*International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137*

*Volume – 03, Issue – 04, April 2018, PP – 99-102*

# Security issues concerned to Cloud deployment in Insurance sector

**S. Balaji[1], Vidyarthini. A[2],**

[1](Research department of Computer Science, Dhanraj Baid Jain College(Autonomous), India)

[2](Research department of Computer Science, Dhanraj Baid Jain College(Autonomous), India)

**Abstract:** Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud. Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose.This article aims to give understanding of cloud technology and its deployment in insurance sector.This article also considers security issues and model for the deployment of cloud.

## I. Introduction

Cloud computing has transformed many industry sectors with its ease of deployment, resourcefulness, and flexibility, and the insurance industry is no different. The number of people working in the industry has grown over the years and, accordingly, so has their way of doing business. As the industry is expected to grow their IT spend by an annual compound rate of 3% by 2020, it's clear that cloud computing will be an essential component in that mix.

Cloud computing is increasingly being adapted by a wide range of users starting from commercial entities to consumers. A survey by Right Scale1 found that an average user runs at least four cloud-based applications and at any point in time is evaluating another four. The survey also found that 41% of commercial entities run significant workload on public clouds. With so much of our workload moving to cloud, security in cloud computing is under increased scrutiny. This assessment is also supported by the 2017 report by Forbes2, which says that in 15 months, while 80% of all IT budgets will be committed to cloud solution, 49% of the businesses are delaying cloud deployment due to security skills gap and concerns. The problem appears to be multi-dimensional, with lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few. Adaption of cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to cloud from not just average Internet users, but also from most if not all commercial entities.

## II. Literature Support

During 2008, the IT consultancy – Gartner identified seven security issues which should be addressed before enterprises consider switching to the cloud computing model. They are as follows: (1) privileged user access – data transmitted from the client through the Internet represents a specific level of hazard because of issues of data proprietorship; enterprises should spend time getting acquainted with theirproviders and their regulations as much as possible before assigning some inconsequential applications first to test the water, (2) regulatory compliance - clients are responsible for the security of their solution, as they can choose between providers that permit to be reviewed by third party organizations that check levels of security and providers that don't (3) data location - relying upon contracts, a fewclients may never comprehend what nation or what locale their information is found (4) data segregation - encoded data from various organizations may be stored on the same hard disk, so a mechanism to separate data ought to be conveyed by the service provider. (5) recovery - every cloud service provider ought to have a disaster recovery system to store userprovider, it might not have numerous lawful ways pursue an enquiry, (7) long-term feasibility - refers to the ability to withdraw an agreement and all information if the present provider is bought out by another firm [1].

ENISA explored the distinctive security risks related to adopting cloud computing along with theaffected resources, the risks probability, effects, and vulnerabilities in the cloud computing may lead to such risks [2]. Balachandra et al, (2009) discussed the security Service Level Agreement's requirement and objectives related to data locations, isolation and data recovery [3]. Kresimir et al, (2010)discussed high level security concerns in the cloud computing model such as information trustworthiness, payment, and protection of

  

sensitive information [4]. Bernd et al, (2010) discuss the security vulnerabilities existing in the cloud platform. The authors gathered the conceivable vulnerabilities into innovation related, cloud qualities related, security controls related [5]. Subashini et al discuss thesecurity difficulties of the cloud service delivery model, concentrating on the SaaS model [6]. Ragovind et al, (2010) discussed the administration of security in Cloud computing concentrating on Gartner's list of cloud security issues and the discoveries from the International Data Corporation enterprise [7].

Morsy et al, (2010) investigated cloud computing issues from the cloud design, cloud offered qualities, cloud partners, and cloud service delivery models perspectives [8].

## III. Cloud Deployment

The level of standardization that the consumer of a cloud service has to deal with is much lower with theInfrastructure as a Service (IaaS) model than with the higher models. For example, the consumer ofSoftware as a Service (SaaS) has very little control over the business processes and functionality offered,the enabling platform, or the infrastructure on which the service is hosted. But at the same time, the cost advantage of services goes up with the increasing level of the models to the point where the advantage is highest for the cloud services model. The cloud services model provides the unique services needed to truly disrupt business models and bring out the true value of cloud computing to enterprises. In other words, cloud is a true enabler of innovation.The shift to customer-facing applications In addition to providing direct access to tools to in-housedecision makers, sales teams and call center staff, many organizations are finding ways to cut costs andimprove service delivery by deploying self-serve tools that customers can navigate on their own. Cloudcomes in handy in accomplishing the same.


