ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

Data security issues in Cloud Contact Center as a service – A Review

Madhusudan KL[1], Dr. Paramashiviah P[2], Dr. Narahari NS[3]

Research Scholar, Dept. of Studies & Research in Management, Tumkur University, Tumkur, Karnataka State, India[1]

Dean and Chairman, Dept. of Studies & Research in Commerce, Tumkur University, Tumkur, Karnataka State, India[2]

Prof, Dept. of Industrial Engineering & Management, RV College of Engineering, Bangalore, Karnataka State, India[3]

Abstract*:* An exhaustive list of security issues/concerns is associated with hosted contact centers and these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers. Today's hosted contact centers are increasingly complex and it is not devoid of the security breaches and issues. One of the most important aspects to be considered before implementing cloud solutions is data security. While some data security issues are inherited from the solutions adopted to create such services, many new security issues which arise, includes those related to how the services are organized and which kind of service/data can be placed in the cloud. Also with the extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization must be adequately configured, managed and secured and its specific concerns include the potential to compromise the virtualize software, or "hypervisor". In this article, an attempt is made to identify and classify the main security concerns and solutions in cloud computing, and propose suitable security taxonomy.

Keywords: IT, Cloud Computing, CCaaS, BPO, IT Security, hacking, CSA, NIST, ENISA, taxonomy

I. INTRODUCTION

Contact Center as a Service is a next generation, cloud-based contact center solution that allows you to minimize capital expenses and reduce operational costs. Cloud Contact Center as a Service (CCaaS) is a global service using cloud based infrastructure and a software as a service model to deliver a features based application to Contact Center customers. It provides a fully integrated approach to multichannel customer service solutions, which delivers information through multiple delivery channels – including phone, E-mail, interactive voice response, portals and IM/web chat. This solution can be provided as a technology only solution or can also be full turned-key solution including the agents. CCaaS cuts down on capital expenditures while providing complete contact center solutions that enhance talent and improve customer service.

A. Business Benefits

Cloud Contact Center as a Service (CCaaS) enables deployment of a ready-to-go IP contact center and introduces next-generation applications such as computer-telephony integration (CTI), social media and multimedia including email and chat. In addition to the standard Contact Center applications offered, CCaaS can also integrate other types of applications such as:

1. skills based routing
2. call recording
3. Interactive Voice Response (IVR) / Voice Portal (VP)
4. Workforce Management (WFM)
5. Voicemail (VM)
6. screen pop (CRM integrated)
7. soft client application

Costs are reduced by the inherent cost savings of for voice, including simplified management when it comes to moves and changes. Calls can be directed transparently to any location that has an Internet connection, including home workers and branch offices, resulting in improved service levels, flexibility and scalability during peak demand. The ability to place representatives remotely will also allow you to hire and retain the best talent.

II. LITERATURE REVIEW

The existing publications related to CCaaS technology and Data security issues in cloud computing is reviewed. The objective is to assess what has already been researched and identified and leverage certain contents relevant to this research thesis.

A. Review of Literature on CCaaS

1. Anthony T. Velte, Toby J. Velte and Robert Elsenpeter, Cloud Computing – A practical Approach, TATA McGraw Hill publication.

The authors have given an in depth coverage of the basics of cloud computing. A thorough understanding of the technologies involved in cloud computing can be gained through a review of this seminal work by the authors.

2. Wikipedia, http://en.wikipedia.org/wiki/Contact_centre(business), Contact Center (business)

The Wikipedia defines contact center as "centralized office used for the purpose of receiving or transmitting a large volume of requests by telephone". This definition helps in building up the basic understanding of the mechanics of the contact center. However the intrinsic aspects and the workflow processes have to be analysed to great level of detail in order to develop secure systems for implementing contact center as a service.

3. Brian Hinton, www.contactcenterpipeline.com, Contact centers in the clouds.

This blog highlights the potential benefits and risks associated with CCaaS technology. A thorough understanding of contact center in the clouds is evident as the blog points out the strong and weak points of CCaaS technology.

B. Review of Literature on Data Security in CCaaS

1. Nelson Gonzalez, Charles Miers, Fernando Redigolo, Tereza Carvalho, Marcos Simplicio, Mats Naslund and Makan Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing.

The authors have provided quantitative analysis and in depth coverage of the current data security issues in the cloud computing technology. A thorough understanding of the data security issues in cloud computing can be gained through a review of this seminal work by the authors.

2. D. Catteddu and G. Hogben, Benefits, risks and recommendations for information security, November 2009

The authors have enlisted information security benefits, risks and recommendations. A thorough understanding of the information security, its benefits, risks and recommendations can be gained through a review of this seminal work by the authors.

3. E. Young, Cloud computing - the role of internal audit, October 2009

The author has given an in depth coverage of the role of internal audit in cloud computing. A thorough understanding of the necessity and role of internal audit in cloud computing can be gained through a review of this seminal work by the author.

