ISSN:2231-0711
www.ijcset.net

DATA SECURITY IN CLOUD: A PROPOSAL TOWARDS THE SECURITY ISSUES

Dayanand Sagar Kukkala[#1], V.P. Krishna Anne[*2], Rajasekhara Rao Kurra[#3]
Department of Computer Science and Engineering, KL University,
Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India
[1]dayanandsagar@gmail.com
[3]krr_it@yahoo.co.in
[2]krishnavpraveen@gmail.com

***Abstract*: - Cloud computing is one of the today's most arising and needed technology and became popular for its flexibility, sharing resources, ease of maintenance, cost-efficiency etc., In very recent times, the cloud computing technology will have all its implementation in all ICT commodities and it became procurement model. In this paper, we characterize the problems in controlling the data and throw a keen limelight on the information security and various models that are proposed. Many existing research thrusts/systems has their own importance and same time drawbacks on maintaining the data security in cloud. The paper deals with much research advances in the area of data security concerns as information - centric security architecture over the cloud. The architecture deals for trusted computing, computation support encryption, advantageous of security over the cloud, which can be most benefitable in the vast area of Business Intelligence.**

***Keywords*—Security, Information, Cloud Computing, Environment, Security Architecture**

I. INTRODUCTION

This environment strives to be dynamic, reliable, and customizable with a guaranteed quality of service. Within this system, users have a myriad of virtual resources for their computing needs, and they don't need a complete understanding of the infrastructure. Cloud computing advent has made the declaration by Scott Mc-Nealy, Sun Microsystems' founder that "The network is the computer" a reality and given the old Sun marketing motto a new life. In this new world of computing, users are universally required to accept the underlying premise of trust. In fact, some have conjectured that trust is the biggest concern facing cloud computing. Now here is the element of trust more apparent than in security, and many believed trust and security to be synonymous. In this paper, we are going to examine some security issues and the associated regulatory and legal concerns that have arisen as cloud computing emerges as a primary distributed computing platform. Also we propose architecture to overcome those security issues.

The term "cloud" originates from the telecommunications world of the 1990s, when providers began using virtual private network (VPN) services for data communication. VPNs maintained the same bandwidth as fixed networks with considerably less cost: these networks supported dynamic routing, which allowed for a balanced utilization across the network and an increase in bandwidth efficiency, and led to the coining of the term "telecom cloud." Cloud computing premise is very similar in that it provides a virtual computing environment that's dynamically allocated to meet user needs [1].

From a technical perspective, cloud computing includes service oriented architecture (SOA) and virtual applications of both hardware and software. Within this environment, it provides a scalable services delivery platform. Cloud Computing shares its resources among a cloud of service consumers, partners, and vendors. By sharing resources at various levels, this platform offers various services, such as an *infrastructure cloud* (for example, hardware or IT infrastructure management), a *software cloud* (such as software, middleware, or traditional customer relationship management as a service), an *application cloud* (application, UML modeling tools, or social networks as a service), and a *business cloud* (for instance, business processes as a service) (see www.thecloudcomputing.org/2009/2/). Cloud computing itself is a field within s*ervice computing*, a cross-discipline that bridges the gap between business and IT services. This discipline aims to enable IT services and computing technology to perform business services more efficiently and effectively. In this paper, we discuss about various security concerns over cloud computing environment and proposed Information-centric security architecture to overcome these security concerns [4]. Today, the latest example of cloud computing is Web 2.0; Google, Yahoo, Microsoft, and other service providers now offer browser-based enterprise service applications (such as webmail and remote data backup).

