Achieving Data Security with the Cloud Computing Adoption Framework

Prof. Kasat P.R.[1], Prof. Shaikh S.I[2]., Prof. Sarda Aditya Subhashchandraji[3], Prof. Chavan D.D.[4], Prof. Khan S.R.[5], Prof. Bhillare P.B.[6]

[1] Lecturer, Computer Science And Engineering, Mitthulalji Sarda Polytecnic Beed, Maharashtra, India
[2]Head Of Department, Computer Science And Engineering, Mitthulalji Sarda Polytecnic Beed, Maharashtra, India

[3] Assistant Professor, Computer Science And Engineering, Aditya Engineering College Beed, Maharashtra, India

[4]Head Of Department, Information Technology, Aditya Polytechnic Beed, Maharashtra, India

[5]Lecturer, Computer Science And Engineering, Aditya Polytechnic Beed, Maharashtra, India

[6] Head Of Department, Computer Science And Engineering, Aditya Polytechnic Beed, Maharashtra, India

ABSTRACT

Offering real-time data security for petabytes of data is important for cloud computing. A recent survey on cloud security states that the security of users' data has the highest priority as well as concern. We believe this can only be able to achieve with an approach that is systematic, adoptable and well-structured. Therefore, this paper has developed a framework known as Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. This paper explains the overview,rationale and components in the CCAF to protect data security. CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. Since our Data Center has 10 petabytes of data, there is a huge task to provide real-time protection and quarantine. We use Business Process Modeling Notation (BPMN) to simulate how data is in use. The use of BPMN simulation allows us to evaluate the chosen security performances before actual implementation. Results show that the time to take control of security breach can take between 50 and 125 hours. This means that additional security is required to ensure all data is well-protected in the crucial 125 hours. This paper has also demonstrated that CCAF multi-layered security can protect data in real-time and it has three layers of security: 1) firewall and access control; 2) identity management and intrusion prevention and 3) convergent encryption. To validate CCAF, this paper has undertaken two sets of ethical-hacking experiments involved with penetration testing with 10,000 trojans and viruses. The CCAF multi-layered security can block 9,919 viruses and Trojans which can be destroyed in seconds and the remaining ones can be quarantined or isolated. The experiments show although the percentage of blocking can decrease for continuous injection of viruses and trojans, 97.43 percent of them can be quarantined. Our CCAF multi-layered security has an average of 20 percent better performance than the single-layered approach which could only block 7,438 viruses and trojans. CCAF can be more effective when combined with BPMN simulation to evaluate security process and penetrating testing results.

Keyword: - *CCAF , BPMN, trojans,*

1. INTRODUCTION

CLOUD Computing and its adoption has been a topic of discussion in the past few years. It has been an agenda for organizational adoption due to benefits in cost-savings, improvement in work efficiencies, business agility and quality of services. With the rapid rise in cloud computing, software as a service (SaaS) is particularly in demand, since it offers services that suit users' need. For example, Health informatics can help medical researchers diagnose challenging diseases and cancers. Financial analytics can ensure accurate and fast simulations to be available for investors. Education as a service improves the quality of education and delivery. Mobile applications allow users to play online games and easy-to-use applications to interact with their peers. While more people and organizations use the cloud services, security and privacy become important to ensure that all the data they use and share are well protected. Some researchers assert that security should be implemented before the use of any cloud services in place. This makes a challenging adoption scenario for organizations since security should be enforced and implemented in parallel with any services. Although organizations that adopt cloud computing acknowledge benefits offered by cloud services, challenges such as security and privacy remain a scrutiny for organizational adoption. While overseeing the importance of security, the software engineering and development process should always design, implement and test security features. The data centers have encountered challenges of rapid increase in the data. For example, in a data center that the lead author used to work with, daily increase of 100 terabytes of data was common. If the organization has encountered a rapid rise of data growth and is unable to respond quickly and efficiently, problems such as data traffic, data security and service level agreement issues can happen. In this paper, we focus on the data security while experiencing a large increase of data, whether they are from the external sources such as attack of viruses or Trojans; or they from the internal sources if users or clients accumulate hundreds of terabytes of data per day. This is a research challenge for data security which is essential for the better management of the data center to handle a rapid increase in the data. Apart from the data center security management for rapid growth in data, the software engineering process should be robust enough to withstand attacks and unauthorized access. The entire process can be further consolidated with the development of a framework to tighten up the technical design and implementations, governance and policies associated with good practices. This motivates us to develop a framework, Cloud Computing Adoption Framework (CCAF), to help organizations successfully adopt and deliver any cloud services and projects. In this paper, we demonstrate our security design, implementation and solution for CCAF. We use penetration testing and related experiments to validate its robustness and measure precision, recall and F-measure to justify advantages over other approaches.