4. NIST, Draft cloud taxonomy, March 2011.
5. Microsoft whitepaper, How Microsoft secures its online services, 2009.
6. J. Oltsik, Information security, virtualization, and the journey to the cloud, August 2010.
7. D. Tompkins, Security for cloud-based enterprise applications, February 2009.
8. J. Brodkin, Seven cloud computing security risks, January 2008.
9. J. Pavolotsky, Top five legal issues for the cloud, April 2010.
10. D. Hubbard, L. J. H. Jr, and M. Sutton, Top threats to cloud computing, March 2010.

III. SIGNIFICANE OF THE STUDY

Aiming to organize the information related to cloud security and to facilitate further studies, this research paper identifies the main problems in the cloud security data area and group them into a model composed of seven categories: network security, interfaces, data security, virtualization, governance, compliance and legal issues. To gather the information required for building these categories, CSA's security guidance and top threats analysis of ENISA's security assessment and the cloud computing definitions from NIST are referenced.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

IV. PROBLEM STATEMENT

Data security is a key feature for cloud computing, by consolidation as a robust and feasible multi-purpose solution. This viewpoint is shared by many distinct groups, such as academia researchers, business decision makers and government organizations. The many similarities in these perspectives indicate a grave concern on crucial security and legal obstacles for cloud computing, including service availability, data confidentiality, provider lock-in and reputation fate sharing. These concerns include not only existing problems, directly inherited from the adopted technologies, but also new issues derived from the composition of essential cloud computing features like scalability, resource sharing and virtualization (e.g., data leakage and hypervisor vulnerabilities). Data security is the number one issue when it comes to cloud computing. Since a third party stores business data, it is never known what's going on with the data. Along with the benefits of BPO comes an increased risk to data. If the Organization cannot protect its data, the business is at risk. However, the organization constricts the use of data too much; the restriction can paralyse the outsourcing effort – and finally the business itself.

A. Quantitative Analysis of CCaaS Security issues

Below mentioned quantitative data is sourced from the research thesis authored by Nelson Gonzalez, in his thesis titled 'A quantitative analysis of current security concerns and solutions for cloud computing'. The objective of the referred thesis was to identify all current security concerns related to cloud computing. The referred research thesis summarizes the possible cloud computing security flaws that are related to CCaaS application architecture and the flaws pertaining to grouped categories of the technology.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