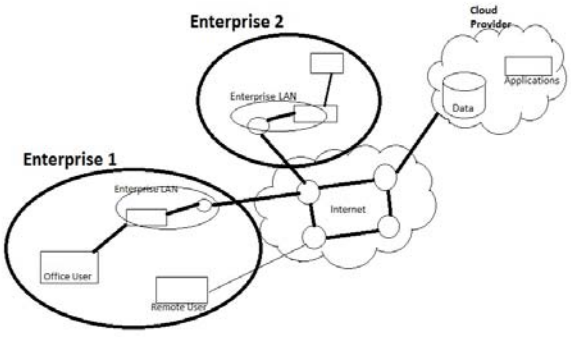

Fig.1 Cloud computing Model

Now that cloud computing has emerged as a viable and readily available platform, many users from disparate backgrounds (for example, financial institutions, educators, or cybercriminals) are sharing virtual machines to perform their daily activities. This environment requires an implicit level of trust as well as an explicit level of vigilance to ensure success.

II. RESPONSIBILITY AND SECURITY ISSUES

Within the cloud computing world, the virtual environment lets user's access computing power that exceeds that contained within their own physical worlds. To enter this virtual environment, requires neither the exact location of their data nor the other sources of the data collectively stored with theirs. To ensure data *confidentiality*, *integrity*, and *availability* (CIA), the storage provider must offer capabilities that, at a minimum, include

• Encryption schema to ensure that the shared storage environment safeguards all data;
• Stringent access controls to prevent unauthorized access to the data; and
• Scheduled data backup and safe storage of the backup media.

To overcome these and other concerns, we must develop a security model that promotes CIA. This model could enable each cloud to offer a measure of it's to date and projected CIA, but the obvious difficulty is that obtaining security data is difficult, if not impossible. This problem has existed since computing's advent due to financial, business, and national security concerns. It might be exacerbated in cloud computing because the need to provide data confidentiality can also impact incident reporting.
Taxonomy of the "security" concerns:

- Conventional security
- Availability
- Third-party data control

A. *Conventional Security*

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company.
Concerns in this category include:

- TS1. VM-level attacks. Potential vulnerabilities in the hypervisor or VM technology used by cloud vendors are a potential problem in multi-tenant architectures.
- Cloud provider vulnerabilities. These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability in salesforce.com.
- TS2. Expanded network attack surface. The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases.
- TS3. Authentication and Authorization. The enterprise authentication and authorization framework does not naturally extend into the cloud. How does a company meld its existing framework to include cloud resources? Furthermore, how does an enterprise merge cloud security data (if even available) with its own security metrics and policies?

B. *Availability:*

These concerns center on critical applications and data being available.

- A1. Uptime. As with the Traditional Security concerns, cloud providers argue that their server uptime compares well with the availability of the cloud user's own data centers. Besides just services and applications being down, this includes the concern that a third-party cloud would not scale well enough to handle certain applications.
- A2. Single point of failure. Cloud services are thought of as providing more availability, but perhaps not – there are more single points of failure and attack.
- A3. Assurance of computational integrity. Can an enterprise be assured that a cloud provider is faithfully running a hosted application and giving valid results? For example, Stanford's Folding@Home project gives the same task to multiple clients to reach a consensus on the correct result.

C. *Third-party data control*

The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality regulatory compliance requires transparency into the cloud.

- BL1. Due diligence. If served a subpoena or other legal action, can a cloud user compel the cloud provider to respond in the required time-frame? A related question is the provability of deletion, relevant to an enterprise's retention policy: How can a cloud user be guaranteed that data has been deleted by the cloud provider?
- BL2. Audit ability. Audit difficulty is another side effect of the lack of control in the cloud. Is there sufficient transparency in the operations of the cloud provider for auditing purposes? Currently, this transparency is provided by documentation and manual audits. Information Security Magazine asks: "*How do you perform an on-site audit when you have a distributed and dynamic multi-tenant*

computing environment spread all over the globe? It may be very difficult to satisfy auditors that your data is properly isolated and cannot be viewed by other customers."

