RESEARCH IN CLOUD SECURITY: PROBLEMS AND PROSPECTS

VAISHALI SINGH¹ & S. K. PANDEY²

¹Department of Computer Science, St. Xavier’s College, Jaipur, Rajasthan, India
²Department of Information Technology, Board of Studies, The Institute of Chartered Accountants of India, Noida, Uttar Pradesh, India

ABSTRACT

Cloud computing continues to be boasted as a major breakthrough in IT management. With the rapid growth as well as demand of Cloud computing, the major concern is on its security and privacy, which is determined by the policies, controls and technologies needed to protect the data, applications, and the related infrastructure of Cloud computing. These challenges impose several new research questions to the research community to ensure proper security of the IT infrastructure. The goal of this paper is to provide the recent advancements and a broad overview of the existing literature covering various dimensions of the Cloud security. The paper also includes various directions for future research in Cloud security based on the related published work and industry trends. This may be very useful, particularly for the entry level researchers, who wish to conduct the research in these related areas.

KEYWORDS: Cloud Security, Cloud Threats, Cloud Computing, Advances in Cloud, IT Management

INTRODUCTION

Cloud computing is a technique to store and access data or a program through internet instead of computer hard drive. Cloud is a metaphor for the Internet [31]. Cloud provides efficient computing by centralizing data reposition, processing and information measures. A simple example of Cloud computing is E-mailing. The Cloud look after the Email management software and server which is totally managed by the Cloud service provider e.g. Yahoo, Google etc. on virtual machines, which brought out of a new transition known as virtualization[31]. Cloud computing is the virtualization of the computer programs through an internet connection rather than installing application/s on every computer. Due to the wide use of virtualization in implementing Cloud infrastructure brings security concerns for the Cloud services. There are various important security issues, which are considered while using virtualization for Cloud computing. Security concerns such as undetected network attacks, allocating and de-allocating resources and Virtual Machine (VM) hypervisor have been seen. Likewise virtualization, there are a number of various Cloud aspects associated with Cloud computing. Cloud issues can be grouped into various dimensions such as Cloud security including privacy, compliance, and legal issues.

Security processes that were once visible are now concealed behind levels of abstraction. This lack of visibility creates a number of Cloud Security issues. The focus is to identify issues in Cloud computing, which considers vulnerabilities, threats, attacks and their countermeasures to provide security at each layer of Cloud computing. These issues along with others have been looked into and various countermeasures have been provided but Cloud needs to be more secure and robust to fulfil the daily needs of the clients. There is a need for development of a process that would help to analyze all high/medium/low risks and provide countermeasures for the same.

There are various research contributions on the related areas, but there is an urgent need for the systematic review of the same. Cloud computing research deals with the advances and research in technical aspects of Cloud computing
security, such as Cloud security requirements, Cloud security vulnerabilities, Cloud threats and its countermeasures, trust, privacy, legal issues and so on.

Beyond this introduction on the background details, the remainder of this paper is organized as follows. The next section highlights the survey of existing research in the related area/s. Afterwards, ‘Future Research Directions’ is given in the next section. Finally, conclusion is reported at the end of the paper.

A SURVEY OF THE RELATED RESEARCH

Researchers are continuously working in the area with many fronts. This section highlights the already accomplished research contributions available in the literature, which is given as follows:

Rongxing Lu, Xiaodong Lin, Xiaohui Liang, Xuemin (Sherman) Shen proposed a new security and provenance model for data forensics and post examination in cloud computing. The system proposed is represented to provide the privacy and security on secret documents/files that are piled up in the cloud [1].

Hasan Tabaki and James B.D. Joshi illustrated the unique issues of security and privacy challenges with Cloud. They explored the roadblocks and solutions to providing a trustworthy Cloud computing environment. They explained the existing security and privacy solutions, which must be critically re-evaluated with regard to their appropriateness for Clouds [2].

La Quata Sumter proposed the design of a system that captured the movement and processing of the information kept on the Cloud. There is a need of security captured device on the Cloud, which would definitely ensured users that their information is secured and safe from security threats and attacks. The proposed implementation was based on a case study and implemented in a small Cloud computing environment [3].

Kresimir Popovic and Zeljko Hocenski provided a generic overview of the security issues, the requirements and the challenges that many Cloud service providers’ encounter. They described twenty recommended security management models and their requirements for Cloud computing that Cloud service providers should definitely consider as they develop or refine their compliance programs [4].

Mladen appraised the issues associated with Cloud computing and virtualization. Further they also assessed Cyber infrastructure, Service oriented Architecture. The paper identifies the research issues and security issues in particular. The researchers ranked security as the primary challenge in cloud computing [5].

