International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Architectures, Applications and Challenges of Cloud Computing-A study.

M.S.Kamal Joshi[1], MD.Juheb[2]

[1, 2] Dept. of Computer Science and Engineering, Veerappa Nisty *Engineering College, Shorapur, India*
[1]mskjoshi@gmail.com
[2]mdzohebahmed@gmail.com

Abstract— **cloud computing can be thought of has the next generation architecture of an IT enterprise. It is the evolution of Parallel computing, Distributed computing and Grid computing virtualization technologies which define the structure of modern era. In this paper, we explore the idea of various cloud architecture, applications, properties, advantages and limitations, and the challenges and issues related to cloud computing and we try to identify some solutions to the challenges and issues of cloud computing this area deserves substantial further research and investigation. However, security and privacy issues present strong barrier for user to adopt into cloud computing systems. In this paper we investigate several cloud computing system providers about their concerns on security and privacy issues. We present the possible architecture for privacy management of data in cloud computing.**

Index terms- cloud computing, architecture, challenges, data privacy and applications.

I. INTRODUCTION

Cloud computing is a latest technology in the field of computing. It is the further enhancement and development of grid computing, parallel computing and distributed computing. It is based on the concept of virtualization, utility computing, Infrastructure as a Service (IaaS), Platform as a Service (Paas), Software as a Service (Saas), Data as a Service (Daas) and Anything as a Service (Aaas). Cloud symbolizes the web as a space where the computing is preinstalled and exists as a service; Data, OS, Applications, storage and computing power exist on the web ready to be shared. To the users, cloud computing plans are Pay-as-you-go (or) Pay-Per-Use-On-Demand mode, which means you only have to pay for the advantages of your computing access i.e. shared IT resources includes network, server, storage, applications, services and so on.

II. ARCHITECTURE

Cloud computing mainly subcategorised as IaaS, SaaS and PaaS. Cloud computing needed to add more structure to the service model which are DaaS and AaaS [3, 4]. The originality and values of cloud computing comes from packaging and offering resources in an economically, scalable and flexible fashion that is affordable to technology. Cloud computing is naturally emerged and integrated in several fields. The following Fig 1[12] gives the conceptual architecture structure of cloud computing. We describe each service model in briefly as follows.

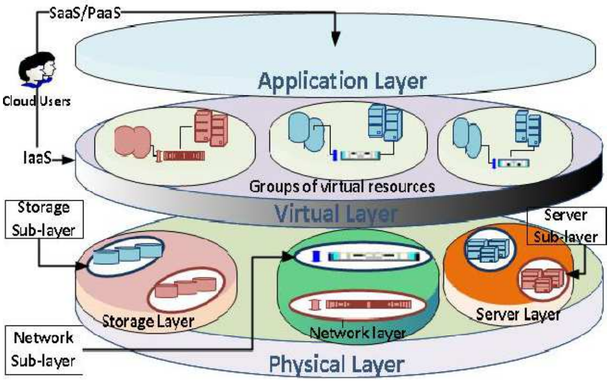

Fig 1: A conceptual model of cloud architecture

A. *Infrastructure as a Service (IaaS)*

The basic strategy of IaaS is virtualization of machines independently. Hardware resources (storage) computing power (i.e. CPU and Memory) are offered as a service to customers. This enables large companies to “rent out” these resources rather than spending money to buy servers and networking equipments. Often companies are billed for their usage following a Utility Computing model, where a usage resource is metered. IaaS allows application to scale in a horizontal manner where the load balancers distribute the workload equally in a common application. This enables flexibility scaling up (or) down amount of required resources on demand. This valuable feature is for companies on computing needs in demand. Examples of IaaS are Amazon offers S3 for storage, EC2 for Computing power, Microsoft, [2, 7, 8, 9, 10] etc.

B. *Platform as a Service(PaaS)*

This refers to providing facilities to support the entire application development lifecycle including design, implementation, debugging, testing, deployment, operations and support for Rich web applications and services on the internet. PaaS enables SaaS users to develop add-0ns and also develop standalone web based applications, reuse the other services and develop collaboratively in a team. Examples of PaaS are Microsoft Azure Services Platform, Google App engine, Salesforce.com, [8, 9, 10]etc.

