Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

Public Key Encryption algorithms Enabling Efficiency Using SaaS in Cloud Computing

J.Purna Prakash[1] , G.Komala[2], A . Poorna Chandra Reddy[3]

[1,2]Assistant Professor, [3]Associate Professor
[1,2,3]Department of Computer Science and Engineering
ChristuJyoti Institute of Technology & Science
Jangaon, Warangal, Telangana State, India

Abstract—The Most great challenging in Cloud computing is Security. Here Security plays key role in this paper proposed concept mainly deals with security at the end user access. While coming to the end user access that are connected through the public networks. Here the end user wants to access his application or services protected by the unauthorized persons. In this area if we want to apply encryption or decryption methods such as RSA, 3DES, MD5, Blow fish. Etc.,

Whereas we can utilize these services at the end user access in cloud computing. Here there is problem of encryption and decryption of the messages, services and applications. They are is lot of time to take encrypt as well as decrypt and more number of processing capabilities are needed to use the mechanism. For that problem we are introducing to use of cloud computing in SaaS model. i.e., scalable is applicable in this area so whenever it requires we can utilize the SaaS model.

In Cloud computing use of computing resources (hardware and software) that are delivered as a service over Internet network. In advance earlier there is problem of using key size in various algorithm like 64 bit it take some long period to encrypt the data.

Keywords: SaaS, Public Key Encryption, Encryption Devices,Scalable, Secure algorithms.

I. INTRODUCTION

Global presence of the Internet and the introduction of the wireless networking and mobile devices that is always feature in Internet connectivity. Utilization demands for services from the Internet. However, the architectures required by service providers to enable Web 2.0 have created an IT service that is differentiated by its resilience, scalability, reusability, interoperability, security, and open platform development. This has effectively become the backbone of Cloud Computing and is considered by a number of vendors and services to be an operating system layer of its own (CPNI, Centre for the Protection of National Infrastructure).

Cloud Computing appears as both a computational model or paradigm and distribution architecture, and its principalobjective is to provide secure, quick, convenient data storage, and net computing services, with all computing resources being visualized as services and delivered via the Internet. The Cloud enhances collaboration, agility, scaling, and availability, the ability to scale to fluctuations according to demand and accelerate development work, and provides the potential for cost reduction through optimized and efficient computing. As cloud computing is an Internet based computer technology. Some of the major firms like Amazon, Microsoft and Google have implemented the "CLOUD" and have been using it to speed up their business. Cloud computing has given a new

dimension to the complete outsourcing arena (SaaS, PaaS and IaaS) and they provide ever cheaper powerful processor with these computing architecture. The cloud infrastructures are much more powerful and reliable than personal computing devices, broad range of both internal and external threats for data integrity still exist. Examples of outages and data loss incidents of noteworthy cloud storage services appear from time to time [2].

In order to achieve the assurances of the cloud data integrity and availability and enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users. YouTube, Facebook, Zoho, Go To Meetingsin this paper the main contribution as follows:

- It compared too many end user applications.
- Providing the secure and dynamic operation (i.e., insert, append, modify and delete) on data blocks.
- The security and performance analysis shows the proposed design is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

The rest of the paper is organized as follows: Section II introduces the system model, and design goals, Section III provides dynamic data operation support, , Section IV providing the detailed description of the scheme end user access through Section V provides the standard for security access issues, section VI performance analysis, and Section VII gives the concluding of the paper.

II. PROBLEM STATEMENT

1. System Model

In the network architecture for cloud storage service having three different network entities are follows:

- *User:* User is an entity or a person or an organization who having the data to be stored in the cloud server and rely on the cloud for data computation.
- *Cloud Server Provider*: CSP is an entity, to provide data storage service and has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.
- *Third Party Auditor*: TPA who has expertise and capabilities that user may not have trusted to assess and expose the risk of the cloud storage service.

