International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 19th August 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-4&issue=ISSUE-4

Title:High security providing by analyzing the previous security issues of Cloud Computing.

Volume 04, Issue 04, Page No: 114 – 118.

Paper Authors

***Y.PAVAN GUPTHA, S.BHANU PRASAD RAO.**

* Dept of CSE, Sri Indu College of Engineering & Technology(autonomous), Tirumala Engineering College.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

HIGH SECURITY PROVIDING BY ANALYZING THE PREVIOUS SECURITY ISSUES OF CLOUD COMPUTING

***Y.PAVAN GUPTHA, **S.BHANU PRASAD RAO**

*Assistant Professor, Dept of CSE, Sri Indu College of Engineering & Technology(autonomous).
**Assistant Professor, Dept of CSE, Tirumala Engineering College.

ABSTRACT:

Cloud computing is an emerging technology solution that provides a robust and scalable computing infrastructure to enable business agility. Cloud computing offers, ongoing availability and low cost services are the main benefits, but as with most new technologies, they also introduce new risks and vulnerabilities. There are several vulnerabilities in cloud computing and several threats to cloud computing. The main obstacle to the growth of this technology is security. In this paper we present the importance of the cloud and various types of security attacks, provider solutions, case studies, and cloud computing trends in 2015-17.

1. INTRODUCTION

Cloud computing has become the latest technology in the computing industry. Its ability to reduce costs, eliminating the need to buy large amounts of software licenses for all employees, reducing the need for advanced hardware, eliminating the need for companies to rent physical space to store servers and databases, and transfer the workload of the local computer that has attracted cloud computing providers such as Amazon, Google, IBM, Yahoo, Microsoft, etc. Cloud has three advantages: it is sold to order (typically by minute or hour), it is scalable (a user may have more or less a service, if needed, at a given time), and the service is completely handled by the vendor. These services are classified as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The infrastructure as a service provides low-level services that can be started with a user-defined hard drive. disk image like Amazon EC2. In Platform you as a service, the Cloud provider offers an API that can be used by an application developer to create platform vendor applications. Examples of PaaS include Force.com, Google Apps, etc. With Software as a Service, the vendor supplies the software product and interacts with users through a front-end portal; Web-based office applications such as Google Docs or Calendar are examples of SaaS. Data security is the means to ensure that data is safe from corruption and that access to them is adequately controlled. Therefore, data security helps ensure privacy. It also helps to protect your personal data. In a traditional application implementation model, important organization data continues to reside within the boundaries of the organization and is subject to its physical, logical and personnel security policies and access control. However, in the SaaS model, organization data stored outside the organization boundary, at the end of SaaS vendor services. Therefore, the service provider must use techniques such as encryption, advanced user authentication and backup to ensure data security.

1.1 CHALLENGES

Protect Data Privacy: Data privacy protection has always been an important aspect of a service level agreement for cloud storage services. Thus, the implementation of a public auditing protocol should not violate the owner's data privacy. In other words a tpa should be able to efficiently audit the cloud

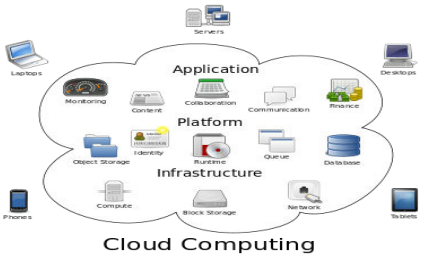
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

data storage without demanding a local copy of data or even learning the data content.

Support: Data Dynamics as a cloud storage service is not just a data warehouse; owners are subject to dynamically updating their data via various application purposes. The design of auditing protocol should incorporate this important feature of data dynamics in cloud computing.