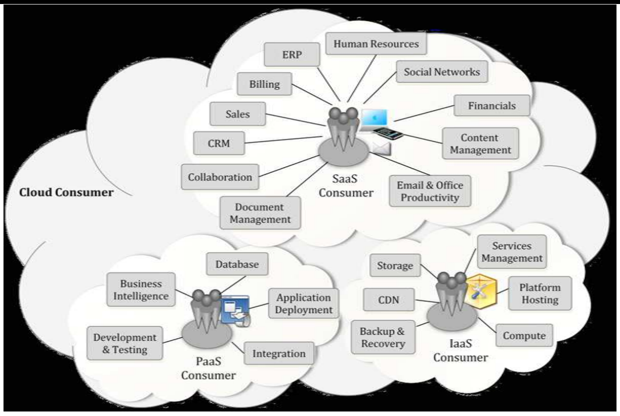

Fig 2 The Cloud Services to the Cloud Consumers

C. *Software as a Service(SaaS)*

Software applications are offered as a Service on the internet rather than software packages to be purchased by individuals as shown in fig 2. Web accessible software enables users to use programs or applications without having to download or install them on their machines. You no longer need to worry about expiration dates, downloading updates (or) installing software on multiple machines; Saas reduces the expenses by allowing you to rent a service and use only specific features rather than buying complete packages of programs. Examples of Saas are Google web-based office applications (word processor, spreadsheets), Microsoft online CRM and SharePoint, Salesforce.com [2, 8, 9, 10] etc.

D. *Data as a Service(DaaS)*

A more specialized type of storage, offering database capability as a service. It can be considered as a sub-organisation of IaaS, DaaS on the cloud often adopts a multi-tenant architecture, where the data of many users is kept in the same physical table. Each Daas provider also gives a query language to retrieve and manipulate data. Daas allows consumers to pay for what they are actually accessing instead paying for the site license for the entire database. Examples of DaaS are Amazon S3, Microsoft SSDS, Google Big Table, Apache HBase and Apache Pig [7, 8, 9] etc.

E. *Anything as a Service(AaaS)*

A most specialized type of SaaS which is to be adopted for particular special tasks. Now-a-days privacy is big concern in cloud computing for example a security service provider can be hired to protect the data in common cloud which is to payed by the clients. So, this field is required further investigation for advancement of services. An idea for developer to provide the special tasked application to the real world to get rid of the drawbacks of that any particular issues in cloud computing.

III. CLOUD CHALLENGES

In Privacy cloud related privacy, security, ownership and reliability issues.In Performance and QoS, Dynamic resource provisioning, Power efficiency. In Load Balancing application streaming, Cloud [Service Level Agreement]SLA`s.In Business Model and Pricing Policies the Cloud service subscription model , Cloud standardized SLA`s.In Managing applications in the clouds Mobile clouds, Roaming services in clouds and Agent Based cloud computing[13].The biggest concern about cloud computing are security and privacy. User might not be comfortable handing over their data to a third party. This is even greater challenge when it comes to companies that wish to keep their sensitive information on cloud computing. To[1,2,5] make their servers more secure, cloud service vendors have developed password protected accounts, security server through which all data being transferred must pass and data encryption techniques. After all, the success of a cloud service depends on its reputation and resulted in a loss of clients and business.Cloud computing, in which services are carried out on behalf of customers on hardware that the customers do not own or manage, is an increasingly fashionable business model. The input data for cloud services is uploaded by the user to the cloud, which means that they typically result in user’s data being present in unencrypted form on a machine that the user does not own or control. This arise some inherent privacy challenges. There[1,11] is a risk of data theft from machines in the cloud, by rogue employees of cloud service providers or by data thieves breaking into service providers machines, or even by other customers of the same service if there is inadequate separation of different customer’s data in a machine that they share in the cloud.

IV. PRIVACY MANAGER

Our contribution to addressing these problems is a Privacy Manager, which helps the user manage the privacy of their data in the cloud. As [1, 11] a first line of defense, the privacy manager uses a feature called *obfuscation*, where this is possible. The idea is that instead of being present unencrypted in the cloud, the user’s private data is sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The result of the processing is de-obfuscated by the privacy manager to reveal the correct result. The obfuscation method uses a key which is chosen by the user and known by the privacy manager, but which is not communicated to the service provider. Thus the service provider is not able to de-obfuscate the user’s data, and this data is not present on the service provider’s machines, reducing (or even eliminating) the risks of theft of this data from the cloud and unauthorized uses of this data. Where obfuscation is practical, the principle of data minimization gives a legal impetus to use it. However, it is not practical for all cloud applications to work with obfuscated data. For applications for which users have to upload some private data to the cloud, the privacy manager contains two additional features, called *preferences* and *personae*, which help the users to communicate to service providers their wishes for the use of this personal data, and thus assist the service providers to respect privacy laws requiring users’ consent.

