

Status review of Contact Center as a Service in India

Madhusudan KL¹, Dr. Paramashiviah P², Dr. Narahari NS³

Research Scholar, Dept. of Studies & Research in Management, Tumkur University, Tumkur, Karnataka State, India¹

Dean and Chairman, Dept. of Studies & Research in Commerce, Tumkur University, Tumkur, Karnataka State, India²

Prof, Dept. of Industrial Engineering & Management, RV College of Engineering, Bangalore, Karnataka State, India³

Abstract: This research paper mainly discusses Contact centers as a service business segment, which is currently experiencing challenges from multiple stakeholders, both internal to the company as well as externally from customers. As customer goodwill is at stake, many companies have recognized the importance and value of hosted contact center solutions. These contact center solutions enable a company to retain critical assets – their contact center staff, and the associated centers in which they work – while enriching them with world class secure contact center tools such as automatic call queuing, workforce management, automated voice responses, quality monitoring and logging, through hosted technology. The hosted contact center as part of the business hub focuses on managing customer relationships along with its technology. Today's contact centers are increasingly complex but yet they are the cornerstone of many businesses and often the first point of interaction that a customer has with the business. Having a hosted contact center allows to focus on core business strengths and providing customers with an overall fantastic customer service experience without having to worry about the mechanics that enable providing that experience. Though the potential of the contact centers is rich in terms of its ability to serve the BPO business segment, it is not bereft of the security breaches and issues. Some of the data security issues are highlighted in this paper.

Keywords: IT, Cloud Computing, CCaaS, BPO, IT Security, hacking, IVR, WFM, call queuing, CTI, HIPAA, PCI

I. INTRODUCTION

As per Wikipedia, Information Technology (IT) is “the study, design, development, application, implementation, support or management of computer based information systems”, but the term has also been applied more narrowly to describe a branch of engineering dealing with use of computers and telecommunications equipment's to store, retrieve, transmit and manipulate data.

IT systems are vital elements in most of the recent business processes. IT system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without any interruption/s.

Organizations in the public and private sectors depend on information systems to successfully carry out their business functions. Information systems can include very diverse entities ranging from office networks, financial and personnel systems to very specialized systems (e.g., telecommunications systems, industrial/process control systems, and environmental control systems).

The cloud computing being the technology base for a contact center, it is appropriate to review the cloud computing scenario.

A Synoptic view of Cloud Computing

As defined by Wikipedia, Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network, typically the Internet. The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams as seen in Figure 1.

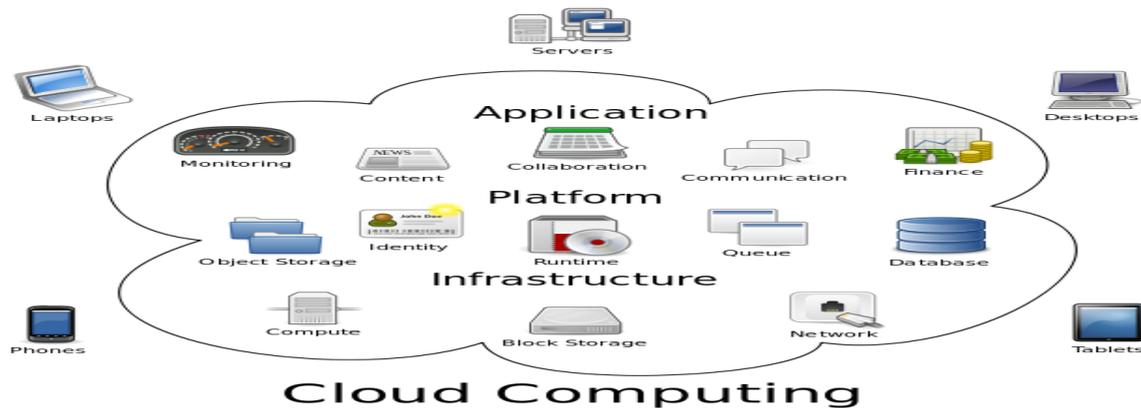


Figure 1 – Synoptic view of Cloud Computing

Cloud computing entrusts remote services with user's data, software and computation.

The cloud computing is broadly classified into three categories on the basis of delivery, which are:

1. **Software as a service (SaaS)** – Applications and products are available on demand for any internet user. For example, an online music company charges a certain amount of money for every track downloaded.
2. **Platform as a service (PaaS)** – The runtime environment is available on demand which is used by developers to deliver their applications. The framework for deployment of application code along with various on demand services is available in PaaS offerings.
3. **Infrastructure as a service (IaaS)** – Computing resources such as power, storage, networking components or middleware are available on demand. IaaS is for architects where the actual hardware infrastructure is deployed on a 'pay per use' basis.

The cloud is also broadly categorized on the basis of deployment models such as: public, private, community and hybrid clouds.

A. BPO – Introduction

As per Wikipedia, Business process outsourcing (BPO) is a subset of outsourcing that involves the contracting of the operations and responsibilities of specific business functions (or processes) to a third-party service provider. Originally, this was associated with manufacturing firms, such as Coca Cola that outsourced large segments of its supply chain. BPO is typically categorized into back office outsourcing - which includes internal business functions such as human resources, finance and accounting, and front office outsourcing - which includes customer-related services such as contact center services.

B. Business Benefits

An advantage of BPO is the way in which it helps to increase a company's flexibility. Therefore business process outsourcing enhances the flexibility of an organization in following ways.