1.1 Security Overview under CCAF

Here generalize the areas for security overview. The following are categories of CCAF security aims to cover:

- ➢ Application software security which deals with how we can build systems that can automatically protect itself.
- ➢ Network (LAN, MAN, and GAN), Wireless network security, and Platform Security include Operating Systems, Virtualization, and other systems software.
- ➢ VoIP security as the application is gaining popularity.
- ➢ Convergence network security where converging, multi-network media infrastructures, social networks and technologies, which is one of the emerging areas of research.
- ➢ Service-oriented security where issues related to system services such as denial of service attacks, distributed denial of services, and web services.
- ➢ Cloud security deals with services security, data security and privacy so that services delivered and assets are protected.
- ➢ Open-source software security deals with issues such as trust, certification and qualification models.
- ➢ Software components and architecture, security which deals with building components and architectures with security can be used as plug-ins.
- ➢ Web services security is essential to ensure secured services are delivered with integrity.
- ➢ Systems & Software security engineering deals with building security in (CCAF) right from requirements. This is also considered developing software applications with CCAF.

2. Literature Survey

If cloud computing (CC) is to achieve its potential, there needs to be a clear understanding of the various issues involved, both from the perspectives of the providers and the consumers of the technology. There is an equally urgent need for understanding the business-related issues surrounding CC. We interviewed several industry executives who are either involved as developers or are evaluating CC as an enterprise user. We identify the strengths, weaknesses, opportunities and threats for the industry. We also identify the various issues that will affect the different stakeholders of CC. We issue a set of recommendations for the practitioners who will provide and manage this technology. For IS researchers, we outline the different areas of research that need attention so that we are in a position to advise the industry in the years to come. Finally, we outline some of the key issues facing governmental agencies who will be involved in the regulation of cloud computing.

3. System Analysis

The **Systems Development Life Cycle (SDLC)**, or Software Development Life Cycle in systems engineering, information systems and software engineering, is the process of creating or altering systems, and the models and methodologies that people use to develop these systems.

In software engineering the SDLC concept underpins many kinds of software development methodologies. These methodologies form the framework for planning and controlling the creation of an information system the software development process.

3.1 Modules Description

➢ **Register:**

• In this module, User wants to access his form. So first he registered with his own details, such as user id and username to Cloud and CCAF Framework.

• Then CCAF Framework generates RSA Private and Public Key pair. Then provide to user.

• Each user wants to upload and download his file to cloud.

➢ **Upload Request:**

• In this module, user wants to upload his file to cloud.

• So he generates the file and encrypts that file using RSA Public Key. At the same time he generates the signature for this file.

• Then he sends the cipher text with signature to CCAF Framework.

➢ **CCAF Framework:** In this module, CCAF multi-layered security can protect data in real-time and it has three layers of security: 1) firewall and access control; 2) identity management and intrusion prevention and 3) convergent encryption.

• If any user upload his file. First this file goes to CCAF framework. Now CCAF conduct these 3 layers of security exam. If the uploaded file is passed that exam successfully, then it can be forward to cloud for upload. Otherwise blocked.

➢ **Download:**

• In this module a user wants to download this file, so first he get the private key from Data Owner for decrypt.

• Then he downloads the file from cloud through CCAF Framework. Then he decrypts and access that file using private key.