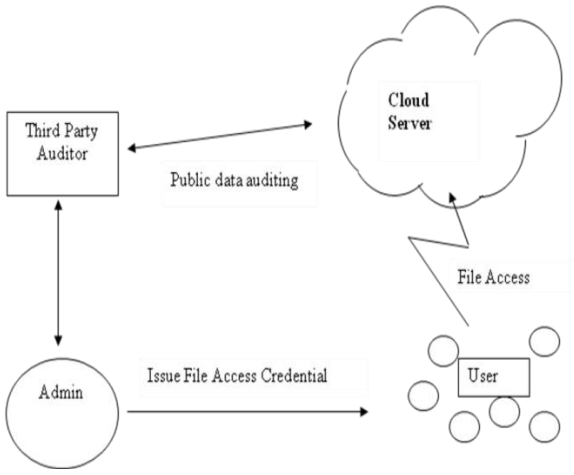

Figure. 1: Cloud storage service architecture

In the cloud data storage, a user stores his data through the cloud service provider into a set of the cloud servers. The cloud servers run on the distributed system. Data redundancy can be applied with technique of erasure correcting code to further tolerate faults or server crash as users grows in size. By using application, the user interacts with cloud server via cloud service provider to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations are considering are block revise, erase, insert and affix [3].

As above mentioned diagram the security problem occurs in third party to user access through cloud server regarding this at the end user access we have to implement different aspects to use our existed algorithms in effective. A normal small company can use high level data secure methods by using large keys towards in algorithms. The algorithms limitations will be taken place again do to in excellent manner. Whereas earlier if we want to use algorithms like this, there is problem of using processing capabilities to encrypt our data.

2. Design Goals

To make sure the security and dependability for data storage in cloud under the aforementioned antagonist model, we aim to design efficient mechanisms for dynamic data verification and operation and achieve the following goals:

I. *Storage accuracy*: to ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.
II. *Fast access of user*: to effectively locate the mal- functioning server when data access has been detected.
III. *Dynamic data support*: to maintain the same level of storage correctness assurance even if users modify, erase or affix their data files in the cloud.

III. PROVIDING DYNAMIC DATA OPERATION SUPPORT

So far, we assumed that U represents User access data. However, in cloud data storage, there are many potential scenarios where data stored in the cloud is dynamic, like electronic documents, photos, or log files etc. Therefore, it is crucial to consider the dynamic case, where a user may wish to perform various block-level operations of revise, erase and affix to modify the data file while maintaining the storage correctness assurance. The straightforward and insignificant way to support these operations is for user to download all the data from the cloud servers and re-compute the whole parity blocks as well as verification tokens. This would clearly be highly inefficient. In this section, we will show how our scheme can unambiguously and efficiently handle dynamic data operations for cloud data storage.

Revise Operation In cloud data storage, sometimes the user may need to modify some data block(s) stored in the cloud, from its current value f to a new one. We refer to this operation as data revise.

An affix operation to the user access file refers to an affix operation at the desired index position while maintaining the same user access as with standard security issues not in depth. Therefore, an efficient affix operation is more on standard security issues in dearth difficult to support and thus we leave it for our future work.

IV. END USER ACCESS THROUGH

Innovation behind the success of cloud services ultimately depends on the acceptance of the offering by the user community. Acceptance of an offering by users changes the economics considerably. As more users embrace such innovation, economies of scale for a product allow implementers to lower the costs, removing a barrier to entry and enabling even more widespread adoption of the innovation. In this session, we will present some of the applications that are proving beneficial to end users, enabling them to be "power collaborators." We will take a look at some of the most popular Software-as-a-Service (SaaS) [2],[1] offerings for consumers and provide an overview of their benefits and why, in our opinion, they are helping to evolve our common understanding of what collaboration and mobility will ultimately mean in our daily lives.

a) YouTube

YouTube is the leader in online video, and a premier destination to watch and share original videos worldwide across the Internet through web sites, mobile devices, blogs, and email. YouTube allows

people to easily upload and share video clips on the YouTube web site.2 Figure shows YouTube's home page.

.