1. Most services provided by BPO vendors are offered on a fee-for-service basis. This can help a company to become more flexible by transforming fixed into variable costs.
2. Another way in which BPO contributes to a company's flexibility is that a company is able to focus on its core competencies, without being burdened by the demands of bureaucratic restraints.
3. A third way in which BPO increases organizational flexibility is by increasing the speed of business processes.
4. Finally, flexibility is seen as a stage in the organizational life cycle.

As the current business contact centers are hosted in the cloud environment, it is necessary to have an understanding of cloud contact center as a service business segment.

C. Contact Center as a Service (CCaaS)

CCaaS or hosted contact center is a next generation, cloud-based contact center solution that allows you to minimize capital expenses and reduce operational costs. CCaaS is a global service using cloud based infrastructure and software as a service model, intended to deliver features based from the application and to the 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 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.

D. Business Benefits

CCaaS enables deployment of a ready-to-go 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.

Operating costs are reduced by the inherent cost savings 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. BACKGROUND

In the present BPO business portfolio, there is an immediate need for a high-performing contact center that delivers unparalleled responsiveness, convenience and service quality. That calls for up-to-the-minute technology — systems, hardware, software, licenses — and top-notch support services, which are reliable and highly secure from the data standpoint of view. Companies have long made huge capital outlays for these critical resources.

Limitations of the traditional contact centers are:

1. Increased decline in customer satisfaction.
2. Managements have reduced IT budgets to buy and manage infrastructure in-house.
3. There is an increase in complex technology environments.
4. Availability of IT resources is limited.
5. Traditional contact center take enormous time to deploy.
6. Need is for scalable flexibility and business agility.
7. Reduced system maintenance and management costs.
8. In secure from the business data point of view.

Today's contact centers are increasingly complex but yet they are the cornerstone of many businesses and often the first point of interaction that a customer has with the business. Having a hosted contact center allows to focus on core business strengths and providing customers with an overall fantastic customer service experience without having to worry about the mechanics that enable providing that experience.

A. Data Security

One of the primary roadblocks in considering a cloud based contact center solution is concern for data security. Cloud based solutions can seem like a panacea since they are so tight at their data centers. However, the data crosses boundaries between many places. Data security is particularly important for HIPAA (Health Insurance Portability and Accountability Act), PCI (Payment Card Interface) and other data security compliances tied to personal information, credit cards, and private data.

A second part of the data security issue is data ownership and data management. To understand where the whole data resides, who "owns" the data, and what options are available for the backup and redundancy. The intent would be to own our own data and back it up onto our own data centers routinely. And finally, what happens to the business data after the termination of the contract is an unanswered question, till today.

III. 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.

B. 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\(business\)](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.

C. 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 authors.

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. Brodtkin, 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.

IV. OBJECTIVES OF THE RESEARCH STUDY

Following is the study objectives:

1. To review basic terminology of Cloud computing technology.
2. To provide an overview of Contact center as a service, which in an essence utilizes an application online.
3. To provide a glimpse of data security issues in contact center as a service platform.
4. Finally, to research the best practices and future of the cloud computing.

V. 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 paralyze the outsourcing effort – and finally business, itself.

In Computer terminology, Security attack is any attempt to destroy, alter, disable, steal or gain unauthorized access to or make use of an asset.

D. Security Breaches in CCaaS Business Segment

A data breach is the intentional or unintentional release of secure information to an untrusted environment, including unintentional information disclosure, data leak and data spill.

Table 1.0 provides latest security breach in cloud computing environment with specific reference to BPO operations.

June, 2012	Over 1,400,000 IDs were compromised in US based public health database alone. These were linked to user social security numbers
June, 2012	Hours ahead of its planned protest against certain incidents of internet censorship in India, hacker collective anonymous attacked and brought down the website run by computer emergency response team India (CERT-I), the country’s premier agency dealing with cyber security contingencies
June, 2012	Anonymous brought down the website of MTNL in a DDoS attack
June, 2012	Over six million passwords were stolen in a hack of the professional networking site linkedin.com.
May, 2012	Protesting hackers defaced Indian political party BJP websites
May, 2012	Protesting hackers targeted social sites on RComm platform.
May, 2012	Hackers target Police, city of Chicago websites, just before NATO summit
May, 2012	Protesting hackers brought down the websites of Supreme Court of India
Jan, 2013	The Daily Mail reports that call center workers in India have been selling confidential information of UK residents.

Table 1.0 – Latest Security attacks and its description

VI. CCAAS DEVELOPMENT STEPS

CCaaS development steps involve seven methodical steps as outlined below:

1. Stage 1:- Gather customer requirement – in this phase, the existing problem areas of the customer is elicited and the needed changeover/requirement is captured by the sales team.
2. Stage 2:- Development of 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 solution architecture – the objective is to integrate the various components of the solution architecture.
4. Stage 4:- Defining product 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.

VII. CONCLUSION

Cloud data security is a crucial aspect for providing a reliable environment, which enables the use of applications in the cloud and for moving data and business processes to virtualized infrastructures. However, the impact of issues such as authentication, network security and legal requirements 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 understand intricacies of data security and 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 Service Level Agreements (SLA’S).

VIII. SCOPE FOR FURTHER RESEARCH

The main scope of this research study is to address data security attacks/breaches related to CCaaS technology. Research study will further evaluate and propose a model to simulate all possible attacks/hacks and its prevention methods.

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.