Security Techniques For Protecting Data Incloud Computing

Choragudi Sasidhar and Dr. Sunita Gond

Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore (M.P.) - 452016, India.

Corresponding Author : Choragudi Sasidhar

ABSTRACT
Portable Cloud Computing is another innovation which alludes to a foundation where both data stockpiling and data handling work outside of the cell phone. Another new innovation is Internet of Things. Web of Things is another innovation which is filling quickly in the field of broadcast communications. Finishing up, we present the commitment of Cloud Computing to the innovation. In this way, it shows how the Cloud Computing innovation improves the capacity of the Cloud Computing. At last, we study the security difficulties of the coordination of Cloud Computing. The effect of distinguished relief procedures is fundamentally on security (30%), trailed by execution (22%) and productivity (17%). Likewise we have recognized 17 future difficulties and 8 moderatingrehearse. During the time spent distinguishing proof from research strategies (SLR and Survey), we had recognized an acceptable number of difficulties and alleviation procedures which are being utilized as of now and furthermore in future Cloud Computing.

Keywords: -Cloud, Architecture, Computing, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Mobile Cloud Computing (MCC).

1. INTRODUCTION
From the past few years, there has been a rapid progress in Cloud Computing. Cloud Computing delivers a wide range of resources like computational power, computational platforms, storage and applications to users via internet. The major Cloud providers in the current market segment are Amazon, Google, IBM, Microsoft, Sales force, etc... With an increasing number of companies resorting to use resources in the Cloud, there is a necessity for protecting the data of various users. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user. Below, we have described the two main states that hold your data is out in the Cloud: when the data is in motion (transit) and when the data is at rest, where the data is much expected to be more secure.
The below illustrated are the two main scenarios which we have focused to understand the security of the data in the Cloud. More specifically, Cloud Computing related with wireless telecommunications. The main goal of the interaction and cooperation between things and objects which sent through the wireless networks is to fulfill the objective set to them as a combined entity. In addition, there is a rapid development of both technologies, Cloud Computing and Internet of Things, regard the field of wireless communications. In this paper, we present a survey of Cloud Computing with a focus on the security issues of both technologies. Specifically, we combine the two aforementioned technologies (i.e Cloud Computing) in order to examine the common features, and in order to discover the benefits of their integration.

FIGURE 1: Unauthorized accesses of data within the Cloud

The above figure 1 describes the scenario where the total data of the local network resides within the Cloud, where the local network and the authorized users can access their data physically in the Cloud. At that instant of time, there exists a possibility for unauthorized users to enter and access the data in the Cloud. In this situation, the virtual machines are allotted to users of the Cloud. These machines have valid logins. However, these logins can be abused and cracked. The data may also be accessed in other perverted ways.

Even though there are numerous variations on the definition of Cloud Computing, some basic principles characterize this emerging computing paradigm. Cloud computing provides technological capabilities—generally maintained off premises—that are delivered on demand as a service via the Internet. Given that a third party owns and manages public cloud services, consumers of these services do not possess resources in the cloud model but pay for them on a per-use basis. Thus virtualization of the resources is the key concept. In the real scenario, they are renting the physical infrastructure, platforms and applications within a shared architecture. Cloud offerings can vary from virtual infrastructure, computing platforms, centralized data centers to end-user Web-Services and Web applications to enormous other focused computing services.
Aims and Objectives

The main aim of this research work is to identify and understand the security issues which affect the performance of Cloud Computing. Also, to understand the security techniques which are being used to mitigate these security issues. Thereby providing the standard guidelines for the Cloud service providers and as well as Cloud users. The main objectives of this research are:

1. To understand the security issues and to identify the appropriate security techniques those are being used in the current world of Cloud Computing.

2. REVIEW OF LITERATURE

Jurcut, A. (2020) Interconnecting “things” and devices that takes the form of wearable, sensors, actuators, mobiles, computers, meters, or even vehicles is a critical requirement for the current era. These inter-networked connections are serving the emerging applications home and building automation, smart cities and infrastructure, smart industries, and smart-everything. However, the security of this connected Internet of things plays a centric role with no margin for error. After a review of the relevant, online literature on the topic and after looking at the market trends and developments, one can notice that there are still concerns with regard to security in IoT products and services.

Yasir Ali; Shah Nazir (2020) a comprehensive and in-depth security analysis of IoT devices has been made in light of mobile computing, which is a novel approach. Mobile computing technological infrastructures such as smart phones, services, policies, strategies, and applications are employed to tackle and mitigate these potential security threats. In this paper, the security challenges and problems of IoT devices are identified by a systematic literature review. Then, mobile computing has been used to address these challenges by providing potential security measures and solutions. Hardware and software-based solutions furnished by mobile computing towards the IoT security challenges have been elaborated. To the best of our knowledge, this is the first attempt to analyze the security issues and challenges of IoT in light of mobile computing and it will open a gateway towards future research.