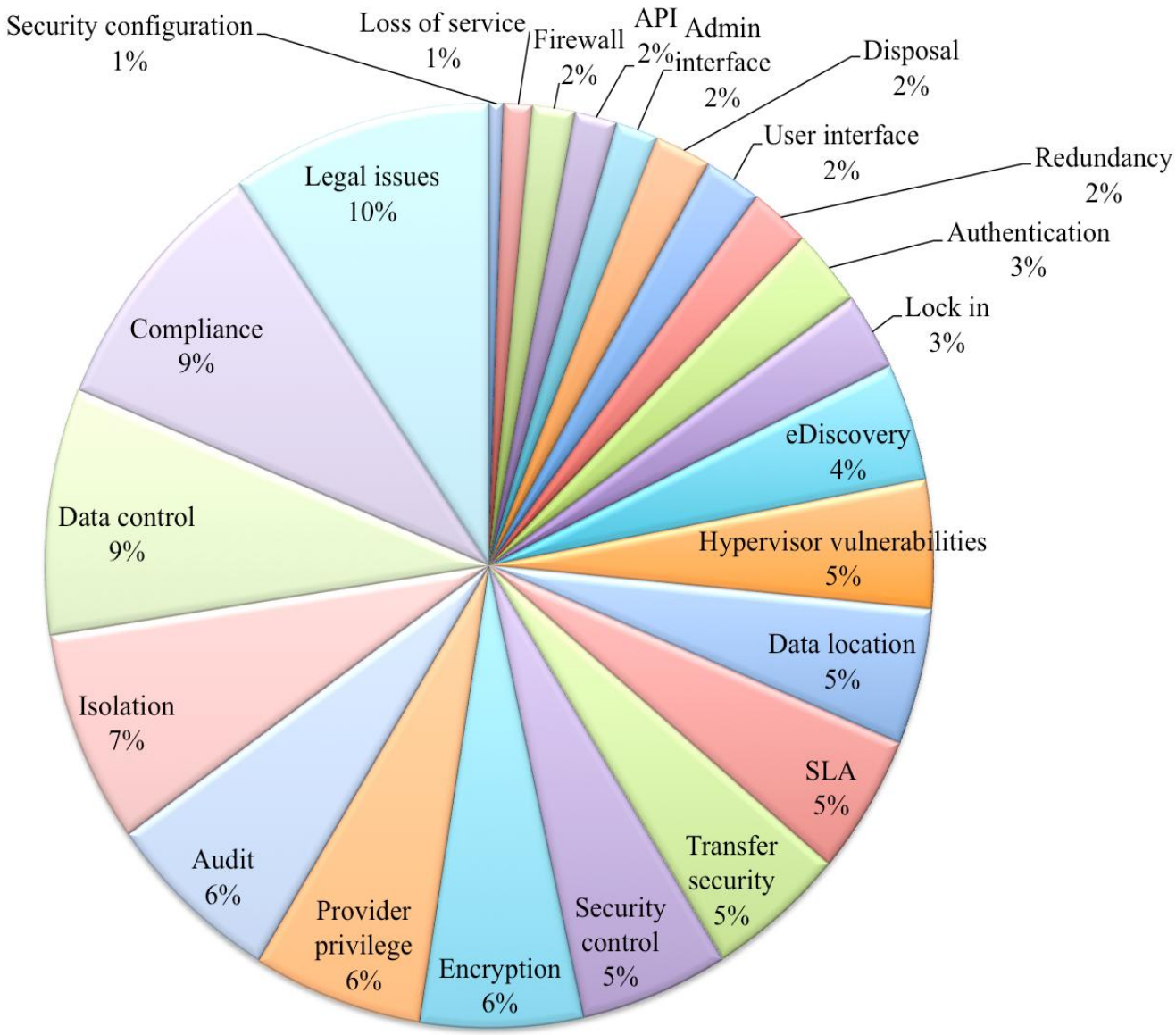

Figure 1: Pie chart showing the distribution of various security concerns in cloud computing solutions

Source: "A quantitative analysis of current security concerns and solutions for cloud computing" by Nelson Gonzalez.

As can be seen from the Figure 1, the top four CCaaS Security issues that frequently occur are listed as:

1. Legal and Administrative issues represent a majority with 10% of the Security issues
2. Compliance issue is the second Security issue with 9% occurrence.
3. Data Control is the third Security issue with 9% occurrence.
4. Isolation, which is technological issue, is fourth with 7% occurrence.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

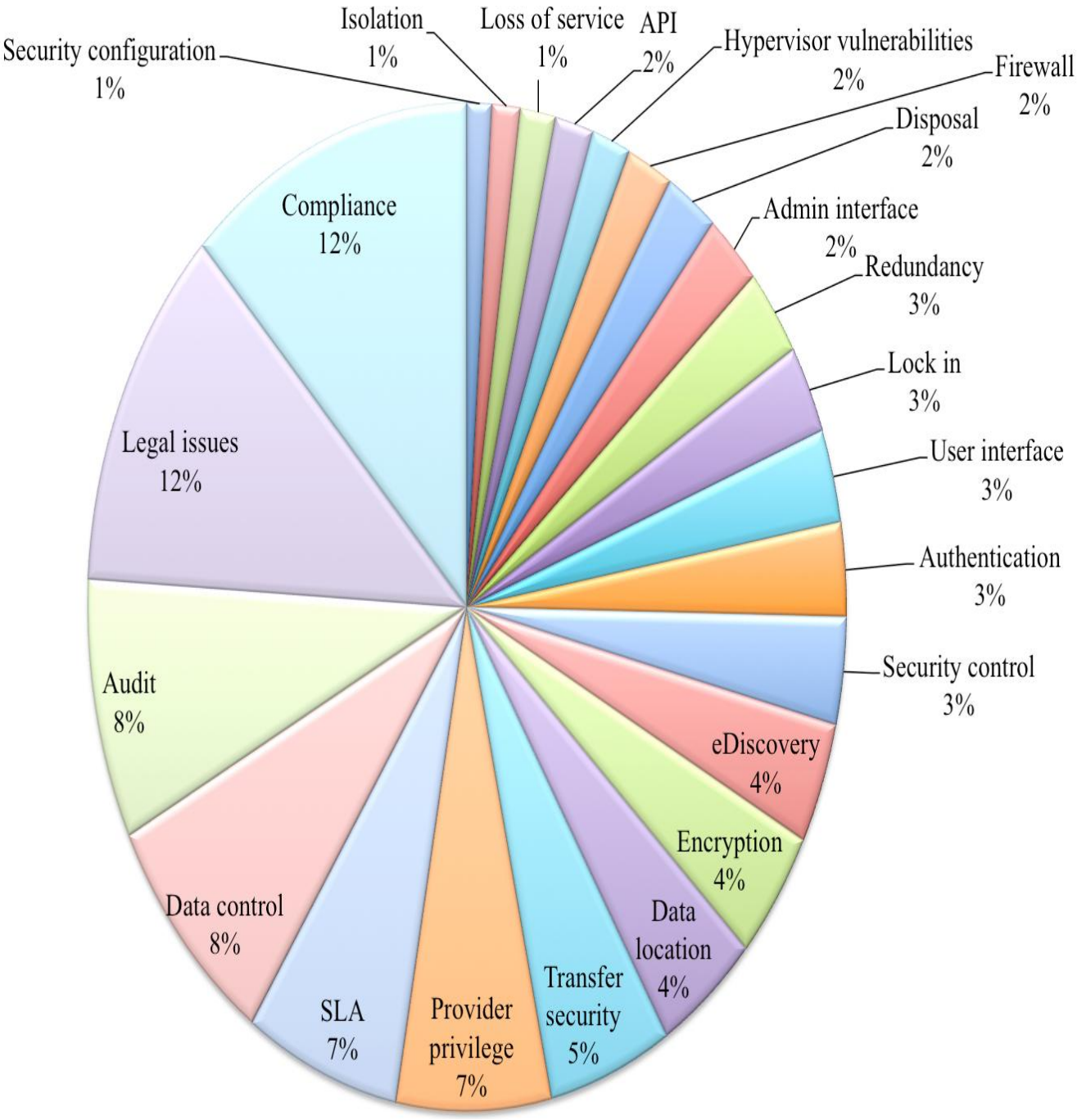

Figure 2 – Pie Chart depicts the various BPO Security issues

Source: "A quantitative analysis of current security concerns and solutions for cloud computing" by Nelson Gonzalez.