2. CLOUD COMPUTING ENVIRONMENT

When software companies decide to migrate to cloud computing, security is a primary consideration. Cloud computing is the client and vendor side. The client side is the end user who uses the cloud for their work. It offers users the ability to choose the cloud. It is the interface that users see after entering valid user credentials and having the ability to use the services provided by the cloud. The user side can be made up of multiple users, laptops, tablets, mobile phones, and multiple computers. The cloud computing provider is the service provider that includes application servers and data centers, and so on. An application server can be the server of the Sphere Web application, which is an application platform based on Java EJB compatible technology [2]. A data center can provide a massive volume for users to store data. Figure 1 is an example showing the overall view of Cloud Computing. Cloud Security Alliance (CSA) assigns certification to cloud service providers that meet the above criteria. The CSA Trusted Cloud Initiative program was developed to help cloud service providers. Cloud service



providers must maintain user privacy and ensure that information stored in the cloud is always safe. The Service Level Agreement (SLA) between cloud providers and a customer specifies the information and service protocols.

3. RESEARCH

3.1 Depot: Cloud Storage with Minimal Trust

This article describes the design, implementation, and evaluation of Depot, a cloud storage system that minimizes trust assumptions. Depot tolerates buggy or malicious behavior by any number of clients or servers, yet it provides safety and liveness guarantees to correct clients. Depot provides these guarantees using two-layer architecture. First, Depot ensures that the updates observed by correct nodes are consistently ordered under Fork-Join-Causal consistency (FJC). FJC is a slight weakening of causal consistency that can be both safe and live despite faulty nodes. Second, Depot implements protocols that use this consistent ordering of updates to provide other desirable consistency, staleness, durability, and recovery properties. Our evaluation suggests that the costs of these guarantees are modest and that Depot can tolerate faults and maintain good availability, latency, overhead, and staleness even when significant faults occur.

3.2 Providing Database as a Service

We explore a novel paradigm for data management in which a third party service provider hosts "database as a service", providing its customers with seamless mechanisms to create, store, and access their databases at the host site. Such a model alleviates the need for organizations to purchase expensive hardware and software, deal with software upgrades, and hire professionals for administrative and

maintenance tasks which are taken over by the service provider. We have developed and deployed a database service on the Internet, called NetDB2, which is in constant use. In a sense, a data management model supported by NetDB2 provides an effective mechanism for organizations to purchase data management as a service, thereby freeing them to concentrate on their core businesses. Among the primary challenges introduced by "database as a service" are the additional overhead of remote access to data, an infrastructure to guarantee data privacy, and user interface design for such a service. These issues are investigated. We identify data privacy as a particularly vital problem and propose alternative solutions based on data encryption. The paper is meant as a challenge for the database community to explore a rich set of research issues that arise in developing such a service.

3.3 Fully Homomorphic Encryption Using Ideal Lattices

We propose a fully homomorphic encryption scheme -- i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Our solution comes in three steps. First, we provide a general result -- that, to construct an encryption scheme that permits evaluation of arbitrary circuits, it suffices to construct an encryption scheme that can evaluate (slightly augmented versions of) its own decryption circuit; we call a scheme that can evaluate its (augmented) decryption circuit bootstrappable. Next, we describe a public key encryption scheme using ideal lattices that is almost bootstrappable.

Lattice-based cryptosystems typically have decryption algorithms with low circuit complexity, often dominated by an inner product computation that is in NC1. Also, ideal lattices provide both additive and multiplicative homomorphisms (modulo a public-key ideal in a polynomial ring that is represented as a lattice), as needed to evaluate general circuits. Unfortunately, our initial scheme is not quite bootstrappable -- i.e., the depth that the scheme can correctly evaluate can be logarithmic in the lattice dimension, just like the depth of the decryption circuit, but the latter is greater than the former. In the final step, we show how to modify the scheme to reduce the depth of the decryption circuit, and thereby obtain a bootstrappable encryption scheme, without reducing the depth that the scheme can evaluate. Abstractly, we accomplish this by enabling the encrypter to start the decryption process, leaving less work for the decrypter, much like the server leaves less work for the decrypter in a server-aided cryptosystem.

3.4 Malware Injection:

In a malware injection attack, an opponent attempts to inject malicious code into a system. This attack may appear in the form of code, script, active content ... When an instance of a legal user is ready to run on the cloud server, the respective service accepts the calculation instance in the cloud. The only check that is made is to determine whether the instance corresponds to an existing legal service. However, the integrity of the instance has not been verified. By penetrating the instance and duplicating it as if it were a valid service, malware activity succeeds in the cloud.