Omar Hayat, Razali Ngah (2020) those mobile D2D protocols normally take different protection mechanisms, which make security investigation considerably challenging. In this paper, we focus on most popular apps in the Google Play Store, with aggregated downloads more than 500 million. Our analysis reveals some critical vulnerability. The key findings are bi-fold. First, the current mobile D2D network framework enabled by Android has significant flaw of over privilege issue. Second, we have identified that most data transfer over mobile D2D network is unencrypted. Furthermore, we exploit the identified Android framework flaws to construct three proof-of-concept attacks and we conclude this paper with security lessons and suggestions of possible solutions against the identified security issues.
Zhisheng Niu (2019) there is little literature that specially investigates the inspection of inappropriate contents in children Android Apps. Toward this end, we propose a novel automatic content inspection and the forensics framework to identify children Android Apps which are not proper for kids under 12. In addition, this framework offers evidence to make users understand why the inspected App is judged as unsuitable. In experiments, we apply this framework on some specially chosen Android Apps which distinctly include inappropriate contents to verify its performance. The results show that it can successfully identify those applications with high precision that reaches 85.7%. Besides, by analyzing the collected children's Android Apps through our framework, we find that 40% of them are identified to be improper, which illustrates the serious issue of unsuitable children Android Apps.

Challa, S.; Wazid, M.; Das (2017) One way to address this problem is by offloading the additional security-related operations to a more resourceful entity such as a fog-based node. Generally, fog computing enables security and analysis of latency-sensitive data directly at the network’s edge. This paper proposes a novel Fog Security Service (FSS) to provide end-to-end security at the fog layer for IoT devices using two well-established cryptographic schemes, identity-based encryption, and identity-based signature. The FSS provides security services such as authentication, confidentiality, and non-repudiation. The proposed architecture would be implemented and evaluated in an OPNET simulator using a single network topology with different traffic loads. The FSS performed better when compared with the PaaS and the legacy method.

3. MATERIALS AND METHODS

Cloud Computing research addresses the challenges of meeting the requirements of next generation private, public and hybrid cloud computing architectures, also the challenges of allowing applications and development platforms to take advantage of the benefits of cloud computing. The research on cloud computing is still at an early stage. Many existing issues have not been fully addressed, while new challenges keep emerging from industry applications.

• Data Analysis Methods

Data analysis or Data synthesis is a means of collecting and summarizing the results of the studies. Data analysis methods are used to structure the data properly based on the findings. In our thesis, initially we have focused on Narrative Analysis for analyzing the results which are obtained from doing Systematic Literature Review and thereafter we have used the Comparative Analysis method for comparing the results of the SLR with the results obtained from the Survey.

• Source of data collection

We have used the direct mailing procedure to send the prepared questionnaire to the experts and few of responses are taken from direct interaction with the experts who is currently having industrial experience in Cloud Computing.
• Reliability of Data

In this work, we followed inclusion-exclusion criteria. As a part of it, total search results after screening by title, duplicates and language are studied individually by both of us to exclude the final papers. In this process, the final individually selected papers are approximately equal. This shows the mutual understanding between both of us in selecting the final outcome. Normally, this relation between both of us is calculated with the kappa analysis approach.

• Survey

In research, Survey is a method of gathering information in the real life from individuals who are working in that particular field. Survey comes under non experimental method. It applies to collect the information surrounding a particular topic which helps the researchers.

4. RESULTS AND DISCUSSION

The Reporting review consist the results from SLR and Survey. In this we have reported the identified security challenges and mitigation techniques from SLR also given information about survey participants and explained the analyzed results from the survey.

• SLR Results

In recent years, the huge amount of research has been done in the area of Cloud Computing. In the process of SLR, we have extracted 69 papers relevant to meet the goals of the research from the large number of papers published since the year 2001. This section covers the results and analysis of the papers that were extracted in the process of SLR. We have given a detailed description of the list of identified challenges and mitigation techniques in appendix section. In the past years, research is followed the distributed computing and mainly focused on service like grid computing. From the last decade, there is a rapid increase in research on new paradigm Cloud Computing which is the next generation computing. We mainly focused on security aspects of the Cloud Computing in last 10 years. Totally 69 papers are retrieved during the literature study. Mostly the selected papers are in between the year 2010 and 2011 which revealed 52 papers and 25 papers respectively. Others include 3 papers published in 2009. The figure below shows the empirical evidence of research on security in Cloud Computing in the last 10 years.

• Identified Mitigation Techniques

From the analysis, we have identified 34 security techniques during the SLR. The detailed description of these techniques is presented in Appendix B. The summary include Identity based authentication, RSA algorithm, Dynamic Intrusion detection system, Multi tenancy based access control model, TLS Handshake, Public key homomorphism, Third party auditor, probabilistic sampling technique, Diffie – Hellman key exchange, Private face recognition, MACs, Data

![Impact of Mitigation Techniques](image)

FIGURE 2: Impact of mitigation techniques

5. CONCLUSION

The identification of security challenges and mitigation techniques in Cloud Computing is challenged by considering the large number of services. Most of the responses from survey, noted that Cloud Computing will place dominant and expandable information transactions. Because it offers many flexible services, provides easy, individualized and instant access control to the services and information where they are for the users. In the process of identification from the research methods SLR and Survey, we have identified satisfactorily number of challenges and mitigation techniques in current and future Cloud Computing. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. As the development of cloud computing technology is still at an early stage, this research effort will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

REFERENCES