As shown in Figure 2, the top four BPO Security Solution issues that frequently occur are listed below:

1. Compliance issue tops the Security solutions issue with 12% occurrence.
2. Legal issue occurs second with 12% occurrence.
3. Audit issue occurs with 8% occurrence.
4. Data Control issue occurs with 8% occurrence.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

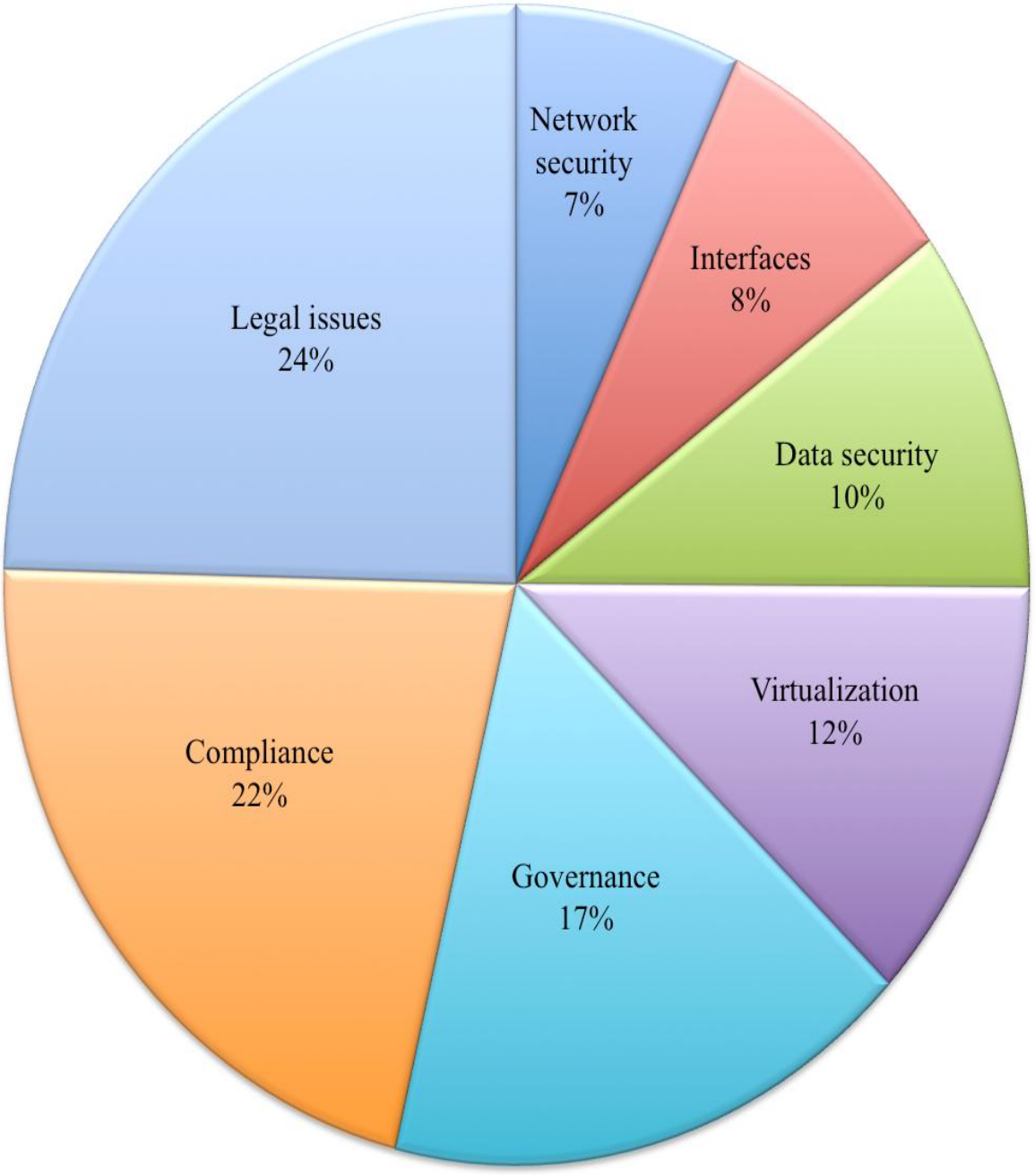

Figure 3 – Pie chart depicts various CCaaS security issues

Source: "A quantitative analysis of current security concerns and solutions for cloud computing" by Nelson Gonzalez.