- BL3. Contractual obligations. One problem with using another company's infrastructure besides the uncertain alignment of interests is that there might be surprising legal implications. For instance, here is a passage from Amazon's terms of use[1]:
  10.4. Non-Assertion. During and after the term of the Agreement, with respect to any of the Services that you elect to use, you will not assert, nor will you authorize, assist, or encourage any third party to assert, against us or any of our customers, end users, vendors, business partners (including third party sellers on websites operated by or on behalf of us), licensors, sublicensees or transferees, any patent infringement or other intellectual property infringement claim with respect to such Services.
- BL4. Cloud Provider Espionage. This is the worry of theft of company proprietary information by the cloud provider. For example, Google Gmail and Google Apps are examples of services supported by a private cloud infrastructure. Corporate users of these services are concerned about confidentiality and availability of their data. According to a CNN article [1]:

  For Shoukry Tiab, the vice president of IT at Jenny Craig, which uses Postini and Google Maps, the primary concern is security and confidentiality. "Am I nervous to host corporate information on someone else's server? Yes, even if it's Google."

III. PRESENT PROBLEMS

In this section we outline new problem areas in security that arise from cloud computing.

A. *Cheap data and data analysis.*

The rise of cloud computing has created enormous data sets that can be monetized by applications such as advertising. Google, for instance, leverages its cloud infrastructure to collect and analyze consumer data for its advertising network. Collection and analysis of data is now possible cheaply, even for companies lacking Google's resources. What is the impact on privacy of abundant data and cheap data-mining? Because of the cloud, attackers potentially have massive, centralized databases available for analysis and also the raw computing power to mine these databases. For example, Google is essentially doing cheap data mining when it returns search results. How much more privacy did one have before one could be goggled?

B. *Cost-effective defense of availability*

Availability also needs to be considered in the context of an adversary whose goals are simply to sabotage activities. Increasingly, such adversaries are becoming realistic as political conflict is taken onto the web, and as the recent cyber attacks on Lithuania confirm. The damages are not only related to the losses of productivity, but extend to losses due to the degraded trust in the infrastructure, and potentially costly backup measures. The cloud computing model encourages single points of failure. It is therefore important to develop methods for sustained availability (in the context of attack), and for recovery from attack. The latter could operate on the basis of minimization of losses, required service levels, or similar measures.

C. *Increased authentication demands*

The development of cloud computing may, in the extreme, allow the use of thin clients on the client side. Rather than a license purchased and software installation on the client side, users will authenticate in order to be able to use a cloud application. There are some advantages in such a model, such as making software piracy more difficult and giving the ability to centralize monitoring. It also may help prevent the spread of sensitive data on untrustworthy clients.

IV.PROPOSED SYSTEM

The proposed system is Developing Information centric security framework for cloud computing to minimize all these problems. Think In Terms of Security Architecture, Not Security Products.

The problem with tactical security products is that they address discrete threats and finite amounts of data in a series of solution silos. Enterprises can continue to add individual confidential security silos for added protection, but this model can quickly become a costly operations nightmare and can't offer the security benefits of an integrated, layered defense [2]. To keep up with sophisticated threats and avalanche of data growth, large organizations need to address confidential data security with a more horizontal, architectural approach. ESG believes that this will ultimately create Information-centric security architecture. Rather than a series of vertical security tools, the Information-centric security architecture is made up of bottom-up of 4 horizontal services (see Figure 2).

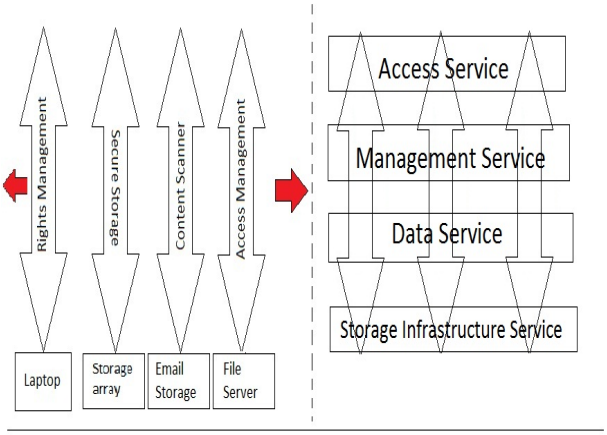

Fig.2 Information-Centric Security Alternatives

1. Storage infrastructure services
2. Data services
3. Management services
4. Access services

Each architectural layer provides services for specific protection across multiple data repositories like storage arrays, file systems, emails and content management archives. The layers work in concert; enabling data access, policy enforcement, and management oversight that can be tailored to business processes across the enterprise (see Fig 3).

