IJCSC Volume 4 • Number 2 September 2013 pp. 213-218 ISSN-0973-7391

Analysis and study of data security issues in cloud computing

Pawan kumar[1], Dr. Sawtantar Singh[2], Dr. Surender[3]

[1]Ph.D Research Scholar, Deptt. of Computer Engineering, Punjab Technical University, Kapurthala (Punjab), INDIA

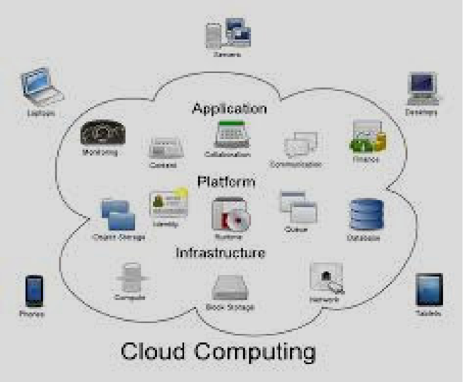
[2]Professor , Deptt. of CSE, BMSCE, Mukatsar(Punjab), INDIA
[3]Associate Professor, Deptt. of CSE, HCTM Technical Campus, Kaithal(Haryana), INDIA
[1]pawanspp@gmail.com , [2]sawtantr@gmail.com, [3]jangra.surender@gmail.com

Abstract: Data protection is a critical issue in cloud computing environments. Clouds have no borders and the data can be physically located anywhere in the world. So this phenomenon raises serious issues regarding user authentication and data confidentiality. To build the trust for the growth of cloud computing the cloud providers must protect the user data from unauthorized access and disclosure. One technique could be encrypting the data on client side before storing it in cloud storage. Encrypting data on client machine and then storing the information to public cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. Therefore it becomes more difficult for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance, the security service provided by the cloud storage provider, the information might be compromised.

Keywords: Data Mining, Cluster Analysis; Statistical Method.

1. Introduction:

In recent year cloud computing has emerged as a new computing example in which various users share the resources in pay per site/ per service basis. The resources in such a computing paradigm are located at distributed sites with control from the service providers. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1] as shown in figure 1



Cloud computing is an emerging technology which provides IT services and resources to the customers through public network specifically internet. The cloud computing services and infrastructure are mostly owned by a third party called cloud service providers. Cloud computing offers an innovative model for the organizations to use software applications, storage and processing capabilities of cloud without investing on the infrastructure. As compared to existing IT models, the cloud computing offers many advantages like scalability, flexibility, efficiency and non-core activities [1]. Despite these extraordinary benefits of cloud computing, the security is a major concern. According to the International Data Corporation (IDC) survey 74% IT managers and Chief Information Officers (CIOs) thinks that security and privacy issues are the main obstacle preventing organizations to adopt cloud computing services and the survey conducted by Garter that more than 70% Chief Technology Officers (CTOs) showed their concern about data security and privacy issues in cloud computing [2, 3].

1.1 Cloud Service Delivery Models

The cloud computing model is based on three service delivery models and three cloud architectural models [2, 3].

- **Cloud Software as a Service (SaaS)**: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email)
- **Cloud Platform as a Service (PaaS)**: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider (e.g., configurations)
- **Cloud Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.(e.g., host fire walls)

According to customers' different demand, cloud computing technology includes three kinds of architectural models, which are public cloud, private cloud and mixed cloud

- **Public cloud:** Run by a third party, public cloud can put many different customers' operation on the cloud of servers, storage systems and other infrastructure mix. End users do not know to the other users who run their operations on the same server, network or disk.
- **Private cloud**: Private Cloud is built for clients to use it privately, and thus it can make the most effective control of data, security and service quality. The company has the infrastructure, on the basis of the infrastructure, it can control the way to deploy applications, control how and where the applications run. They have server, network and disk, and can determine which users are allowed to use these infrastructures. Private clouds can be deployed in enterprise's data centers; it can also be deployed in a hosting site. Private cloud can be built by the companies themselves or by the cloud providers.
- **Mixed cloud**: The mixed cloud is to mix the public cloud model and private cloud model together.

1.2 Mobile cloud computing

Mobile Cloud Computing (Fig.2) is a new concept that can be described as the availability of Cloud Computing resources and services for mobile devices. As in the case of Cloud Computing, several definitions were proposed to define Mobile Cloud Computing.

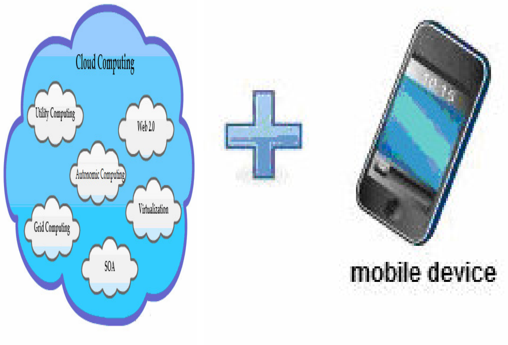


Figure: 2 Mobile Cloud Computing

Mobile Cloud Computing is defined in as follows: “Mobile cloud computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smart-phone users but a much broader range of mobile subscribers.”