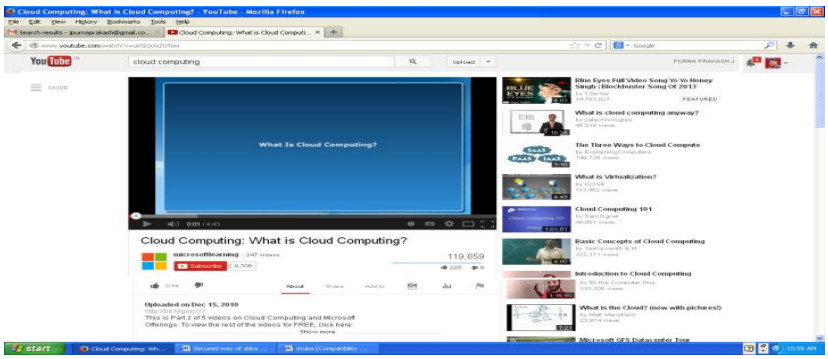

Figure2. YouTube Website

Figure 3. Facebook website

By simply configuring some basic settings for the player interface, you can build a highly customized player control. The player APIs provide mechanisms that enable you to control how YouTube videos will look on your site [4].

It is important to distinguish between the two types of players, the normal "embedded" player you most likely have already seen on the Internet, and a second, chrome less player, which is just a video box w_ controls. The chrome less player is intended to be implemented by experienced web programmers who want to design a customized video player for their users. Both players have the same API, which is exposed via JavaScript and/or Action Script. The following sections discuss each option in further detail.

b) Facebook

The Facebook web site currently has more than 175 million active users worldwide. Users can join networks organized by city, workplace, school, and region to connect and interact with other people. People can also add friends and send them messages, and update their personal profiles to notify friends about themselves. The web site's name refers to the paper Facebook depicting members' of a campus community that some U.S. colleges and preparatory schools give to incoming students, faculty, and staff as a way to get to know other people on campus[12][2].

Facebook serves up over 50 billion page views a month while employing fewer than 200 engineers.

It is the second most-trafficked PHP hypertext preprocessor site in the world (Yahoo is number 1), and it is one of the world's largest MySQL installations, running thousands of databases. In terms of total photo page views, Facebook exceeds all of the next-largest photo sites combined. It is the largest photo-sharing site in the United States, with over a billion photos. Facebook is the fourth most-trafficked web site in the United States, and Facebook users upload more than 14 million new photos every day show in Figure 3.

c) ZOHO

Zoho is an office productivity suite from AdventNet, Inc., which was founded in 1996. The Zoho product is supported by over 120 developers. To date, Zoho has launched 15 different applications, and more are in the works. When you first go to the Zoho web site, you see the page shown in

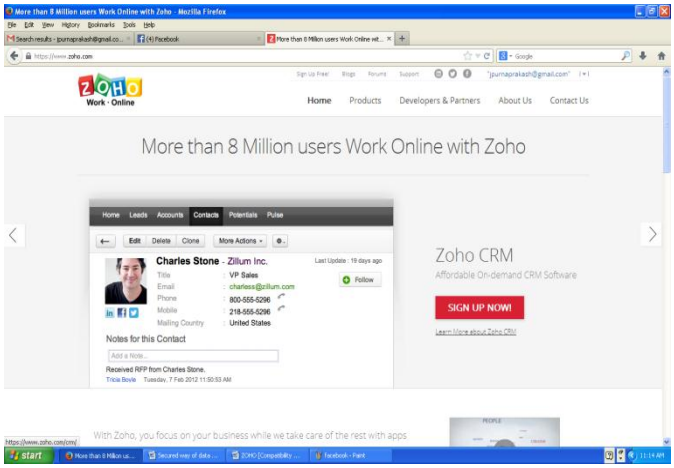

Figure 4. Zoho website

Zoho Mail provides ample storage space. You can store and search through every email you have ever received, and it offers offline support so you can" take your mail with you. You can read and compose emails without an active Internet connection and send them out once you are connected. Zoho Mail supports both traditional folders as well as labels. A label is a type of folder that you can customize by both name and color[17].

d) Go To Meeting

Go to Meeting invested more engineering development into making a product to support complex web meetings. This free service lets anyone communicate using rich media in real time. Unlike competing web conference products, does not require users to install software on their computers in order to attend a web meeting. Users can start or join meetings using only a few mouse clicks [16].

