Privacy Concerns Impact in Cloud Computing Environment

Rupal Yadav
M.Tech Scholar
Dept: CSE
TIEIT, Bhopal, M.P.

Kaptan Singh
Professor
Dept: CSE
TIEIT, Bhopal, M.P.

Amit Saxena
Head of Department
Dept: CSE
TIEIT, Bhopal, M.P.

ABSTRACT
'Cloud' is a generic term for a large variety of innovations and opportunities. This isn't development, but rather a "practical breakthrough," incorporating a variety of previous innovations into anything unique and informative. Cloud storage applies to the delivery of on-demand computing resources via a cloud network, such as software, repositories, file services, emails, etc. Both information and apps are completely contained on the user's device in the conventional computing system. In cloud services, the customer's machine may contain almost no technology or information (maybe just a simple operating system and a web browser), serving as nothing more than a display interface for operations that take place far away on a communications network. Cloud computing is a paradigm that provides fast, on-demand access to a separate fund of customizable computer resources (e.g. routers, databases, memory, software, and facilities) that can be quickly distributed and distributed with minimal effort to manage or interact with service providers. Cloud computing offers computing, technology, access to data, and space resources which do not involvemiddle-user understanding of the physical location and configuration of the computers delivering the services. Parallels to this conceptcan be taken from the power grid, where middle-users burn fuel without understanding the components or resources required to deliver the service.

For project work, a safety system with authentication will be put in place. The proposed solution will bring the RC6 & AES Cryptography Authentication Function. Subsequently, an authentication table may also be set up towards the end of the application server to ensure that the user can access what they want.

Keywords
Cloud, Cloud Computing, Computer Network, authentication, RC6, AES algorithm.

1. INTRODUCTION
Cloud Computing holds vast amounts of data for various users. It can be described as the provision of various services over the Network on a pay-as-you-gobasis. These facilities provide data storage, infrastructure, networking and applications. And the facilities can be both private and public.
Example:

Cloud computing makes it possible for patients, physicians and supervisors to access information from anywhere. This also prevents expenses byallowing massive data files to be exchanged instantly for full convenience. This is a big boost to success.

In the end, cloud computing ensures that patients get the best treatment possible without unnecessary delay. The status of the patient can also be changed in seconds by video conferencing.

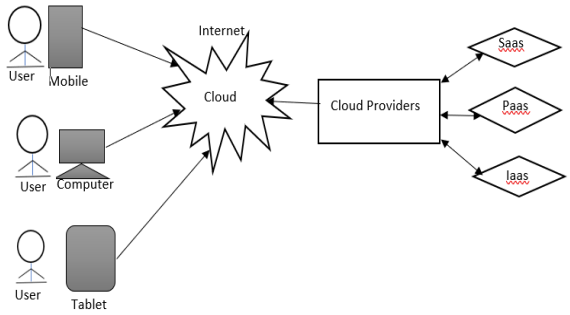

Fig. 1: Cloud Computing

1.1 Evolution of Cloud Computing:

YEAR	DESCRIPTION
2014	Estimated global cloud spending.
2013	The largest demand for public cloud services.
2010	The one server field service managementsoftware moves top of the cloud.
2008-2009	Google App
2006	Amazon launches Elastic computing cloud (EC2), Simple Storage Services(S3).
2002	Launches Amazon Web Services
1999	Sales Force
1997	Cloud Computing is defined by Prof. RamnathChellappa
1970	Virtualization Software launched
1969	ARPNET by J.C.R. Licklider
1960	John McCarthy introduces mainframes timesharing

1.2 Why Cloud Computing?
Cloud computing effectively harnesses small firms with limited resources, allowing new enterprises access to technology that previously was o n n dut of control. Cloud computing helps small firms make the most of converting their maintenance costs.

You have to pay a great deal of attention on an in-house IT server to make sure there are no flaws in the system so it runs smoothly.

And you are completely responsible in case of any technical failure; it will be looking for a lot of care, time and money to fix it. Whereas in cloud computing the service provider takes full responsibility for the uncertainty and technological shortcomings.