Another definition given in: “Mobile cloud computing is a model for transparent elastic augmentation of mobile device capabilities via ubiquitous wireless access to cloud storage and computing resources, with context-aware dynamic adjusting of offloading in respect to change in operating conditions, while preserving available sensing and interactivity capabilities of mobile devices.” [4]

The first definition emphasizes that Mobile Cloud Computing benefits from Cloud Computing features – storage and data processing, and also reveals a Mobile Cloud Computing characteristic – moving part of the computation and the storage away from mobile phones. The second definition is more concise. It starts by saying what is Mobile Cloud Computing – a model; it also tells the purpose of using Mobile Cloud Computing –

to overcome the mobile device challenges; it tells the way – using storage and computation resources offered by Cloud Computing model; it also specifies that is appropriate to take into account the context of the mobile operating conditions. As a conclusion, we can say that Mobile Cloud Computing offers Cloud Computing resources such as storage and computations to the mobile devices with limited CPU speed, memory capacity and display size which allows the development, deployment and execution of powerful mobile applications [5].

1.3The security challenges in cloud computing

The security status of cloud computing has strong government support and promotion in Europe, the United States and other countries, cloud computing security issues have also been extensive attention of Governments. In November of 2010, the U.S. Government CIO Council published the government documents that the government agencies use cloud computing, in which described the challenges of cloud computing and security for cloud computing, asked the Government and various institutions to assess the security risks, which be compared with their security needs .the analysis show that unified risk assessment and authorization identified by the government authority institution can accelerate the assessment and the use of cloud computing and reduce the cost of risk assessment.

In the March of 2010, the European network of legal experts and leaders in the European Parliament called for a global agreement on data protection to address data security of cloud computing. European Network and Information Security Agency (ENISA), said management will be required to promote cloud computing providers to notify customers about security attack situation.

The main security problem of cloud computing

- **Network attacks:** currently, the network attack is still the biggest challenge of network security. As more and more packages, customers, and enterprises migrate their data into the cloud computing, cloud computing will appear more and more network attacks and fraud. Security experts said that cloud computing will be the focus of hackers within five years.
- **Data Security:** Data of Cloud is stored in different physical locations, distributed in various parts of the Earth, in the absence of corresponding technical and regulatory constraints, data security is difficult to get protection. First of all, different places have different levels of technology, some advanced and some behind. Data is safe somewhere, but there may be some risk in another place. Secondly, there are different regulations in different places.
- **The lack of safety standards:** Recently, there were not the security model and standards for cloud computing architecture, the confidentiality, integrity and availability of data in the cloud service will be borne by the ultimate consumers of cloud computing, not by the cloud service providers. the rapid development of cloud computing is Promoted by several major IT giants, although they are taking the money in the IT field, after all cloud computing is a new thing, and structural standard between the different cloud computing service provider is not perfect.
- **Private information is difficult to ensure:** Cloud users store data in the cloud, but they cannot ensure if their private information is sold out by cloud service providers or not. How to select the Trusted Cloud Computing service provider? For example, in March of 2009, the famous Google has admitted that it leaked private customer information accidentally [6].

2. RELATED WORK

Mutum Zico Meetei, Anita Goel [6] This paper focuses on security issues arising from the usage of cloud services. Enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the key factor which hampers growth of cloud computing. Some of the fundamental security challenges are data storage security, data transmission security, application security and security related to third-part resources.

Parsi Kalpana, Sudha Singaraju [7] proposed a method by implementing RSA algorithm for cloud computing. Since Cloud computing stores the data and disseminated resources in the open environment, security has become the main obstacle which is hampering the deployment of Cloud environments. RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman. In their proposed work, they were using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, they were allowing unauthorized access to it.

Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros [8] proposed CloudSim which is an extensible simulation toolkit that enables modeling and simulation of Cloud computing environments. The CloudSim toolkit supports modeling of one or more virtual machines (VMs) on a simulated node of a Data Center, jobs, and their mapping to suitable VMs. It also allows simulation of multiple Data Centers to enable a study on federation and associated policies for migration of VMs for reliability and automatic scaling of applications

M. Sudha, Dr.Bandaru Rama Krishna Rao and M. Monica [9] proposed to implement a simple Data Protection framework which performs authentication, verification and encrypted data transfer, thus maintaining data confidentiality. Advanced Encryption Standard security algorithm is implemented for ensuring security framework. Some examples of emerging Cloud computing infrastructures are Microsoft Azure, Amazon EC2, Google App Engine, and Aneka. Cloud service providers enable users to access and use the necessary resources via the internet. To provide these resources, providers often fall back upon other providers in the cloud, hence this raises security issues in Cloud Environment as Clouds have no borders and the data can be physically located anywhere in the world. So this phenomenon raises serious issues regarding user authentication and data confidentiality. Programming is performed using JAVA platform, Cloud environment is created using wired and wireless LAN networks.