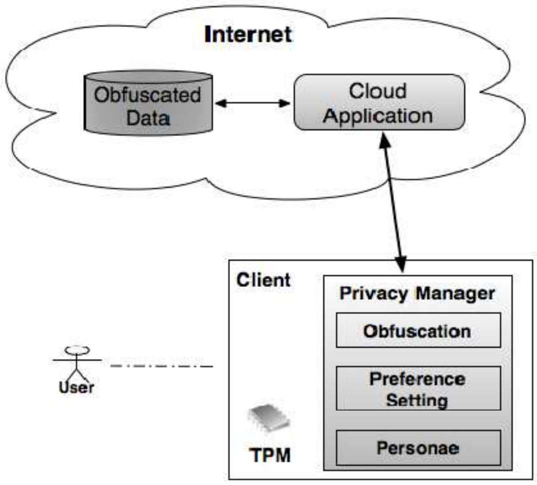

Fig. 3 Client based privacy manager

The preferences feature allows users to set their preferences about the handling of personal data that is stored in an obfuscated form in the cloud. The persona feature allows the user to choose between multiple personae when interacting with cloud services. In some contexts a user might want to be anonymous, and in others he might wish for partial or full disclosure of his identity. The overall architecture of our solution is illustrated in Fig 3[11]. Privacy Manager Software on the client helps users to protect their privacy when accessing cloud services. Privacy Manager in a Hybrid Cloud as an alternative, as illustrated in Fig 4, the Privacy Manager may be deployed in a local network, or a private cloud, to protect information relating to multiple parties. This would be suitable in environments, such as enterprise environments, where local protection of information is controlled in an adequate manner and its principal use would be to control personal information passing to a public cloud. The Privacy Manager can itself be virtualized within the internal cloud. Note that the TPM could also be virtualized, within the private cloud.

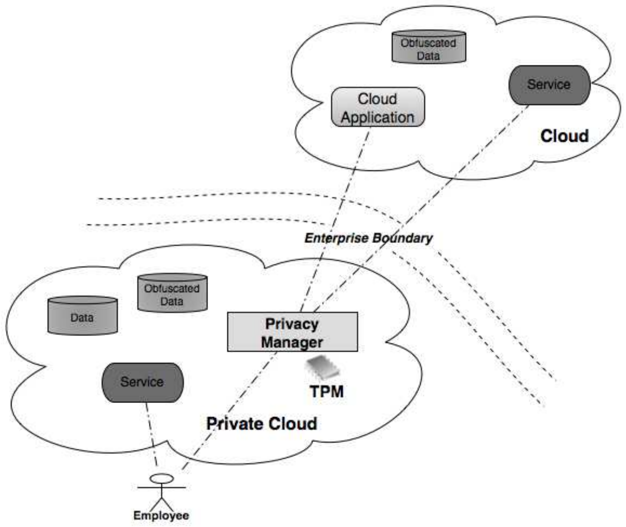

Fig 4 Privacy manager for enterprise

A central feature of the Privacy Manager is that it can provide *obfuscation and de-obfuscation service*, to reduce the amount of sensitive information held within the cloud. Trusted computing solutions, like those being developed by the Trusted Computing Group (TCG)[11], can address the lower-level protection of data, and this can be exploited in our solution. The TCG is an organization set up to design and develop specifications for computing platforms that create a foundation of trust for software processes, based on a small amount of extra hardware called a Trusted Platform Module (TPM). This tamper-resistant hardware component within a machine acts as a root of trust. In the longer term, as specified by TCG, trusted computing will provide cryptographic functionality, hardware-based protected storage of secrets, platform attestation and mechanisms for secure boot and integrity checking.