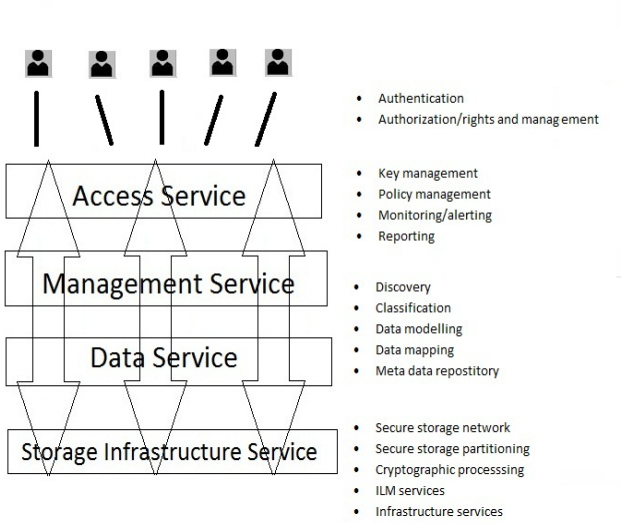

Fig.3 Information-Centric Security Architecture

A. *Storage Infrastructure Services*

Since storage devices such as hard disk drives, tape libraries, and storage arrays ultimately house all the data, the information-centric security architecture starts with this physical tier. The objective is to add security protection to the existing storage infrastructure with capabilities such as:

- **Secure storage networking and partitioning.** The storage layer should support features for secure storage networking like trusted relationships between devices, secure Fibre Channel switch zoning, and LUN masking. Progress here depends upon the creation and implementation of standards such as the Fiber Channel Security Protocol (FC-SP), ANSI T10 and T11, IEEE p1691, and the Trusted Computing Group's storage specification.

- **Cryptographic processing.** Over the next few years, more and more cryptographic processing will migrate from software and appliances to dedicated co-processors on storage devices. Indeed, this is already happening with a growing sub-set of laptop hard drives and tape drives. As on-board cryptographic processors become more ubiquitous, encryption will become a core storage security service in the information-centric security architecture.

- **Information lifecycle management functionality**. Storage software functionality such as automated archiving, data consolidation and tiering must merge with security protection for encryption, key management and auditing. The storage security services tier will be built with secure open interfaces to enable secure ILM.

B. *Data Management Services*

Information security is an information management problem. You can't secure what you don't manage, and you can't manage what you don't know exists. Data management inventory and tag sensitive data, and make this intelligence available to other layers in the stack to enable policy enforcement. These key services include:

- **Data discovery and classification**. Data and infrastructure sprawl has created islands of information across the organization that would-be stewards may not even know exist. Discovery tools must auto-discover repositories and shares of information, and classify this information automatically based on file metadata, predefined patterns, or advanced semantic analysis.
- **Data modeling.** Once the data is discovered and classified relationships between data elements must be modeled to define the right access and usage rights needed for business processes. While complex, this exercise can help enable business collaboration while simultaneously identifying areas of significant risk.
- **Meta data tagging.** Data classification must be enabled through standard Meta data tagging of all data elements. These tags travel with the data and tell technology devices what actions need to be taken. For example, the payroll file can be tagged as confidential specifying who can see it and what actions they can take. When a malicious HR administrator tries to copy the file to a flash drive, email it to a headhunter or export the data to an Access Database, she will be foiled in all cases by intelligent infrastructure acting on the encapsulated Meta data. This type of policy enforcement will only work when storage devices can enforce policies based upon specific instructions contained in the Meta data tags.
- **Data mapping.** To keep up with activities, the management layer will know where confidential data is, when it changes, and where it moves to. This information will likely be stored in a database but will be supported by strong visualization and analysis tools. When the Chief Privacy Officer wants to see where data flows, she will be able to

get real-time and historical maps to review to look for policy and technology vulnerabilities.