Mervat AdibBamiah and Sarfraz Nawaz Brohi discussed the characteristics of a stormy Cloud that contains threats and vulnerabilities. However, beside these benefits, there were seven deadly threats and vulnerabilities encountered in the technology [6].

Wenchao in his paper have taken alternative perspective and proposed data centric view of Cloud security. The researches explored the security properties of secure data sharing among the applications hosted on Cloud. They discussed the data management issues in distributed query processing, Forensic and system analysis and query correction assurance. They proposed a new security platform for Cloud computing, which is named as Declarative Secure Distributed Systems (DS2) [7].

Anthony Bison ghashed out security risks in Cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. The paper discussed about the Cloud computing strengths, vulnerabilities, and relevant areas in information risk management. In addition, they analyzed the organization security risks, threats, and
useable countermeasures before adopting this technology [8].

Paul Wooley provided a list of security risks reported in the selected literature that were associated with the Infrastructure as a Service (IaaS) Cloud computing service offerings. This paper identified security risks, which were aligned within the Confidentiality, Integrity and Availability (CIA) security objectives model. Eight identified types of attacks are classified in relation to three origins and mapped to the CIA model of security risks [9].

Yoshiaki Hori, Takashi Nishide and Kouichi Sakurai reported the security aspects for internal threats on Cloud computing. They discussed about the countermeasures against insider threats in network security aspect. According to them, in the context of countermeasure against insider threats, access control in a network has no perimeter to be verified. A conventional access control process by using a firewall on a perimeter is not suitable. They showed a mechanism of countermeasure against insider threats in network security for countermeasure technically and legally [10].

Sören Bleikertz, Matthias Schunter, Konrad Eriksson, Christian W. Probst and Dimitrios Pendarakis mentioned that benefits of Clouds are shadowed with the security, safety and privacy challenges and due to these challenges the adoption of Cloud computing had been inhibited to a great extent. An approach has been presented for analyzing security at client side and server side. Amazon's Elastic Compute Cloud (EC2) has been chosen for this assessment. The primary aim was focused on the accessibility, vulnerabilities in the entire Cloud infrastructure. They implemented the security analysis model & weigh up it for realistic environments [11].

Michael Jordon, Sven Schlüter, Karl Madden, James Cormack, David Orubaraised awareness of the technical security risks associated with the Cloud and provided practical proposal to defend the Cloud against these risks, and to intimate questions for the service provider by the Cloud client in future. The researchers suggested that clients should adopt a specialised set of security policies relating to Cloud environments to ensure that they remain secure when migrating to and using the Cloud [12].

Sara Qaisarand Kausar Fiaz Khawaja proposed that Cloud computing is a new term that is introduced in business environment where users can interact directly with the virtualized resources and safe the cost for the client. Cloud security issues and their counter measures were discussed in the paper. It had several models to protect its data for the business users [13].

Flavi and Roberto explained, integrity protection problem in the Clouds, sketches a novel Architecture and Transparent Cloud Protection System (TCPS) for improved security of cloud services. They have identified the integrity safety problem in clouds. They proposed a system, and the system is named as Transparent Cloud Protection System (TCPS) for increased security of Cloud resources [14].

Ayesha Malik, and Muhammad Mohsin Nazir defined a methodology for Cloud providers that would protect data of user and crucial information, which is of high importance. The paper brought summarized details of Cloud computing, it’s various models considering to services and deployment and including main security risks and issues [15].

Raghu Yeluri, Enrique Castro-Leon, Robert R. Harmon and James Greene reported about the experiences of Intel team with threats to security and resources control in Cloud computing. They explored challenges in deploying and managing services in a Cloud infrastructure from a security perspective. They discussed the work that Intel is doing with partners and the software vendor ecosystem to enable a security enhanced platform and solutions with security anchored and rooted in hardware and firmware to increase visibility and control in the Cloud [16].

Wayne A. Jansen explained the benefits of Cloud computing and highlighted the basic security issues that are still
associated with Cloud services. The paper brought primary problems in terms of Cloud security, which are alleged to Cloud computing security and privacy issues. It focused on the public Clouds that needs significant consideration and presents required facts and figures to make organizations data security decisions [17].

KuiRen, Cong Wang, and Qian Wang investigated various security challenges for the public Cloud without considering the threats in service models. They discussed several critical security challenges that current research thrusts aren’t yet addressing. [18].