Now here the comparison between personal system and cloud computing:

Personal System/Single Organization	**Cloud Computing**
It gives higher pay and less scalability.	Pay for what you use.
It allot huge space for servers.	There are no space for servers.
There are no automatic updates.	There are automatic updates for software.
It appoint team for software and hardware maintenance.	There are no team for software and hardware maintenance.
There are lack of flexibility.	There are high flexibility.
Data can't be accessed remotely.	Data can be accessed and shared anywhere over the internet.
It takes longer implementation time.	It does not take longer time for implementation.
Poor data security.	Better data security.

Data security is a major concern in the cloud because all data is transmitted via the internet. The data must be stored in an encrypted form in the cloud. This constrains the client form directly accessing the shared data. For this reason, it is appropriate to employ proxy and brokerage services. Encryption helps protect the data transferred and the data stored in the cloud as well. Encryption also helps protect data from unauthorized access but does not prevent loss of data.

Let's discuss some violations of security in the past:

- LinkedIn faced cyber attack in 2012, 6.5M login id and passwords were hacked from linkedIn database and published to public site.
- Sony also faced the most violent hacking assault in a record, when hackers reported openly in their economic and film ventures.
- iCloud faced similar attack where in private images of clients from their database were made public.

2. LITERATURE RIVIEW

The cloud computing infrastructure can provide easy consumer support for both computer hardware and software resources.

There are four types of service available on cloud services.

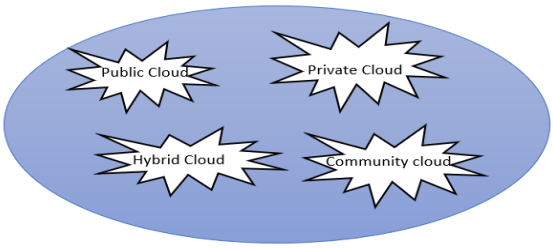

Fig.2 : Deployment Models in cloud

2.1 Public Cloud Model

Public cloud easily access to general public. It can access everywhere that's why it is less secure. This may be available on a pay-per-use basis or free of charge. Technically, there may be little or no difference between public and private cloud infrastructure, but perception of security may be substantially different for services (applications, storage, and other resources) that are made available to a public audience by a service provider, and when communications are made over an untrusted network.

2.2 Private Cloud Model

Personal access to the cloud within an organization. It's safer because it's private. A private cloud is a web service that is run entirely by a single entity, either internally or through a third party and is hosted internally or externally.

2.3 Hybrid Cloud Model

Hybrid cloud is a combination of private and public cloud that remains separate entities but are connected together, offering the advantages of multiple deployment models.

2.4 Community Cloud Model

Team cloud access within the organisation's community. Community cloud access within group of organization. Community clouds are often built for companies and organizations collaborating on joint projects, applications or research needing a central cloud computing facility to develop, administer and execute these projects, irrespective of the leased solution.

1.	Cloud Security Ecosystem for Data Security and Privacy	Akshay Arora, AnmolRastogi, Abhirup Khanna, Amit Agrawal	IEEE	2017	The research focuses on building a stable cloud environment in which we use multifactor authentication along with multiple hashing and encryption rates. Along with the algorithm, the suggested program is simulated using the CloudSim simulator. To that end, along with the simulated tests, we explain the workings of our proposed program.	Problem is these services could be easily accessed via smartphones with rapid technological advances, enabling users to exchange pictures, video, documents and other essential data on a real-	We propose in this paper a Hybrid Cryptographic System (HCS) that incorporates the advantages of both symmetric and asymmetric encryption.