The top four grouped categories CCaaS Security Problems are listed herein:

1. Legal issue tops the grouped categories Security problems with 24% occurrence.
2. Compliance issue occurs second with 22% occurrence.
3. Governance issue occurs with 17% occurrence.
4. Virtualization issue occurs with 12% occurrence.

V. RESEARCH GAPS

Below mentioned quantitative data is referred to research thesis authored by Mr Nelson Gonzalez, in his thesis titled 'A quantitative analysis of current security concerns and solutions for cloud computing.

ISSN: 2319-8753
International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

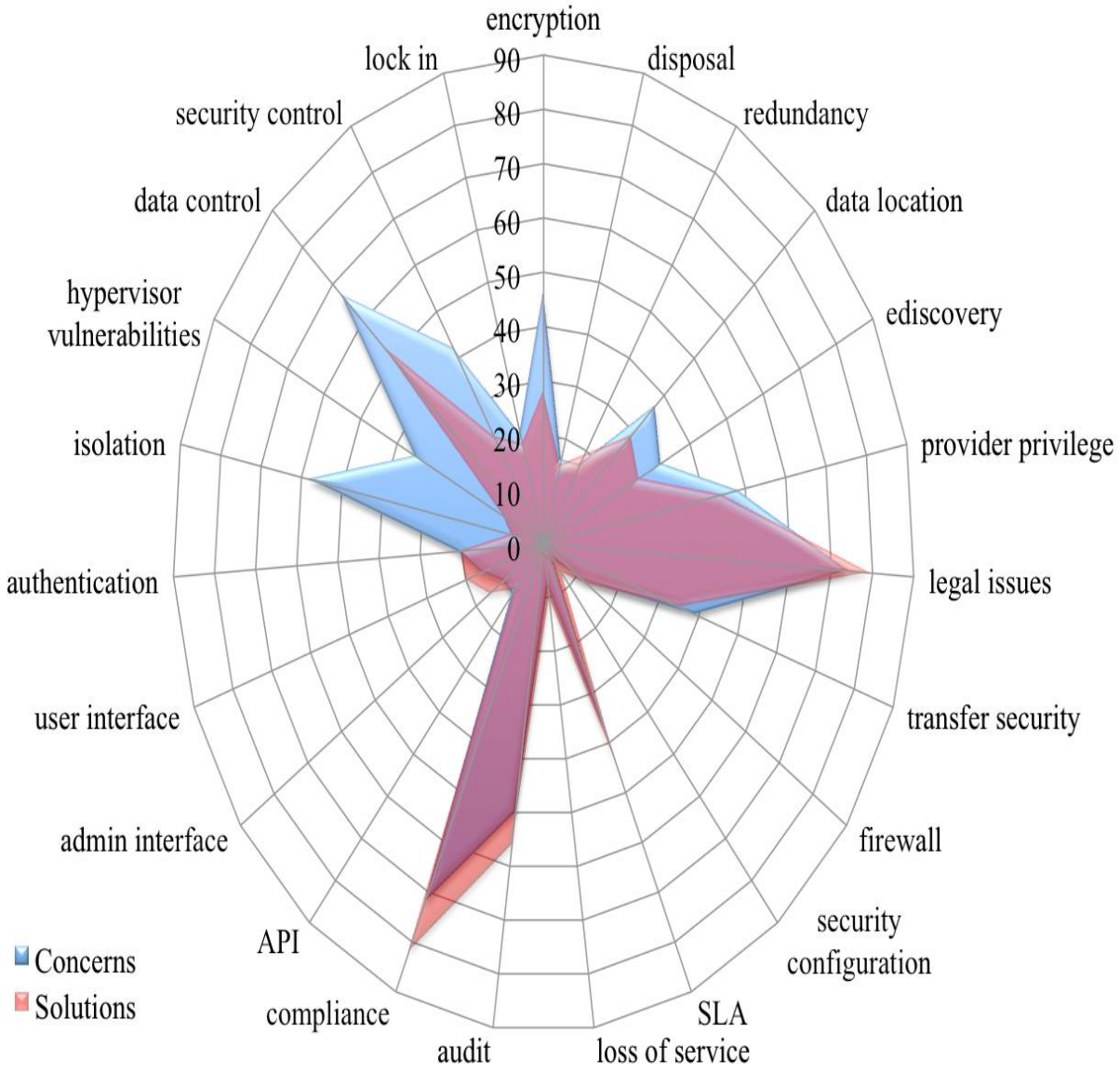

Figure 4 – Pie chart depicts the security gaps

Source: "A quantitative analysis of current security concerns and solutions for cloud computing" by Nelson Gonzalez.
The differences between problem and solution citations presented in the second chapter are observed in Figure.

The blue areas represent concern citations, lighter red for solutions and darker red where they overlap. In other words, light red areas are problems with more citations for solutions than problems – they might be meaningful problems, but there are many solutions already addressing them – while blue areas represent potential subjects that have received little attention so far, indicating the need for further studies.