The first case occurred in May 2009. The United States Treasury Department has put out four public Web sites offline for the Bureau of Engraving and Printing after finding out that a malicious code had been added to the parents. The third cloud service provider hosting the company's Web site was the victim of an intrusion attack. As a result, many websites (BEP and non BEP) have been involved. Roger Thompson, Research Director of Anti-Virus Guard (AVG) Technologies, found that malicious code was injected into the affected pages. Hackers added a small fragment of an almost irrelevant iFrame HTML that redirected visitors to a Ukrainian website. IFrame (Online

Frame) is an HTML document embedded in another HTML document on a website. From there, a number of web-based attacks were launched using a malicious and easy-to-access kit called Eleonore Exploit Pack.

3.5 Wireless Local Area Network Attack:

Local wireless network of a user authorized to perform attacks as man-in-the-middle, accidental association, theft identification, service denial, network injection attacks, etc. In January 2011, German security researcher Thomas Roth used cloud computing to decipher wireless networks based on previously shared key phrases such as those found in homes and small businesses. The attack results have revealed that WPA-PSK-based wireless computing for security is fundamentally insecure. The Roth program was run on Amazon's Elastic Cloud Computing (EC2) system. Using the enormous power of the Amazon cloud, the program was able to run up to 400,000 possible passwords per second. It typically costs tens of thousands of dollars to buy computers to run the program, but Roth says EC2 and its software can guess a typical password in about six minutes. The type of EC2 computer used in attack costs $ 0.28 cents per minute, so $ 1.68 is all that's needed to hack a wireless network.

4. CONCLUSION

Cloud computing security involves several areas and problems. Numerous security mechanisms have been developed to prevent various attacks and protect cloud computing systems. Researchers continue to develop new technologies to improve the security of cloud computing. In this document several real cases are presented in which clouds of companies have been infiltrated by attacks. Discussion of the social engineering attack, the signature attack on the XML, malware injection, account hijacking, and attack on the local wireless network are being discussed. The above discussed in this document are the main security issues that block the growth of cloud computing so far.

5. REFERENCES

1. M. Armbrust et al., “A View of Cloud Computing,” Comm. of the ACM, vol. 53, no. 4, pp. 50-58, 2010.
2. W. Jansen and T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing,” Technical Report Special Publication 800-144, NIST, 2011.
3. A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten, “SPORC: Group Collaboration Using Untrusted Cloud Resources,” Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, Oct. 2010.
4. J. Li, M. Krohn, D. Mazie`res, and D. Shasha, “Secure Untrusted Data Repository (SUNDR),” Proc. Sixth USENIX Conf. Opearting Systems Design and Implementation, Oct. 2004.
5. J. Li and E. Omiecinski, “Efficiency and Security Trade-Off in Supporting Range Queries on Encrypted Databases,” Proc. 19th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, Aug. 2005.
6. E. Mykletun and G. Tsudik, “Aggregation Queries in the Database-as-a-Service Model,” Proc. 20th Ann. IFIP WG 11.3 Working Conf. Data and Applications Security, July/Aug. 2006.
7. D. Agrawal, A.E. Abbadi, F. Emekci, and A. Metwally, “Database Management as a Service: Challenges and Opportunities,” Proc. 25th IEEE Int’l Conf. Data Eng., Mar.-Apr. 2009.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Y.Pavan Guptha

B.Tech completed 2009 in scient institute of technology

M.Tech completed 2014 in anurag college of engineering

Work Experience july 2010 to july 2012 as a asst.prof and Examinaion branch incharge in Siddhartha institute of technology &sciences

Work Experience nov 2016 to jan 2017 as a asst.prof and Examinaion branch incharge in Tirumala enginnering college

Work Experience jan 2017 to july till now as a asst.prof . Sri Indu College of Engineering & Technology(autonomous)

NAME: **S.BHANU PRASAD RAO**

Branch: CSE

Qualification: BTECH(CASE)(SRTIST Nalgonda affiliated to JNTUH) 2003-2007 ,MTECH(NIT Rourkela) (CSE) 2008-2010

Designation: Assistant Professor.

Experience: 2 years 6 months

(Tirumala Engineering College)