015): 204-209.

[21]. Akhil Bhel, Emerging Security Challenges in Cloud Computing. Information and Communication Technologies, in: 2011 World Congress on, Mumbai, 2011.p.217-222

[22]. Jon Brodkin, “ Gartner: Seven Cloud-Computing Security Risks”, Available: http:// www.infoworld.com, published July 2008, pp. 1-3.