Fig 3.1. Above figure illustrates the Portfolio of Line of Business Applications in Insurance IT.

**The Factors that drive insurance sector for the cloud adoption across the different Line of business applications are as follows –**

1) Need for innovative applications which increases customer intimacy & friendliness
2) Need to move away from highly paper driven processes & eliminate errors
3) Growing number of users per application
4) Automating and optimizing business processes
5) Integration imperatives due to mergers & Acquisitions and the technology costs associated withthe integration process
6) Increasing transaction volumes / Sheer volume of data
7) Growing demand for real-time access to information

The parameters that will decide what applications may be moved to the cloud and when can bebroadly classified into three groups:Maturity of Cloud Computing: This is a function of robustness, reliability, and cost effectiveness ofthe services available.Business Criticality: The business criticality of an application is a function of various factors, such aswhat business functions are enabled, impact of standardization of the business processes involvedon competitive advantage, revenue impact, influence on customer experience, and competitiveadvantage.Insurers' Willingness: The third and most critical piece of the puzzle is the risk that insurers arewilling to take to put their systems onto a cloud environment. Based on the combination of the first two factors, insurers are likely to calculate the risk of migration and adopt cloud computing in an incremental manner.8) Need & ability to do business with a larger set of partners.

  

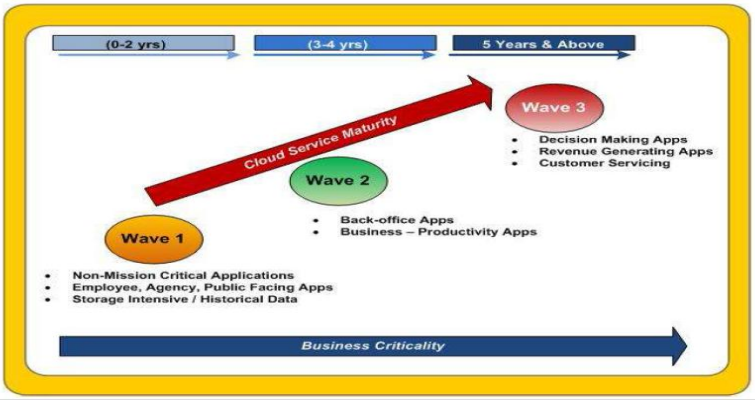


Fig 3.2 Incremental levels for cloud adoption

## IV. Methodology for security in cloud environment

The level of standardization that the consumer of a cloud service has to deal with is much lower with the Infrastructure as a Service (IaaS) model than with the higher models. For example, the consumer of Software as a Service (SaaS) has very little control over the business processes and functionality offered, the enabling platform, or the infrastructure on which the service is hosted. But at the same time, the cost advantage of services goes up with the increasing level of the models to the point where the advantage is highest for the cloud services model. The cloud services model provides the unique services needed to truly disrupt business models and bring out the true value of cloud computing to enterprises. In other words, cloud is a true enabler of innovation.

In fact, cloud computing is not the only trend they are embracing. Their information security had to be strengthened due to the growing amount of data they collect as well as the widespread adoption of bring your own device (BYOD) policies.

Each cloud service provider and cloudconsumer have to devise countermeasures and controls to mitigate the risks based on their assessment.

However, the following are some of the best practices in countermeasures and controls that can be considered:

a. End-to-end encryption – the data in a cloud delivery model might traverse through manygeographical locations; it is imperative to encrypt the data end-to-end.
b. Scanning for malicious activities – end-to-end encryption while highly recommended, induces newrisks, as encrypted data cannot be read by the Firewall or IDS. Therefore, it is important to haveappropriate controls and countermeasures to mitigate risks from malicious software passing throughencryption.
c. Validation of cloud consumer – the cloud provider has to take adequate precautions to screen thecloud consumer to prevent important features of cloud being used for malicious attack purposes.
d. Secure Interfaces and APIs – the interfaces and APIs are important to implement automation, orchestration, and management. The cloud provider has to ensure that any vulnerability is mitigated.
e. Insider attacks – cloud providers should take precaution to screening employee and contractors,along with strengthening internal security systems to prevent any insider attacks.
f. Secure leveraged resources – in a shared/multi-tenancy model, the cloud provider has secure sharedresources such as hypervisor, orchestration, and monitoring tools.
g. Business Continuity plans – Business continuity plan is a process of documenting the response ofthe organization to any incidents that cause unavailability of whole or part of a business-criticalprocess.