						time basis across different platforms.	
2.	Measuring Data Security for a Cloud Computing Service	Rizwana A.R. Shaikh, Masooda M. Modak	IEEE	2017	The security and privacy of cloud computing data is also an area of concern for cloud users and providers. The identity of the customer, passwords and data protection etc. are some of the things that the customer has to ensure that the provider has full control.	Main security issues in cloud computing are data protection concerns including data confidentiality, privacy, and availability.	A data security assessment framework is introduced here that will be used to measure the data protection of cloud computing.
3.	Critical Security Issues in Cloud Computing: A Survey	Xiaotong Sun	IEEE	2018	A survey was conducted among this paper to review all crucial aspects of cloud computing's security. Three sections of the integration were coordinated, which were computer security, network protection, and information security.	Cloud computing security issues arising from both insider and outsider attacks.	This paper offers X-as-a Service (XaaS), and allows versatile on-demand adoptions. Cloud computing still poses a host of security issues
4.	Data Recovery and Security in Cloud	JayachanderSurbiryala, ChunmingRong	IEEE	2018	Data recovery is one of the main principles when dealing with storage devices that are essentially the cornerstone of cloud infrastructure. Anyone with access to these servers or devices can use data recovery techniques to retrieve customer confidential data after customers have deleted their private or confidential data from the cloud.	Data recovery creates issues of trust between providers and consumers of cloud services.	We introduced a simple mechanism for securing cloud customer data until the data is used in a cloud environment.
5.	Study on Data Security Policy Based On Cloud Storage	DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan	IEEE	2017	Safety in cloud storage includes data protection for the customer. The aim of this paper is to achieve cloud storage data protection and formulate the correct security policy for cloud storage.	Data security is an important issue for cloud storage technologies to tackle as a matter of urgency.	Cloud storage technology uses server, network or distributed file systems, etc.
6.	Security Pattern for Cloud SaaS: from system and data security to privacy	BojanSpasic, AnnandaTh RATH, Philippe Thiren,	IEEE	2018	The cloud, and the versatility it offers, is fast becoming a popular SaaS platform, a common model of software delivery. Cloud has many benefits, such as greater flexibility, no maintenance, quick access and fast knowledge sharing	There are many concerns surrounding issues such as system protection, protection of communication, data security, latency and availability. And when designing and developing the cloud SaaS framework, these security concerns need	We are discussing the protection pattern for Cloud SaaS in this paper. We are focusing on patterns covering different protection aspects, from device and data security to privacy.

						to be tackled to provide security enforcement and safe environment for users using cloud SaaS.	

3. SERVICE MODELS

Service Models of cloud computing are divided into three parts. A final user layer that encapsulates a customer viewpoint on cloud services completes these business models or layer.

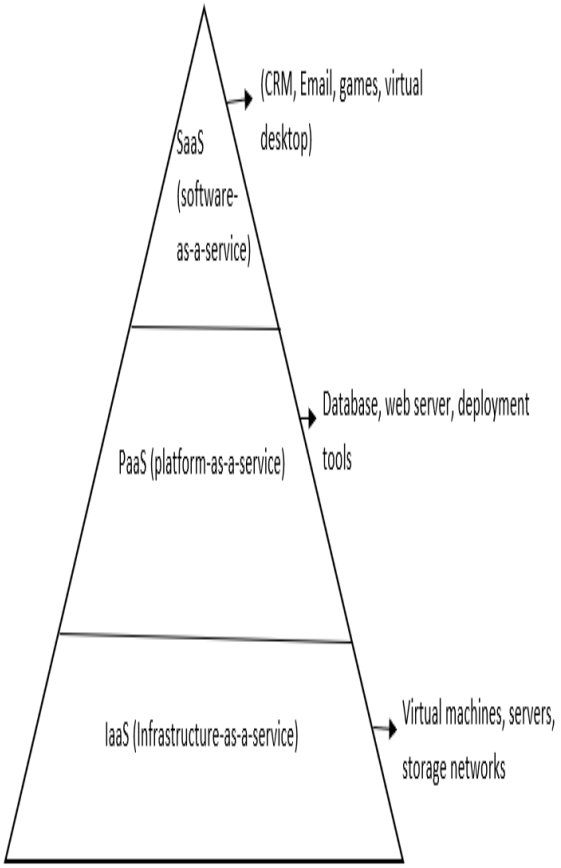

Fig.3: Service Models of Cloud Computing

2.1 Infrastructure-as-a-service (IaaS):

It is one of the core cloud computing service model next to Platform as a Business.It provides access to fundamental resources such as physical machine, virtual machine and so on.

2.2 Platform-as-a-service (PaaS):

It is one of the cloud computing services model. It provides forum to software-as-a-service (SaaS). It includes software support and management services, storage, networking, uploading, monitoring, partnering, hosting and maintenance of applications. It is a middleware, creator.