Miranda and Siani stated that most important obstacle to wide acceptance of Cloud computing services is security and privacy issues in Cloud computing; users have serious concerns about confidential data seepage. Privacy is not observed while critical data is being processed in the public accessible Cloud. Some practical scenarios has been discussed in the paper, Based on these scenarios it is recommended strongly that use of sensitive information must be minimized when data is processed on Clouds and privacy to end users must be assured. To address this issue, a client-based privacy manager tool has been proposed in this paper. The proposal reduces security issues, and provides added privacy features [19].

Dimitrios Zissis and Dimitrios Lekkas identified generic design principles of a Cloud environment, which stem from the necessity to control relevant vulnerabilities and threats through adopting software engineering and information systems design approaches. Cloud environment security requires a systemic point of view, based on trust, mitigating protection to a trusted third party [20].

K.Valli Madhavi, R. Tamilkodi and K. Jaya Sudha proposed to construct a perfect system with powerful computing capability through a large number of relatively low-cost computing entity, and using Cloud models like SaaS, PaaS, and IaaS to distribute the computing capacity to end user’s hands and introduced the background and service model of Cloud computing and also introduced the existing security issues in Cloud computing [21].

Vahid Ashktorab and Seyed Reza Taghizadeh explained the major security threats of Cloud computing systems and introduced the suitable countermeasures for them. They also cited the aspects to be focused on when talking about Cloud security and through different viewpoints, categorized these threats, providing a useful and little-known list of threats. Afterward, some effective countermeasures are listed and explained [22].

Mardiana Mohamad Noor and Wan Haslina Hassan presented that wireless network is an easy access to local system if the network is not properly segregated. The developments of wireless network give flexible access especially under (bring your own device) BYOD policy [23].

Carlo Marcelo Revoredo da Silva, Vinicius Cardoso Garcia, Ricardo Batista Rodrigues, Leandro Marques do Nascimento and José Lutiano Costa da Silva proposed a Systematic Mapping metrics about publications available in prior literature that deal with some of the seven security threats in Cloud Computing, based in the guide entitled "Top Threats to Cloud Computing" from the Cloud Security Alliance (CSA). They identified the more threats and distributed between fifteen Security Domains. They also identified the types of solutions proposed for the threats [24].

A. Padmapriya and P. Subhasri highlighted the Cloud computing Security Challenges & Encryption Practices and presented the comparative study of several algorithms. The paper analyzed the importance of security to Cloud and compared three algorithms namely Data Encryption Standard (DES), RSA, Homomorphic encryption for data security in Cloud based on scalability, security and authentication type [25].

According to the Security of Cloud Computing Users conducted in 2013 by Ponemon Institute, one of the primary
challenges is for organizations to encourage greater cooperation and collaboration between IT security and end-users. The purpose should be to improving security of Cloud computing with the organizations’ business goals [26].

Abhinay B. Angadi, Akshata B.Angadi and Karuna C.GullIn illustrated various security concerns related to three basic services provided by a Cloud computing environment [27].

FUTURE RESEARCH DIRECTION

Security is a wide area of research with respect to Cloud Computing [32]. Researchers have done a significant work in the area/subthere is still a need to work further in the related area/s for making them more imperative. Accordingly, various future research directions in the aforementioned area/s have been identified and given as follows:

- There is a need for structured approach for conducting risk analysis in order to uncover security threats lying with the Cloud deployed. A backup plan can be proposed to solve security issues in both Cloud providers and Cloud consumers [25].

- Cloud providers need to cover end-users concerns about security and safety of storing confidential data on the Cloud. They should provide user’s authentication and authorization, up-time and performance, as well as data backup and disaster recovery and provide reliable SLAs for their Cloud applications. This aspect concerns the view of Cloud computing as SaaS to ensure security of data transfer rather than a traditional secure application life cycle. This can be considered as a future work [13][15] [25].

- An appropriate symmetry between the potency of controls and the relative risk associated with particular programs and operations must be ensured [17].

- There is need to develop and design in-depth security techniques and policies in terms of people, processes and technology [6] [33].

- By looking at the contributions from various IT industries worldwide, it’s obvious that cloud computing will be one of the leading strategic and innovative technologies in the near future [6].

- There is a need to examine the existing framework to make feasible for large scale Cloud computing environments [3].

- There is a need to find out the solution for the drawbacks found in different security methods and come up with new solution or method to secure the Cloud [27].

- There is a need to study the secure provenance system, which had limitation as it was difficult to implement due to on complex mathematical model, which is very difficult to understand [1].

- Clients should not assume that Cloud providers automatically provide security; in fact, future research indicates that there are more security risks associated with the Cloud than with a traditional dedicated hosting solution [12].