To avoid access of data from other users, applying encryption on data that makes data totally unusable and normal encryption can complicate availability. Before uploading data into the cloud, the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged. Calculate the hash of the file before uploading to cloud servers will ensure that the data is not altered. This hash calculation can be used for data integrity but it is very difficult to maintain it. RSA based data integrity check can be provided by combining identity-based cryptography and RSA Signature. SaaS ensures that there must be clear boundaries both at the physical level and application level to segregate data from different users. Distributed access control architecture can be used for access management in cloud computing. To identify unauthorized users, using of credential or attributed based policies are better. Permission as a service can be used to tell the user that which part of data can be accessed.

  

Fine grained access control mechanism enables the owner to delegate most of computation intensive tasks to cloud servers without disclosing the data contents. A data driven framework can be designed for secure data processingand sharing between cloud users. Network based intrusion prevention system is used to detect threats in real-time.

To compute large files with different sizes and to address remote data security RSA based storage security methodcan be used.

## V. Conclusion

Security is bound to be a concern in an industry where money plays a key role. It goes without saying that people working in the insurance sector are not necessarily technology experts. . This is a huge gain for insurance companies as they never have to worry about storage, up gradation, maintenance or the security of their IT infrastructure.To provide a secure data access in cloud, advanced encryption techniques can be used for storing and retrieving data from cloud. Also, proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data.

## References

[1]. Brodkin, J. (2008). Gartner: Seven cloudcomputing security risks. Infoworld, 2008, 1-3.
[2]. European Network and Information Security Agency. (2009). Cloud Computing:
[3]. Benefits, risks and recommendations for information security. ENISA.
[4]. Kandukuri, B. R., &Rakshit, A. (2009,September). Cloud security issues. In Services
[5]. Computing, 2009. SCC'09. IEEE International Conference on (pp. 517-520). IEEE.
[6]. Kresimir, P. and Zeljko, H. (2010). Cloud computing security issues and challenges. PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349.
[7]. Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing
[8]. vulnerabilities. IEEE Security & Privacy, 9(2), 50-57.
[9]. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
[10]. Ramgovind, S., Eloff, M. M., & Smith, E.(2010, August). The management of security in cloud computing. In 2010 Information Security for South Africa (pp. 1-7). IEEE.
[11]. Almorsy, M., Grundy, J., & Müller, I.(2010, November). An analysis of the cloud computing security problem. In Proceedings of APSEC 2010 Cloud Workshop, Sydney,Australia, 30th Nov.
[12]. State of the Cloud Report. (2017). https://www.rightscale.com/lp/state-of-the-cloud (Retrieved 25 May 2017)
[13]. State of Cloud Adoption And Security. (2017). https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoptionand-security/ (Retrieved 25 May 2017).
[14]. Abhuday Tripathi, Parul Yadav, "Enhancing Security of Cloud Computing using Elliptic Curve Cryptography", International Journal of Computer Applications (0975 – 8887), Volume 57– No.1, November 2012
[15]. Nagesh M.Wankhade, Kiran A. Sahare, Prof. Vaishali G. Bhujade, "SECURE CLOUD SIMULATION USING TRIPLE DES ", International Journal of Research in Advent Technology, Volume 2, Issue 1, January 2014
[16]. S.Sathish, D.Sumathi, P.Sivaprakash, " Security Services using ECDSA in Cloud Computing", Volume 4, Issue 5, May 2014
[17]. Martin Leslie. Elliptic curve cryptography. (An ECC research project), 2006.
[18]. Padma Bh, D.Chandravathi , P.PrapoornaRoja, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz‟s Method ", International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1904-1907
[19]. VeerrajuGampala, SrilakshmiInuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-3, July 2012.
[20]. S. Subashini and V. Kavitha. (2010) "A Survey on Security issues in Service Delivery Models of cloud computing" Journal of Network and Computer Applications (JNCA), Vol. 34, No. 1, Jul, 2010.
[21]. Chang-Lung Tsai and Uei-Chin Li, "Information Security of Cloud Computing for Enterprises", Advances on Information Sciences and Service Sciences. (AISSS), Vol. 3, No. 1, pp. 132-142, Feb 2011.

  