C. Management Services

The management services tier provides shared services for instituting, monitoring, and enforcing security and privacy policies. These services are centralized in order to provide scale, improve security, and streamline operations. Information-centric security needs will vary across data sets, business processes, and functional IT teams. To accommodate these diverse needs management services must provide published APIs for integration with many types of individual applications. Furthermore, management services must support role-based access control to ensure that users are limited to functionality needed for their job responsibilities and nothing more. Management services include:

- **Policy management.** The goal here is implement once, enforce broadly. In other words, the information-centric security architecture centralizes policy creation and changes. Once established, technology widgets throughout the enterprise are provided with policy enforcement rules. When Acme Co. decides to buy XYZ Inc., it sets up a policy that covers all data (i.e. emails, documents, database objects, etc.) related to the due diligence process. This action triggers specific data management and security policies that are enforced across the architecture: Document storage will be limited to specific repositories with restricted access to a cross-functional group of employees and external constituents. All data will be encrypted at rest and in flight, and accessing documents will require two-factor authentication.
- **Key management.** It is likely that actual cryptographic processing will be take place on storage devices, databases, file systems, laptops, and appliances. This is a good model as it maximizes performance and allows for scale over time. That said however, enterprise organizations will want to centralize key management. Why? Keys need to be closely guarded and administered or data gets lost, stolen, or rendered unreadable. Centralized key management must provide high availability, role-based access controls, strong data management, and detailed auditing.
- **Auditing and reporting.** Each services layer will provide health and status data for analysis. This data will be accessible as a management services for analysis, reporting, and auditing customized for different roles and needs, including proof of regulatory compliance.

D. Access Services

This layer is centered on who gets the right to use data and what they allowed to do with it once they gain access. Services include:

- **Authentication.** Whether a knowledge worker wants a document or a storage administrator needs access to a Fibre Channel switch, everyone will authenticate through a central service. This will help map users, roles, and groups to specific activities while providing an audit trail.
- **Fine-grained authorization.** When users gain access to devices, networks, or data repositories someone still has to define what they can see and do. In the information centric security architecture, this authorization moves from individual applications to become a shared service. Actual policy enforcement is communicated from the policy management service to the authorization service and then to technology elements for enforcement.

The Information-Centric Security Architecture

By layering these services, the information-centric security architecture can monitor and enforce security/privacy policies AND enable collaborative business processes. Geographically dispersed individuals with no organizational ties to each other can securely share documents on an ad hoc basis. These documents carry rules with them so that each technology element can enforce policies while logs capture activities and violations. Process automation and service integration allows organizations to respond as business or security needs change over time.

Figure 4 below presents an example of how information-centric security architecture can enable a specific business process for a pharmaceutical company [2]. To formulate a new drug, the chief scientist of a major pharmaceutical company hires a university professor as a part-time consultant. Even though the professor is not an employee, he is given access to extremely confidential documents for review. Since these documents have been tagged as “top secret,” they are stored and transmitted in Cipher text. The remote professor can only access these documents by authenticating using multi-factor authentication and while the Chief Scientist can save these documents and view them on a home computer, the professor is granted read-only access. When the professors consulting project ends after 30 days he can no longer view the encrypted file (see Figure 4).