The Figure 4 clearly shows the lack of development regarding data control mechanisms, hypervisor vulnerabilities assessment and isolation solutions for virtualized environments. On the other hand, areas such as legal concerns, SLAs, compliance and audit policies have a quite satisfactory coverage. The results for grouped categories are depicted in the below figure.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

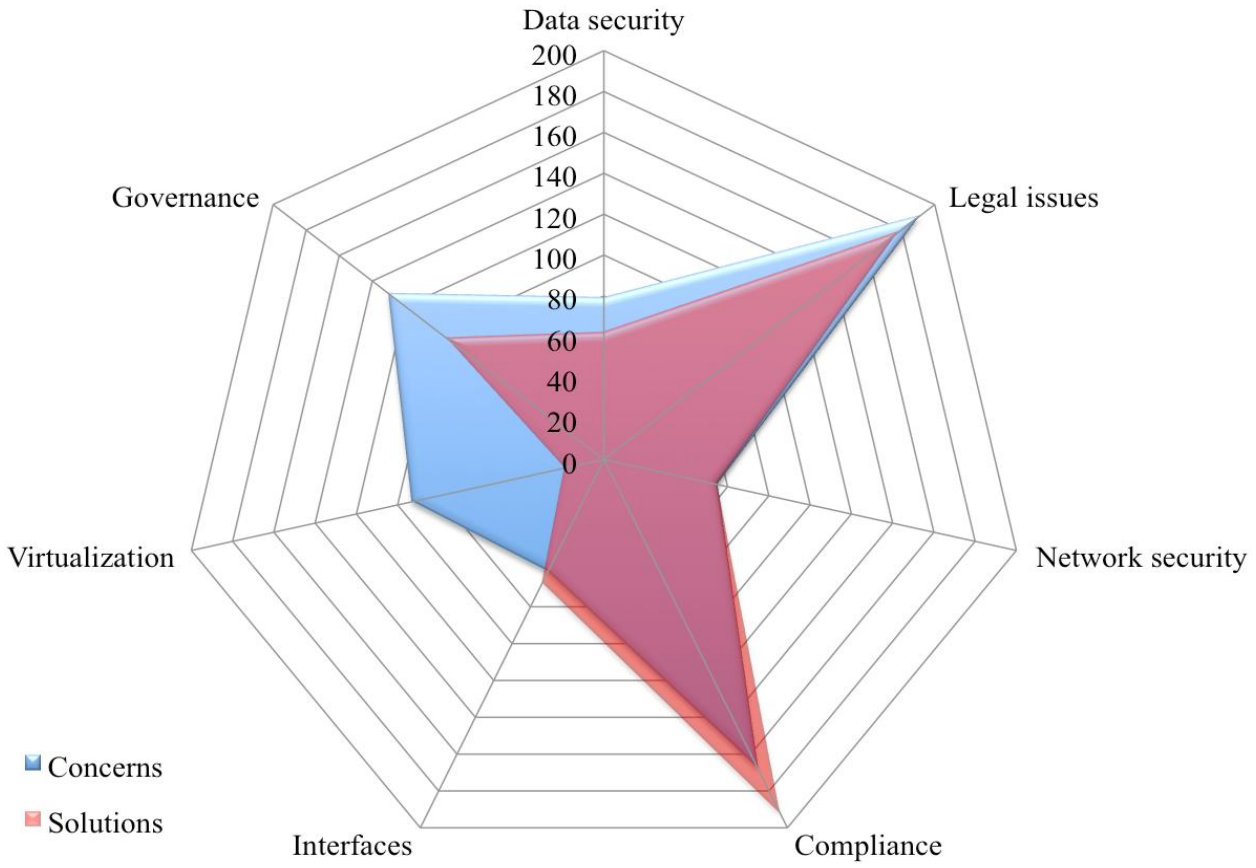

Figure 5 – Pie chart depicts the security gaps in different areas

Source: "A quantitative analysis of current security concerns and solutions for cloud computing" by Nelson Gonzalez.

The figure 5 shows that virtualization problems represent an area that requires studies for addressing issues such as isolation, data leakage and cross-VM attacks; on the other hand, areas such as compliance and network security encompass concerns for which there are already a considerable number of solutions or those are not considered highly relevant.

Considering the discussion in the previous section, a straightforward conclusion is that cloud security includes old and well researched and addressed issues such as:

1. Network and other infrastructural vulnerabilities
2. User access, authentication and privacy
3. Novel concerns derived from new technologies adopted to offer the adequate resources (mainly virtualized ones)
4. Isolation and hypervisor vulnerabilities (the main technical concerns according to the studies and graphics presented)
5. Data location and e-discovery (legal aspects)
6. Loss of governance over data
7. Security and even decision making, where the cloud must be strategically and financially considered as a decisive factor.
8. While adopting a cloud service or provider is easy, migrating to another is not.
9. After moving local data and processes to the cloud, the lack of standards for protocols and formats directly affect an attempt to migrate to a different provider, even if this is motivated by legitimate reasons such as non-fulfillment of SLAs, outages or provider bankruptcy.
10. Consequently, the first choice must be carefully made, as SLAs are not perfect and services outages happen at the same pace that resource sharing, multitenancy and scalability are not fail proof.
11. After that is made, future migrations between services can be extremely onerous in terms of time and costs; most likely, this task will require an extensive work for bringing all data and resources to a local infrastructure before redeploying to the cloud.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

Finally, the analysis of current trends for cloud computing reveals that there is a considerable number of identified security concerns, for which solutions and best practices have yet to be developed. The major impetuses in the future domain of time will be related to researching and addressing legal and administrative concerns through advances in cloud technology and practices.