Mr. D. Kishore Kumar, Dr.G.Venkatewara Rao, Dr.G.Srinivasa Rao [10] They make an attempt to investigate the crucial security threats with respect to cloud computing. They further focuses on the available security measures which can be used for the effective implementation of cloud computing. In order to provide quality of service, this environment makes every effort to be dynamic and reliable. As in most other streams of computers, security is a major obstacle for cloud computing. There are various opinions on the security of cloud computing which deal with the positives and negatives of it.

Cong Wang, Qian Wang and Kui Ren [11] They focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, they propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, their scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

M. Vijayapriya [12] This research paper presents what cloud computing is, security algorithms and the challenges in cloud computing. A network security system typically lies on the layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and the appliances. All components work together to increase the overall security of the computer network. For enhancing the security, many algorithms are widely used. Cloud Computing is a set of IT based Services that are provided to a customer over a network and these services are delivered by a third party provider who owns the infrastructure. It is often provided "as a service" over the Internet and that was typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), data storage as a service (DSaaS).

Rohit Bhadauria, Sugata Sanyal [14] This extensive survey paper aims to elaborate and analyze the numerous unresolved issues threatening the cloud computing adoption and diffusion affecting the various stake-holders associated with it. Since data-centre may be located in any part of the world beyond the reach and control of users, there are multifarious security and privacy challenges that need to be understood and addressed. Also, one can never deny the possibility of a server breakdown that has been witnessed, rather quite often in the recent times. There are various issues that need to be addressed with respect to security and privacy in a cloud computing environment.

Mohit Marwaha, Rajeev Bedi [15] The paper analyzes the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage. Even though the cloud continues to grow in popularity, Usability and respectability, Problems with data protection and data privacy and other Security issues play a major setback in the field of Cloud Computing. Privacy and security are the key issue for cloud storage. Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval.

Soeung-Kon(Victor) Ko), Jung-Hoon Lee), Sung Woo Kim [16] This paper discusses the different security issues that arise about how safe the mobile cloud computing environment is. Building applications on on-demand infrastructures instead of building applications on fixed and rigid infrastructures were provided by cloud computing provides. By simply tapping into the cloud, enterprises can gain fast access to business applications or infrastructure resources with reduced Capital Expenditure (CAPEX). The more and more information is placed into the cloud by individuals and enterprises, security issues begins to grow and raised.

D. Popa1 K. Boudaoud M. Cremene1 M. Borda [17] This paper is an overview on Mobile Cloud Computing security issues. Mobile Cloud Computing, the combination of mobile devices with Cloud Computing services. It brings several advantages to the devices with low resources advantages that lead to the development of rich functionality applications. The security issues in Mobile Cloud Computing can be classified as follows: mobile threats and cloud threats. The main purpose of these menaces is to steal personal data (e.g. credit card numbers, passwords, contact database, calendar, location) or to exploit mobile device resources.

A. Cecil Donald, S. Arul Oli, L. Arockiam[18] In this paper, the working concepts of MCC and its various security issues and solutions given by researchers are analyzed. Mobile Cloud Computing (MCC) technology is growing rapidly among the users and at the same time it introduces the new security threats also. In MCC, a lot of investigations are being carried out to eradicate the issues to make IT more reliable and secure because more precious data are stored in the cloud environment. As the Internet-enabled mobile devices including smartphones and tablets continue to grow, web-based malicious threats will continue to increase in number to make more complex. Securing data is more critical in the Mobile Cloud Environment. In MCC, Security is the major issue.

Pragati Chavan, Rakesh Rajani[19] In this paper, we discuss recent mobile application models related to cloud computing technologies. This paper was explained how cloud computing and mobile devices combine present and future new imperatives and challenges for developing countries. They were conclude that the future of mobile clouds will be in novel technologies such as network coding as well as in combination with social networks in order to boost cooperation among users as well as connect people over the shared content.

Joshi Ashay Mukundrao [20] This paper has been written to focus on the problem of data security. Service providers must have a viable way to protect their clients' data, especially to prevent the data from disclosure by unauthorized insiders. To ensure the security of users' data in the cloud, we propose an effective and flexible scheme with two salient features, opposing to its predecessors. Avoiding unauthorized access to user's data by signaling user by sending message to his/her mobile number at the start of transaction. Displaying fake information in case of unsuccessful login for avoiding further login trials by intrusion.