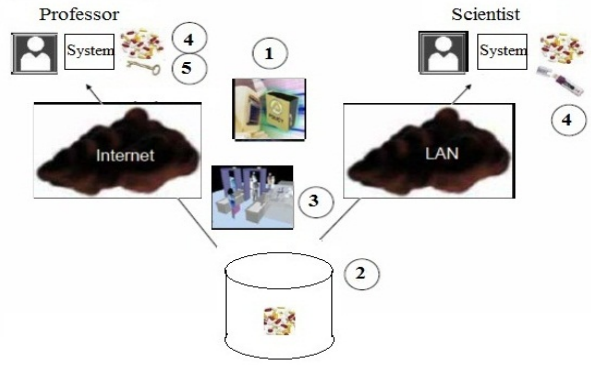

Fig.4 The Information-Centric Security Architecture

1. The policy created for access/usage rules for "Top Secret" documents.
2. Document is classified as "Top Secret" and tagged accordingly
3. University professor hired as consultant and given access to "Top Secret" document
4. An encrypted copy is sent to the professor with authorization rules. Professor can only read the document while the chief scientist is allowed to save it to a flash drive.
5. After 30 days, the professor's local encryption key is destroyed and he can no longer access the file.

V.CONCLUSION

Cloud Computing is one of the most popular scenario for today IC technologies. But cloud Computing fears largely in the aspect of loss of control of sensitive and worthy data. Present preventive measures do not adequately address cloud computing's data storage and processing needs. So, we discussed in this paper on the various security concerns and proposed architecture to overcome them. We conclude the paper; the measures proposed on information security are up to the mark and make greater reliance of cloud computing in all business intelligence aspects.

ACKNOWLEDGEMENT

We are greatly delighted to place my most profound appreciation to Er.K.Satyanarayana Chancellor of K.L.University,Dr.K.RajasekharaRao,Principal,Prof.S.Venkateswaralu Head of the department, Dr.Subramanyam in-charge for M.Tech and Mr.A.V.Praveen Krishna under their guidance and encouragement and kindness in giving us the opportunity to carry out the paper. I also extend my deep regards to my friends M.V.Sumanth, K.Parvathi Devi and Ch.Sudheesha who helped me in doing this paper. Their pleasure nature, directions, concerns towards us and their readiness to share ideas enthused us and rejuvenated our efforts towards our goal. We also thank the anonymous references of this paper for their valuable comments.

REFERENCES

[1] Richard Chow, Philippe Golle, et.al . "*Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control*" In preceedings of ACM '09 workshop on Cloud computing security November 13, 2009, Chicago, Illinois, USA.

[2] Jon Oltsik," *The Information- Centric Security Architecture*" by Enterprise Strategy Group, July 2009.

[3] Narayanan, A. and Shmatikov, V." *Robust De-anonymization of Large Sparse Datasets*". In IEEE Symposium on Security and Privacy. IEEE Computer Society, 2008.

[4] Salesforce.com Warns Customers of Phishing Scam. http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html.

[5] Shi, E. Bethencourt, J., Chan, H., Song, D., and Perrig, "*A. Multi-Dimensional Range Query over Encrypted Data*". In IEEE Symposium on Security and Privacy. 2007.

[6] Google Docs Glitch Exposes Private Files. http://www.pcworld.com/article/160927/google_docs_glitch_exposes_private_files.htm

[7] End-User Privacy in Human–Computer Interaction. http://www.cs.cmu.edu/~jasonh/publications/fnt-end-user-privacy-in-human-computer-interaction-final.pdf.

[8] Song, D., Wagner, D., and Perrig, A. Practical Techniques for Searches on Encrypted Data. In IEEE Symposium on Research in Security and Privacy. 2000.

[9] ESG White Paper, The Information-Centric Security Architecture. http://japan.emc.com/collateral/analyst-reports/emc-white-paper-v4-4-21-2006.pdf.

[10] Lithuania Weathers Cyber Attack, Braces for Round.http://blog.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html.

[11] Armbrust, M., Fox, A., Griffith, R. et al. Above the Clouds: A Berkeley View of Cloud Computing. UCB/EECS-2009-28, EECS Department, University of California, Berkeley, 2009.

[12] Boneh, B., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. Public Key Encryption with Keyword Search. In EUROCRYPT. 2004.