2.3 Software-as-a-service (SaaS):

It is one of the Cloud Computing cloud service model. It is a software distribution model in which application hosted by vendor or service provider and made available to customer over a network typically the internet. There are some SaaS application which are as follows:

- Billing and invoicing system.
- Customer Relationship Management.
- Human Resource Management.
- Help desk application.

3 EXISTING WORK

Mobile networking device characters are wired network settings that use laptops, terminals, etc. Wireless network networks use cell phones or any other apps. Nowadays, many consumers have PCs, tablets, cell phones, and other apps. And they all have nomadic and cooperative ability activity. Therefore, future networking infrastructure wants to support wireless communication environments and capabilities.

4 PROBLEM DOMAIN

Information security is a major concern in the cloud because all information is distributed over the Cloud. The information should be encrypted by default in plaintext. It prevents the application process from directly accessing the shared data. It is also necessary to hire proxy and brokerage services. Authentication allows us to encrypt the data transmitted and the data stored in the cloud. Encryption also helps to shield information from identity fraud but does not avoid data loss.

In security planning, there is a need to analyze various aspects of services before implementing a particular cloud resource as follows:

- Pick tool that needs moving into the cloud and investigate its chance of vulnerability.
- Cloud software templates, that is. IaaS, PaaS, and SaaS need to be considered for protection at various rates of operation.
- We also need to understand the types of cloud, i.e. public, private, community, hybrid.
- The risk generally depends on the types of software and service models in a cloud implementation.

Jin-Mook Kim and Jeong-KyungMoon have proposed a RADIUS system composed of several modules to accomplish a protected authentication requirement in order to solve the above-listed problems. RADIUS is a well-integrated computing system, but still has some scope for improvement:

1. It uses IDEA which is an algorithm of 256 bit symmetric key which not only increases the overhead encryption but also decryption.
2. Cell phone or third party device is not involved for runtime & human authentication.
3. OTT generation doesn't have a special algorithm.
4. There is no Access Control Mechanism.

5 CONCLUSION

AS we know cloud computing is crucial for security. There are so many services like software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS). These services have their own functionality. PaaS is used to reduce needs for system administration. And most important there are so many algorithms for security like RSA, Diffies Hellman, and so on.

6 REFERENCES

[1] Jin-Mook Kim and Jeong-KyungMoon,"*Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments*" published in International Journal od Distributed Sensor Networks by Hindwai Publication Corporation. Volume-1, 2014.

[2] Anurag Jain, Dr. Rajneesh Kumar "Confidentiality Enhanced Security Model for Cloud Environment" ICTCS '16, March 04-05, 2016, Udaipur, India

[3] NasrinKhanezaei, ZurinaMohdHanapi "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia

[4] Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering.

[5] BokefodeJayant D, UbaleSwapnaja A, PingaleSubhash V, KarandeKailash J., ApateSulabha S., "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model" International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015

[6] Cindhamani.J, NaguboyniaPunya, RashaEalaruvi, L.D. Dhineshbabu "An enhanced data security and trust management enabled framework for cloud computing systems" IEEE 5th International Conference on Computing, Communications and Networking Technologies July 11-13, 2014, Hefei, China

[7] Shilpi Singh, Vinod Kumar "Secured User's Authentication and Private Data Storage- Access Scheme in Cloud Computing Using Elliptic Curve Cryptography" 2015 IEEE 2nd International Conference on Computing for Sustainable Global Development.

[8] KawserWazedNafi, TonnyShekhaKar, SayedAnisulHoque, Dr. M. M. A Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012

[9] Garrison, G., Kim, S., Wakefield, R.L.: Success Factors for Deploying Cloud Computing. Commun. ACM. 55, 62–68 (2012).

[10] Herhalt, J., Cochrane, K.: Exploring the Cloud: A Global Study of Governments' Adoption of Cloud (2012).

[11] Sales force, ―CRM‖,http://www.salesforce.com/.

[12] Venters, W., Whitley, E.A.: A Critical Review of Cloud Computing: Researching Desires and Realities. J. Inf. Technol. 27, 179–197 (2012).

[13] Yang, H., Tate, M.: A Descriptive Literature Review and Classification of Cloud Computing Research. Commun. Assoc. Inf. Syst. 31 (2012).

[14] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A.: Cloud computing — The Business Perspective. Decis. Support Syst. 51, 176–189 (2011).