JASLEEN [21] The various modules of this paper are MCC applications, major concerns and security concern with the preventive measures. Mobile Cloud Computing (MCC) is a revolution in the field of mobile world. This paper presents the concept of mobile cloud computing which is a current gist in the field of computer. Beside this it acquaint with a new term called Mcloud that is still to be explored more.

3. PROBLEM FORMULATION

Data protection is a critical issue in cloud computing environments. Clouds have no borders and the data can be physically located anywhere in the world. So this phenomenon raises serious issues regarding user authentication and data confidentiality. To build the trust for the growth of cloud computing the cloud providers must protect the user data from unauthorized access and disclosure. One technique could be encrypting the data on client side before storing it in cloud storage.

3.1 Research Problem

Encrypting data on client machine and then storing the information to public cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people. Therefore it becomes more difficult for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance, the security service provided by the cloud storage provider, the information might be compromised.

In our proposed work we will use various encryption description algorithms like Advanced Encryption Standard (AES), Ron Rivest, Adi Shamir and Len Adleman (RSA) etc. to solve the above problem. This proposed system can be mainly divided into two parts: Server and Client.

3.2 Research Methodology

In our proposed work we will use Cloudsim simulator and JAVA for simulating the above algorithms. The client requests the server and server responses by granting the clients request. The proposed system will provide the features.

1. Server - The server should be able to perform the following features:
The first and foremost problem is to find the server. We should identify the program in the server which processes the client's request. Authentication of user's generation of keys encryption of data files
2. Client: The client should be able to perform the following features:
Authenticate itself from server request for keys decrypt data files in our proposed work Time monitoring of the whole process will be done to ensure it's feasible in real-time environment of a network.

REFRENCES

[1] S. O. Kuyoro, F. Ibikunle and O. Awodele, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), vol. 3, Issue 5, (2011).

[2] Abid Shahzad, Mureed Hussain, "Security Issues and Challenges of Mobile Cloud Computing "International Journal of Grid and Distributed Computing Vol.6, No.6 (2013), pp.37-50.

[3] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering (ICCSEE), (2012) March 23-25.

[4] Mobile cloud Forum, available online: http://www.mobilecloudcomputingforum.com

[5] White Paper, "Mobile Cloud Computing Solution Brief," AEPONA, November 2010.

[6] Mutum Zico Meetei, Anita Goel "Security Issues in Cloud Computing" International Conference on BioMedical Engineering and Informatics, IEEE 2012

[7] Parsi Kalpana, Sudha Singaraju "Data Security in Cloud Computing using RSA Algorithm" International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[8] Rajkumar Buyya1, Rajiv Ranjan2 and Rodrigo N. Calheiros, ―Modeling and simulation of scalable cloud computing Environments and the CloudSim Toolkit: challenges and opportunities□ 978-1-4244-4907-1/09, 2009 IEEE

[9] M. Sudha, Dr.Bandaru Rama Krishna Rao and M. Monica "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment" International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010

[10] Mr. D. Kishore Kumar, 2 Dr.G.Venkatewara Rao , 3 Dr.G.Srinivasa Rao "Cloud Computing: An Analysis of Its Challenges & Security Issues" International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 5, October 2012 www.ijcsn.org ISSN 2277-5420

[11] Cong Wang, Qian Wang and Kui Ren. ―Ensuring Data Storage Security in Cloud computing□ 978-1-4244-3876-1/2009 IEEE

[12] M. Vijayapriya, "Security Algorithm in Cloud Computing: Overview" International Journal of Computer Science & Engineering Technology (IJCSET) ISSN: 2229-3345 Vol. 4 No. 09 Sep 2013

[13] Bhaskar Prasad Rimal,Admela Jukan, Dimitrios Katsaros, Yves Goeleven, "Architectural Requirements for Cloud Computing Systems" An Enterprise Cloud Approach Grid Computing Conference, Future generation computer systems (Springer), 2011.

[14] Rohit Bhadauria, Sugata Sanyal "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques" International journal of computer applications volume 47-number 18 2012

[15] Mohit Marwaha1, Rajeev Bedi "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing "IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013

[16] Soeung-Kon(Victor) Ko1), Jung-Hoon Lee2), Sung Woo Kim3) "Mobile Cloud Computing Security Considerations" Journal of Security Engineering 2012

[17] D. Popa1 K. Boudaoud2 M. Cremene1 M. Borda "Overview on Mobile Cloud Computing Security Issues" Tom 58(72), Fascicola 1, 2013

[18] A. Cecil Donald, S. Arul Oli, L. Arockiam "Mobile Cloud Security Issues and Challenges: A Perspective" International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013

[19] Pragati Chavan, Rakesh Rajani "Mobile Cloud Computing for Cloud based application and services-Security Considerations" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 10, October – 2013

[20] Joshi Ashay Mukundrao "Enhancing Security in Cloud Computing" Information and Knowledge Management Vol 1, No.1, 2011