- Security in a Cloud environment requires a general point of perspective, from which security will be built on trust, mitigating protection to a trusted third party. One of the future works may be to develop a model to detect and prevent the most common Virtualization related threats [20][28].

- In the last few years, there have been various studies that concentrate on internal security aspects in particular areas. There is a need to develop a model, which provides pathway for separation of duties, like isolating security organization to security force, can ensure protection from internal threats [10].
Cloud supplier cannot know all business requirements in detail. They may be unaware of the regulations to which it must adhere. A model is needed that may help various clients meet the Legal and Regulatory Issues [13][21][26].

The future work need to have detection on faults and attacks, in order to secure the services, data and resources and threads. Also examine workload, particular workloads of high security isolation and execution at specific locations with declared security policies that are appropriate [29].

Requirement for development of a conceptual Cloud security methodology that would include not only listing of all possible threats but also all plausible countermeasures may be one of the futures works [22].

There is a need to develop a mitigation mechanism whose sole objective should be prevention of client’s data loss. Also there is no systemic point of view as a whole that encourages greater cooperation and collaboration between IT security and end-users [13].

The future work need to have contribution more in empirical/practical aspects of Cloud computing [5].

Only identifying on Cloud computing security issues is not sufficient. There is a need to propose any tool or framework to address identifies issues [17].

The research on security issues of Cloud computing is vast. There are no security standards for secure Cloud computing. A future work on security standards for secure Cloud computing is need through prior researches.

In future work, there is a need to propose a backup plan to solve security issues in both Cloud providers and Cloud consumers [25].

New monitoring techniques and tools specifically designed for Cloud Computing are needed, which can be easily integrated with a control methodology that manages the performance of the enterprise system.

One of the major area of research may be to a structured approach for conducting risk analysis in order to uncover security threats lying with the Cloud deployed.

This is a need to plan and investigate in more detail the obstacles of a given compliance to be inserted in Cloud Computing scene.

Future work is needed to understand the tradeoffs between security and performance for each Cloud [30].

Through reviewing the existing papers, it resulted that the future work is needed develop a model to detect and prevent the most common virtualization related threats.

To palliate the threat Cloud stakeholders need to invest in risk assessment. For this a depth study of risks need to be done.

One of the future works may be to explore new attack vectors on clouds. It is important to determine the actual threat conventional worms pose to the cloud.

There is a need to study Cloud Security Model for dealing with complex structured Services of Cloud computing.

Based on these aforementioned research directions, various sub areas have been identified; a pictorial representation of the same is given as follows:
CONCLUSIONS

Research studies reveal that Cloud environment needs to recognize the importance of security within its various areas. There should be a bond of trust and privacy between the service provider and the client. Security must be viewed as a continuous process to meet the changing needs of a highly volatile computing environment. There is a need to have a holistic approach regarding cloud computing security methodology, which can be used in general, in any service model, at any stage till the client is using the service. There should be self-awareness from the client side too, regarding its own security. Keeping in view these observations, this study provided a detailed review of the existing literature and offered a number of research areas where future work is required, based on the existing published work. The paper can provide a significant help to get the research areas, where further work is required especially for entry level researchers.

REFERENCES


AUTHOR’S DETAILS

Vaishali Singh is presently working as an Assistant Professor in the Department of Computer Science, St. Xavier’s College, Jaipur, India. She has an excellent academic background right from the school level. Under the Institute-Industry linkage program, she delivers expert lectures on various areas of Computer Science. She has contributed many research papers in the conferences of national repute. Her research interest includes: Cloud Security, Cloud Security vulnerabilities, threats and countermeasures, Access control, Identity measurement etc.
Dr. Santosh K. Pandey is presently working as a Faculty of Information Technology with Board of Studies, The Institute of Chartered Accountants of India (Set up by an Act of Parliament) New Delhi. Prior to this, he worked with the Department of Computer Science, Jamia Millia Islamia (A Central University) New Delhi and Directorate of Education, Govt. of NCT of Delhi. He has a rich Academics & Research experience in various areas of Computer Science. His research interest includes: Software Security, Requirements Engineering, Security Policies and Standards, Formal Methods, Cloud Computing, Security Metrics, Vulnerability Assessment etc. He has published around 46 high quality research papers and articles in various acclaimed International/National Journals (including IEEE, ACM, CSI) and Proceedings of the reputed International/ National Conferences (including Springer). Out of these publications, most of them have good citation records. He has been nominated in the board of editors/reviewers of various peer-reviewed and refereed Journals. In addition, he has also served as a Program Committee Member of several reputed conferences in India as well as abroad. He has also been designated in various academic/research committees by the government organizations as well as software companies as a subject expert.