Host unlimited meetings, webinars or trainings.“It's efficient. It's effective. It's not very expensive. The people who have never seen such a thing before are amazed.” *It as follows*

- Includes License of GoToMeeting
- Includes HDFaces High-Definition Video Conferencing
- Desktop or Application Sharing
- Instantly Change Presenters
- Includes HDFaces High-Definition Video Conferencing
- Desktop or Application Sharing
- Instantly Change Presenters
- Share Keyboard and Mouse Control
- One-Click Recording

- Drawing Tools
- Includes audio (via telephone and computer)One-Click Meetings

As shown in fig 5

.

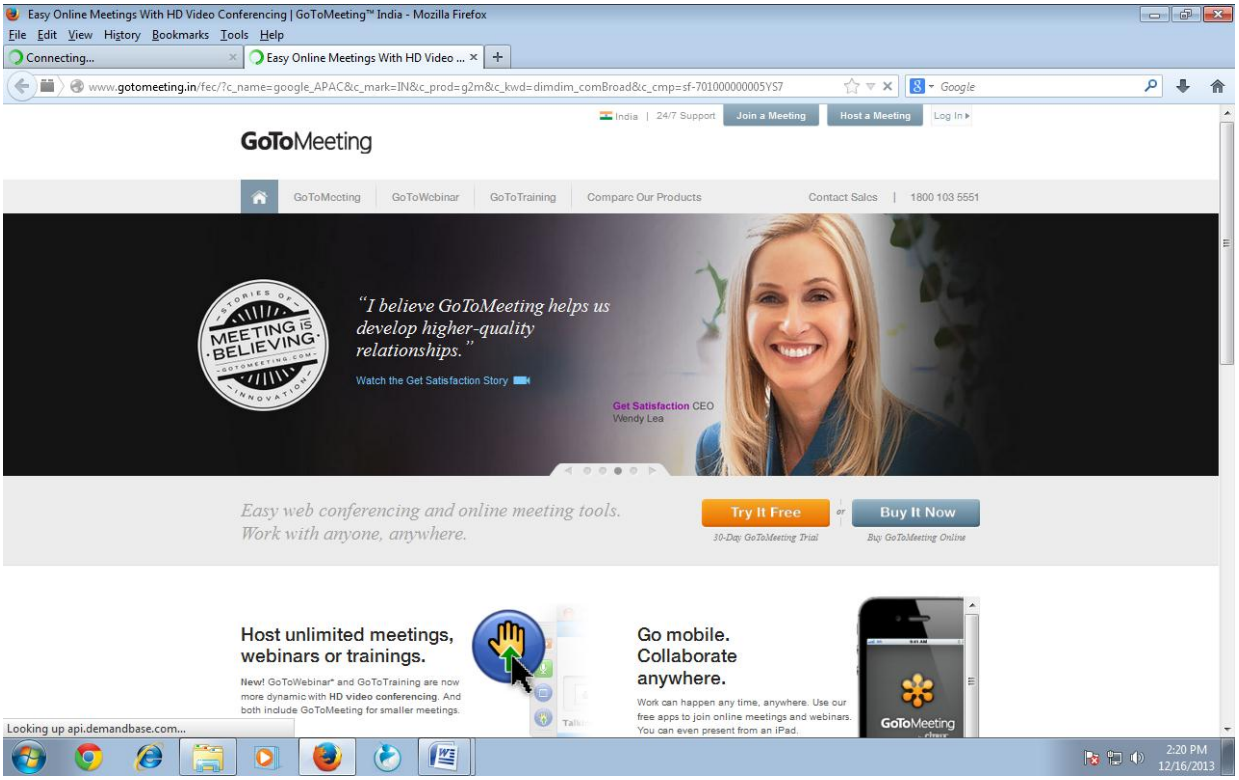

Figure 5. Go To Meeting

Figure. 6. Zimbra home page

e) **Zimbra**

On September 17, 2007, Yahoo! announced that it had entered into an agreement to acquire Zimbra,

Inc., a company specializing in web-based email and collaboration software, for approximately $350 million. The Zimbra email and calendar server is available for Linux, Mac OS X, and virtualization platforms. Zimbra can synchronize with smartphones (such as iPhone and BlackBerry) and desktop clients (such as Outlook and Thunderbird).The Yahoo! Zimbra desktop is shown in Figure 5.