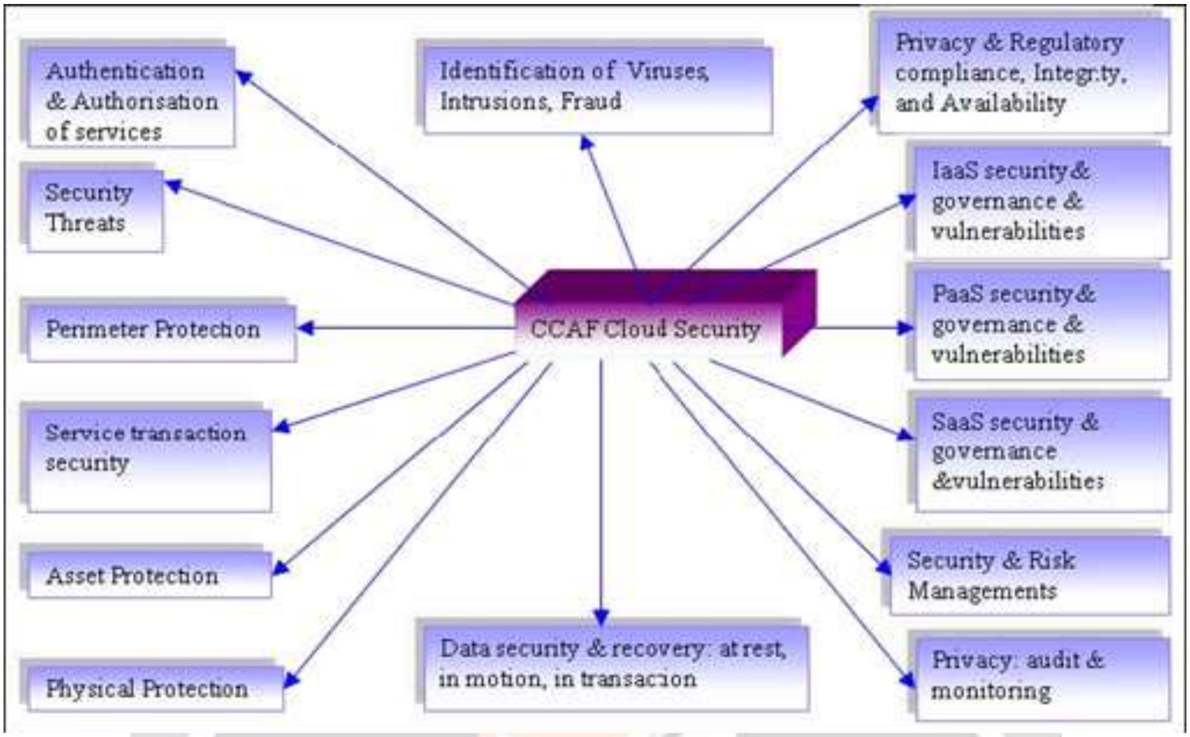
Authentication & Authorisation of services
Identification of Viruses, Intrusions, Fraud
Privacy & Regulatory compliance, Integr.ty, and Availability
Security Threats
IaaS security & governance & vulnerabilities
Perimeter Protection
CCAF Cloud Security
PaaS security & governance & vulnerabilities
Service transaction security
SaaS security & governance &vulnerabilities
Asset Protection
Security & Risk Managements
Physical Protection
Data security & recovery: at rest, in motion, in transacion
Privacy: audit & monitoring

Fig.4.3 System architecture

4. CONCLUSIONS

In this project the Cloud security presented by CCAF from its system design, development and implementation. Here illustrate the required attributes and explain its significance for CCAF, including the security design. To demonstrate how CCAF works, software schema is developed. CCAF can perform quarantine and protective actions based on “Rescue”. The CCAF implementations have been illustrated to show how to enforce security and ensure all users are protected. It provides three layers of security in Access control and firewalls; Intrusion Detection Systems (IDS) and Prevention System; and Isolation Management to optimize Cloud security. CCAF security offers a framework to serve the Cloud community. The key characteristics have been explained. Organizations that are involved in the development and adoption of CCAF have been presented. To develop more service updates and demonstrations for our forthcoming projects to ensure that CCAF security can provide more use cases and added value for the Cloud community.

5. REFERENCES

[1]. S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, “Cloud computing – The business perspective,” Decision Support Syst., vol. 51, no. 1, pp. 176–189, 2011.

[2]. M. A. Vouk, “Cloud computing—issues, research and implementations,” J. Comput. Inf. Technol.—CIT, vol. 4, pp. 235–246, 2008.

[3]. A.K. Jha, C. M. DesRoches, E. G. Campbell, K. Donelan, S. R. Rao, T. G. Ferris, and D. Blumenthal, “Use of electronic health records in US hospitals,” New England J. Med., vol. 360, no. 16, pp. 1628– 1638, 2009.

[4]. H. T. Peng, W. W. Hsu, C. H. Chen, F. Lai, and J. M. Ho, “Financial cloud: open cloud framework of derivative pricing,” in Proc. Int. Conf. Social Comput., Sep. 2013, pp. 782–789.