Advantages to this approach include that the benefits of the cloud can be reaped within the private cloud, including the most efficient provision of the Privacy Manager functionality. It can provide enterprise control over dissemination of sensitive information, and local compliance. A significant issue however is scalability, in the sense that the Privacy Manager might slow down traffic, provide a bottleneck and may not be able to adequately manage information exposed between composed services. There are various different options with respect to this type of architecture. For example, the proxy capability could be combined, even in a distributed way, with other functionalities, including identity management. Another example is that trusted virtual machines could be used within the privacy cloud to support strong enforcement of integrity and security policy controls over a virtual entity (a guest operating system or virtual appliance running on a virtualized platform). It would be possible to define within the Privacy Manager different personae corresponding to different groups of cloud services, using different virtualized environments on each end user device. In this way, virtualization is used to push control from the cloud back to the client platform. As with the previous architecture, there could be mutual attestation of the platforms, including integrity checking [11].

The aim of obfuscation is to solve the following general problem. A user has private data *x*. He wishes to carry out some communication protocol with a service provider, which will enable him to learn the result of some function *f* on *x*, without revealing *x* to the service provider. (The function *f* may itself depend on some data known to the service provider but not to the user, and on some data supplied by the user which is not private).If the user and service provider are both willing to use whatever protocol will solve the problem, and have sufficient computing power and storage to do so, Yao's protocol for secure two-party computation [14] solves this problem for any *f* which can be expressed as a circuit.. In fact, Yao's protocol can be used to ensure that the service provider learns no information at all about *x*. Yao's protocol requires several rounds of interactions between the user and service provider, which depend on the choice of *f*. Gentry [14] has recently removed this requirement for interaction by constructing a remarkable encryption scheme which allows the service provider to calculate the encrypted value of *f*(*x*) given the encrypted value of *x*, for *any f* which can be expressed as a circuit, while also ensuring that the service

Provider learns no information about *x*. Gentry's encryption scheme improves on prior work on homomorphic encryption, e.g. [15].However, there are two problems with applying these solutions in cloud computing. The first is efficiency. Gentry's full scheme is impractical due to its rather high computational complexity. Although there has been a body of work improving the efficiency of Yao's protocol and related secure

Computation techniques such as privacy-preserving data mining [14, 15], when the input data *x* is large these methods can still require a large amount of storage or computation on the part of the user. One of the attractions of cloud computing is that it can enable users to process or store large amounts of data at times of peak demand without having large amounts of computing resources in-house. The other problem is that cloud computing providers may not be willing to rewrite their applications. If this is the case, the user has to calculate *f*(*x*) using only the functions provided by the service, which in this section are denoted *f*1… *fn*. The set of functions *f* for which it is possible to do this without revealing *x* to the service provider depends on *f*1… *fn* and on the extent of the user's computing resources. For some specialized cloud computing services, only one function is provided, which will typically be a Map Reduce-style function [16]. If the input data is a large data set; some more generic services offer full SQL SELECT functionality [17].The requirement that we make of obfuscation in this paper is only that it is difficult for the service provider to determine *x* given the obfuscated data. It may be that the service provider can easily obtain some information about *x*, but not enough to determine *x*. As a different example of obfuscation methods that allow some but not all information about the input data to be learned from the obfuscated data, Narayanan and Shmatikov [18] describe an obfuscation method which allows individual records to be retrieved from an obfuscated database by anyone who can specify them precisely, while making "mass harvesting" queries matching a large number of records computationally infeasible. As remarked in [18], there is a tension between the strict security definitions and loose notions of efficiency used by the cryptography community, and the strict efficiency requirements but loose security requirements of the database community. Like the database community we prioritize efficiency over strength of the security definition, as it is essential for us that the privacy manager be practical and scalable to implement.

The user interface for the privacy manager is shown in Fig 3. The end user selects the pictures that will be shared through certain cloud services. Specific personae, e.g. family, business, anonymous etc, will be applied to obfuscate certain attributes associated with the photos. The user can also customise the personae (i.e. choosing attributes to be obfuscated using certain obfuscation methods) by changing the default setting through privacy personae configuration window. By using the Privacy Manager, only the owner has the control to the attributes and the underlying obfuscation methods are transparent to the end users. Nevertheless, this method will not affect photo quality and still allows the photos to be further encrypted.

V. APPLICATIONS

Flexibility

The second a company needs more bandwidth than usual, a cloud-based service can instantly meet the demand because of the vast capacity of the service's remote servers. In[6] fact, this flexibility is so crucial that 65% of respondents to an InformationWeek survey said the ability to quickly meet business demands was an important reason to move to cloud computing.