As above mentioned diagrams whereas end user access now a days it is very famous every using their personal information is maintained at their sites. So many of the Companies are build their servers at various locations once they are getting problem of unauthorized persons there is problem utilizing in reliable manner. That's the reason to implement algorithm in more secure way by using saas model in cloud computing to utilizing resources.

V. STANDARDS FOR SECURILY ACCESS

Security standards are based on a set of key principles intended to protect this type of trusted environment. Especially for security in the cloud, must also include nearly all the same considerations as any other IT security endeavor. The following protocols, while not exclusively specific to cloud security [4].

A) Security (SAML OAUTH, OPENLD, SSL/TLS)

A basic philosophy of security is to have layers of defense, a concept known as *defense in depth.* This means having overlapping systems designed to provide security even if one system fails in end user access. An example is a firewall working in conjunction with an intrusion-detection system (IDS)[4]. Defense in depth provides security because there is no single point of failure and no single entry vector at which an attack can occur. For this reason, a choice between implementing network security in the middle part of a network (i.e., in the cloud) or at the endpoints is a false dichotomy.

Traditionally, security was implemented at the endpoints of end user acess , where the user controlled access. An organization had no choice except to put firewalls and antivirus software inside its own network. Today, with the advent of managed security services offered by cloud providers, additional security can be provided inside the clouds for end user acess.

a. Security Assertion Markup Language (SAML)

SAML is an XML-based standard for communicating authentication, authorization, and attribute information among online partners such as end user access. It allows businesses to securely send assertions between partner organizations regarding the identity and entitlements of a principal. The Organization for the Advancement of Structured Information Standards (OASIS) Security Services Technical Committee is in charge of defining, enhancing, and maintaining the SAML specifications. SAML is built on a number of existing standards, namely, SOAP, HTTP, and XML. SAML relies on HTTP as its communications protocol and specifies the use of SOAP (currently, version 1.1) [4].
SAML defines XML-based assertions and protocols, bindings, and profiles.

A SAML binding determines how SAML requests and responses map to standard messaging protocols. An important (synchronous) binding is the SAML SOAP binding. SAML standardizes queries for, and responses that contain, end user authentication, entitlements, and attribute information in an XML format.

SAML queries: the authentication query, the attribute query, and the authorization decision query. Of these, the attribute query is perhaps most important. The result of an attribute query is a SAML response containing an assertion, which itself contains an attribute statement.

SAML assertions contain a packet of security information in this form:

<saml: Assertion A…>

<Authentication>
….
</Authentication>
<Attribute>
….
</Attribute>
<Authentication>
….
</Authentication>
</saml: Assertion A…>
Assertion A, issued at time T by issuer I, regarding S, provided conditions c are valid.

b. Open Authentication (OAuth)

OAuth is an open protocol, initiated by Blaine Cook and Chris Messina, to allow secure API authorization in a simple, standardized method for various types of web applications. Cook and Messina had concluded that there were no open standards for API access delegation [4].

OAuth is a method for publishing and interacting with protected data for end user access. For developers, OAuth provides users access to their data while protecting account credentials. OAuth allows users to grant access to their information, which is shared by the service provider and consumers without sharing all of their identity.
provides no privacy at all and depends on other protocols such as SSL to accomplish that. OAuth can be implemented in a secure manner, however. In fact, the specification includes substantial security considerations that must be taken into account when working with sensitive data.

c. OpenID

OpenID is an open, decentralized standard for user authentication and access control that allows users to log onto many services using the same digital identity. It is a single-sign-on method of access control. As such, it replaces the common log-in process (i.e., a log-in name and a password) by allowing end users to log in once and gain access to resources across participating systems.