VI. RESEARCH HYPOTHESIS

Following Research Hypothesis is proposed:

1. **Hypothesis 1**:- The nature of CCaaS operations induces application security breaches in cloud environment.
   This hypothesis articulates that security breaches in cloud environment are primarily due to loop holes present in the nature of business that is conducted in a CCaaS business segment.
2. **Hypothesis 2**:- The existing bi-lateral legal IT policies of governments require modifications to support building secure applications for CCaaS operations leveraging cloud environment.
   This hypothesis articulates that due to existing complex bi-lateral IT policies of different government's, leads to security breaches and these laws needs to be studied and modifications will be proposed to thwart future security breaches.
3. **Hypothesis 3**:- Legal issues and compliance requirements can be technology enabled using security measures.
   This hypothesis articulates that within the cloud environment architecture, the legal and compliance requirements can be technology enabled and regulated using security measures.
4. **Hypothesis 4**:- Solutions can be synthesized through development of a hybrid security framework for CCaaS environment addressing security issues. This hypothesis articulates the need to develop a hybrid security framework to address identified security issues.

VII. DATA COLLECTION METHODOLOGY

Primary and secondary data collection's methods are proposed as listed below:

A. Primary Data

Primary data of a Cloud environment – CCaaS business segment will be used for research investigation. Research study will use primary data by camouflaging the real time data, which is protected by Intellectual Property (IP) rights. Secondary data will be used as a support to primary data source and in any case for unavailability of primary data due to IP issues.

Cluster sampling method will be employed to collect and analyse the data. Researchers experience in IT industry will provide access to some primary data which can be quoted without source identification.

The researcher will employ the following data collection methods:

1. **Survey Method** – The researcher will design a survey, with questions related to identifying all possible root causes in cloud computing for a CCaaS business segment.
2. **Observation Method** – The researcher with vast IT industry exposure will collect primary sources of data of real time CCaaS business segment applications and will present the coded data to avoid data IP issues.

B. Secondary Data

In addition to the primary data that can be accessed, the research will be supplemented through secondary data from sources such as:

1. Open access Research papers.
2. Published White papers.
3. Web links.
4. University published online material.
5. Research monographs.
6. Published books.
7. Technical Research articles.
8. Publications in Business media and
9. Published theses.

VIII. DATA SECURITY DEVELOPMENT METHODOLOGY

CCaaS data security assessment and development steps involve seven methodical steps as outlined below:

1. Stage 1:- Gather customer view point of data security requirement – in this phase, the existing data security problem areas of the customer is elicited and the needed changeover/requirement is captured by the sales team.
2. Stage 2:- Development of data security technology alternatives – after the customer requirements are agreed, the next stage is to frame an alternative technology likely to meet the customer requirements.
3. Stage 3:- Synthesizing data security solution architecture – the objective is to integrate the various components of the data security solution architecture.
4. Stage 4:- Defining product security components – in this phase, the technical architecture for each of the product components is defined.
5. Stage 5:- System Integration – the objective is to validate how the system as a whole behaves when the all the products components are integrated.
6. Stage 6:- Testing, Deployment & Delivery – to verify and validate if the fully integrated product components are functionally tested, deployed and delivered to the customer.
7. Stage 7:- Evaluation of solution, assessment and continuous improvement – Finally, the delivered software product is solution evaluated, assessed for quality and continuous improvements steps are initiated.

IX. CONCLUSION

A straightforward conclusion is that cloud security includes old and well-known issues – such as network and other infrastructural vulnerabilities, user access, authentication and privacy – and also novel concerns derived from new technologies adopted to offer the adequate resources (mainly virtualized ones), services and auxiliary tools. These problems are summarized by isolation and hypervisor vulnerabilities (the main technical concerns according to the studies and corresponding graphics presented), data location and e-discovery (legal aspects), and loss of governance over data, security and even decision making, where the cloud must be strategically and financially considered as a decisive factor. After moving local data and processes to the cloud, the lack of standards for protocols and formats directly affect an attempt to migrate to a different provider, even if this is motivated by legitimate reasons such as non-fulfilment of SLAs, outages or provider bankruptcy. Consequently, the first choice must be carefully made, as SLAs are not perfect and services outages happen at the same pace that resource sharing, multitenancy and scalability are not fail proof. After that is made, future migrations between services can be extremely onerous in terms of time and costs; most likely, this task will require an extensive work for bringing all data and resources to a local infrastructure before redeploying to the cloud. The analysis of current trends for cloud computing reveals that there is a considerable number of well-studied security concerns, for which plenty solutions and best practices have been developed, such as those related to legal and administrative concerns. On the other hand, many issues still require further research effort, especially those related to secure virtualization.