Disaster recovery

When companies start relying on cloud-based services, they no longer need complex disaster recovery plans. Cloud computing providers take care of most issues, and they do it faster. That business which used the cloud were able to resolve issues in an average of 2.1 hours, nearly four times faster than businesses that didn't use the cloud (8 hours). The same study found that mid-sized businesses had the best recovery times of all, taking almost half the time of larger companies to recover.

Capital-Expenditure Free

Cloud computing services are typically pay as you go, so there's no need for capital expenditure at all. And because cloud computing is much faster to deploy, businesses have minimal project start-up costs and predictable ongoing operating expenses [2].

Work from anywhere

As long as employees have internet access, they can work from anywhere. This flexibility positively affects knowledge workers' work-life balance and productivity. One [2] study found that 42% of working adults would give up some of their salary if they could telecommute, and on average they would take a 6% pay cut.

Increased collaboration

Cloud computing increases collaboration by allowing all employees – wherever they are – to sync up and work on documents and shared apps simultaneously, and follow colleagues and records to receive critical updates in real time. A survey by Frost & Sullivan found that companies which invested in collaboration technology had a 400% return on investment [3].

Document control

According to one study, 73% of knowledge workers collaborate with people in different time zones and regions at

least monthly. If a company doesn't use the cloud, workers have to send files back and forth over email, meaning only one person can work on a file at a time and the same document has tones of names and formats. Cloud computing keeps all the files in one central location, and everyone works off of one central copy. Employees can even chat to each other whilst making changes together. This whole process makes collaboration stronger, which increases efficiency and improves a company's bottom line[5].

Security

Some 800,000 laptops are lost each year in airports alone. This can have some serious monetary implications, but when everything is stored in the cloud, data can still be accessed no matter what happens to a machine [6].

Competitiveness

The cloud grants SMEs access to enterprise-class technology. It also allows smaller businesses to act faster than big, established competitors. A study on disaster recovery eventually concluded that companies that didn't use the cloud had to rely on tape backup methods and complicated procedures to recover slow, laborious things which cloud users simply don't use, allowing us to once again to fetch our data [2].

Environmentally friendly

Businesses using cloud computing only use the server space they need, which decreases their carbon footprint. Using the cloud results in at least 30% less energy consumption and carbon emissions than using on-site servers. And again, SMEs get the most benefit: for small companies, the cut in energy use and carbon emissions is likely to be 90% [2].

VI. CONCLUSION

This paper discussed about the basic architecture and services of cloud computing and a vision of advancement in service model which is to be further investigated at both individual and enterprise levels. And the challenging concerns which can be overcome by the privacy manager as a solution to privacy issues. Finally few applications of cloud computing results in the migration of computing world to cloud computing. It could be the next generation's era for peak computing needs in short span of time frames.

REFERENCES

[1] Pearson, S. (Ed.): Trusted Computing Platforms. Prentice Hall (2002).

[2] Intelligent computing chip insider "Your Life in the Cloud" May 2011.

[3] Developer IQ vol. 11| No.7 July 2011.

[4] International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012.

[5] J.F.Yang and Z.B.chen,"Cloud Computing Research and security Issue", 2010 IEEE International Conference on Computational Intelligence and Software Engineering (CiSE), wuhanpp.1-3, DOI=10-12 Dec.2010.

[6] http://www.salesforce.com/uk/socialsuccess/cloud-computing/why-move-to-cloud-benefits-cloud-computing.jsp

[7] http://www.amazon.com

[8] http://www.microsoft.com/azure/data

[9] http://www.code.google.com/appengine

[10] http://www.salesforce.com/paas

[11] Trusted Computing Group: Trusted Platform Module (TPM) Specifications. https://www.trustedcomputinggroup.org/specs/TPM/ (2009).

[12] National Institute of Standards and Technology Special Publication 500-292 Natl. Inst. Stand. Technol. Spec. Publ. 500-292, 35 pages (September 2011).

[13] http://www.iaria.org/conferences2013/cloudcomputing13.html

[14] Boneh, D., Goh, E-J. Nissim, K.: Evaluating 2-DNF formulas on ciphertexts.

[15] Lindell, Y., Pinkas, B.: Privacy Preserving Data Mining. J. Cryptology 15(3), 151—222 (2011) .

[16] http://www.cs.umbc.edu/~kunliu1/research/privacy_review.html.

[17] Date, C.J.: A guide to the SQL standard.

Narayanan, A, Shmatikov. V.: Obfuscated Databases and Group Privacy. Proceedings of the 12th ACM conference on Computer and Communications Security, pages 102—111.