d. SSL/TLS

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographically secure protocols designed to provide security and data integrity for communications over TCP/IP. TLS and SSL encrypt the segments of network connections at the transport layer. Several versions of the protocols are in general use in web browsers, email, instant messaging, and voice-over-IP. TLS is an IETF standard protocol which was last updated in RFC 5246. The TLS protocol allows client/server applications to communicate across a network in a way specifically designed to prevent eavesdropping, tampering, and message forgery of end users. TLS provides endpoint authentication and data confidentiality by using cryptography. TLS authentication is one way-the server is authenticated, because the client already knows the server's identity [4]. In this case, the client remains unauthenticated. At the browser level, this means that the browser has validated the server's certificate-more specifically; it has checked the digital signatures of the server certificate's issuing chain of Certification Authorities (CAs).

VI. RESULT

Validation does not identify the server to the end user. For true identification, the end user must verify the identification information contained in the server's certificate (and, indeed, its whole issuing CA chain). This is the only way for the end user to know the "identity" of the server, and this is the only way identity can be securely established, verifying that the URL, name, or address that is being used is specified in the server's certificate. More important, an understanding of why they have

evolved. Standards are important, to be sure, but most of these standards evolved from individuals taking a chance on a new innovation in end user access in best way.

VII. CONCLUSION

This paper provided an overview of end-user access to cloud computing. We first talked about key trends we believe will drive collaboration further into the cloud environment. We chose five significant entities to present you with an overview of the types and levels of capability available in the cloud today-things you can use now. YouTube, an online video repository, has an amazing hold on the global audience. Collaboration suites such as Zoho both enhance mobility and allow you to maintain a virtual office in the cloud. Social networking with Facebook has become very popular, especially in academic settings. Zoho is a SaaS vendor to watch. Backed by Google, Zoho offers something for everyone.

We have discussed some of the more prevalent standards used in cloud computing. Although we have not analyzed each standard in depth, you should now have a feel for how and why each standard is used and, more important, an understanding of why they have evolved. Standards are important, to be sure, but most of these standards evolved from individuals taking a chance on a new innovation. As these innovative techniques became acceptable to users and implementers, more support for the technique followed. At some point, enough support was present to make the innovation be considered a "standard," and groups formalized protocols or rules for using it. Such a "standard" is used until more new innovation takes us elsewhere.

REFERENCE

[1] Paul McDougall, ”The Four Trends Driving Enterprise CloudComputing”.http://www.informationweek.com/cloudcomputing/blog/archives/2008/06/the_four_trends.html, 10 june 2008,retrieved 26 Feb 2009.
[2] John W. Rittinghouse, James F. Ransome, ” Cloud Computing Implementation, Management, and Security”, CRC Press 2010 by Taylor and Francis Group, LLC.
[3] Journal of Theoretical and Applied Information Technology, “CLOUD COMPUTING”, www.jatit.org, 2005 – 2009.
[4] http://www.youtube.com
[5] http://www.google.com/uds/solutions/videosearch/reference.html
[6] ActionScript is a scripting language based on ECMMScript.It is used primarily for development of web sites and software using Adobe Flash Player(in the form of embedded SWF[Shockwave Flash file)
[7] Chromeless is a term used by developers to refer to a basic player without buttons, gadhers,or menu controls-essentially, the stuff usually found in the silver(or chrome)part of a dialog or window.when those are not present, the control is said to be chromeless.
[8] http://code.google.com/apis/youtube/2.0/reference.html
[9] http://code.google.com/apis/gdata.
[10] http://googledataapis.blogspot.com/2008/07intro-to-atom-publising-protocol.html.
[11] http://www.Zimbra.com
[12] http://www.facebook.com
[13] http://www.dimdim.com/support/dimdim_help.html.
[14] Bruce Schnier,Http://www.schneier.com/blog/archives/2006/02/security_in-the.html,15 Feb 2006,retrieved 21 Feb 2009
[15] The reader is encouraged to consult http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.
[16] http://www.gotomeeting.com
[17] www.zoho.com