A secure cloud computing environment depends on several security solutions working harmoniously together. However, in this research study, the authors have not identified any security solution provider owning all the facilities necessary to get high levels of security conformity for clouds. Thus, cloud providers need to orchestrate / harmonize security solutions from different places in order to achieve the desired data security level.

X. SCOPE FOR FURTHER RESEARCH

Security is a crucial aspect for providing a reliable environment and then enables the use of applications in the cloud and for moving data and business processes to virtualized infrastructures. Many of the security issues identified are observed in other computing environments as well. These include authentication, network security and legal requirements, for example, are not a novelty. However, the impact of such issues is intensified in cloud computing due to characteristics such as multitenancy and resource sharing, since actions from a single customer can affect all other users that inevitably share the same resources and interfaces. On the other hand, efficient and secure virtualization represents a new challenge in this context with high distribution of complex services and web-based applications, thus requiring more sophisticated approaches. It is strategic to develop new mechanisms that provide the required security level by isolating virtual machines and the associated resources while following best practices in terms of legal regulations and compliance to SLAs. Among other requirements, such solutions should employ virtual machine identification, provide an adequate separation of dedicated resources combined with a constant observation of shared ones, and examine any attempt of exploiting cross-VM and data leakage. A secure cloud computing environment depends on several security solutions working harmoniously together. However, in this part of the research study the authors did not identify any security solutions' provider owning all the facilities necessary to get high levels of security conformity for clouds. Thus, cloud providers need to orchestrate / harmonize security solutions from different places in order to achieve the desired security level.

REFERENCES

1. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the clouds: A Berkeley view of cloud computing, page 3-6, February 2009.
2. Cloud Security Alliance, Security guidance for critical areas of focus in cloud computing, Tech Republic, page 1-5, November 2009.

3. D. Hubbard, L.J.H.Jr, and M. Sutton, Top threats to cloud computing, Tech Republic, Page 7, March 2010.
4. D. Catteddu and G. Hogben, Benefits, risks and recommendations for information security, Tech Republic, Page 8, November 2009.
5. D. Tompkins, Security for cloud-based enterprise applications, Cloud Security Alliance, Page 3-4, March 2010.
6. E. Young, Cloud computing - the role of internal audit, Page 5, October 2009.
7. J. Pavolotsky, Top five legal issues for the cloud, Page 4, April 2010.
8. J. Oltsik, Information security, virtualization, and the journey to the cloud, Cloud Security Alliance, Page 5, August 2010.
9. NIST, Draft cloud taxonomy, Page 8, March 2011.
10. N. Anand, The legal issues around cloud computing, Page 10, April 2010.
11. S. Shankland, HP's Hurd dings cloud computing, Page 15, October 2009.
12. T. Mather and S. Kumaraswamy, Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 1st edition, October 2009.
13. Y. Chen, V. Paxson and R.H. Katz, What's new about cloud computing security? University of California, Page 15, January 2010.

BIOGRAPHY

Madhusudan KL is a management research scholar in Tumkur University, under the guidance of Dr Paramashiviah P. He is a Graduate in Engineering (IEM) from Indian Institute of Industrial Engineering (IIIE) and obtained his Master's degree in Business Administration (MBA) from Sikkim Manipal University (SMU), India. He has over 20+ years of experience in software management and development. He is working as Senior Project Manager in an MNC.

Dr Paramashiviah P is currently Dean, Chairman and Professor in Dept. of Studies & Research in Commerce, in Tumkur University since last two years. He has been awarded the Doctorate degree and has obtained Master's degree in Commerce, Master's degree in Business Administration, Master's degree in Philosophy. He has over 16 years of teaching and research experience for Courses like M.com. M.B.A., M.F.A. He has attended many national and international conferences and presented papers on various themes in Commerce & Management. He has also published books on subjects in Commerce & Management. Among few topics are Income Tax, Cost Accounting, Auditing, Banking Law and Practice, Indian Financial System etc.

Dr.N.S.Narahari is currently the Dean of Placement & Training and Professor of Industrial Engineering & Management Department at RV College of engineering Bengaluru. He is a Bachelor of Engineering in Industrial Engineering from Bangalore University and obtained his Master degree in Reliability Engineering from Indian Institute of Technology, Mumbai. He has been awarded the Doctorate degree by the Avinashilingam Deemed University in the Faculty of Engineering for his research on the topic "Application of Decision Support System for Human Resource Management Problems Using System Dynamics Approach", in the area of Computer Science & Engineering. He has got over 25 years of teaching experience. His research interests are in the fields of Industrial Ergonomics, Quality Engineering, Reliability Engineering and Industrial Engineering. He has presented and published paper at national and International conference/journals. He has been awarded Fellowship by the Indian Institution of Industrial Engineering and also been recognized with the Dr. S.R. Gollapudi award and H. K. Firodia award for his contribution to the field of Industrial Engineering. He has presented and published paper at national and International conference/journals. He has guided many projects at the undergraduate and post graduate levels. He is on the executive committee of many professional associations.