International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 5, May - 2013

Cloud Based Intra-College Information Communication System Using Mobile Clients

Neeraj Patane
MMIT,Lohgaon,Pune
Dept. Of Information Technology
University Of Pune

Prashant Bhujbal
MMIT,Lohgaon,Pune
Dept. Of Information Technology
University Of Pune

Nikita Borkar
MMIT,Lohgaon,Pune
Dept. Of Information Technology
University Of Pune

Abstract

In this paper, the author discusses about the cloud computing architecture, the web services and other aspects that are required for communication over cloud. The author primarily focuses on using of web services through mobile phones. Cloud computing is the use of computing resources that are delivered as a service over a network. The name comes from the use of a cloud shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Mobile phones are devices that are cheap and widely used all over the globe today. The cloud services and applications can be used by people for communication and various other activities. People can use their mobile gadgets and other devices like tabs, laptops, ipad etc. for using these services. These services prove to be of great use in fields like education (e.g. providing educational resource storage and databases, e-mails, educational applications and tools for students and teachers and clients located within the college campus involving in an educational program). Considering the present communication system, the proposed system provides a cost effective application for users in their daily life. The' cloud based intra college communication system using mobile clients (CICCSM)' can raise the quality of education system to a new level [2].

1. Introduction

Cloud Based Intra College information communication system using mobile clients , we are using software as a services (SaaS architecture).
we need to implement web service for intra college communication. The communication will occur between non-teaching staff, teaching staff and students. The non teaching staff and teaching staff use pc's and students use mobile phones for the communication. Section 1.1. and 1.1.1 discuss about the cloud computing and its working. Section 1.2. discuss about the security using cryptographic hash function. section 2. gives the sketch of the implementation of cloud based intra college information communication system using mobile clients. Section 3. discuss about the features provided. and Section 4. enhances with the future scope.

1.1 Cloud Computing

Cloud computing refers to the logical computational resources (data,software) accessible via a computer network (through WAN or Internet etc.), rather than from a local computer. Data are stored on Server Farms generally located in the countryof the service provider. The on-line service is offered from a cloud provider. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services.Cloud computing differs from the classic client-server model by providing applications from a server that are executed and managed by a client's web browser, with no installed client version of an application required. Centralization gives cloud service providers complete control over the versions of the browser-based applications provided to clients, which removes the need for version upgrades or license management on individual client computing devices. The phrase "software as a service" (SaaS) is sometimes used to describe application programs offered through cloud computing. A common shorthand for a provided cloud computing service (or even an aggregation of all existing cloud services) is "The Cloud"[1].

1.1.1 How it works. A cloud user needs a client device such as a laptop or desktop computer, pad computer, smart phone, or other computing resource with a web browser (or other approved access route) to access a cloud system via the World Wide Web. Typically the user will log into the cloud at a service provider or

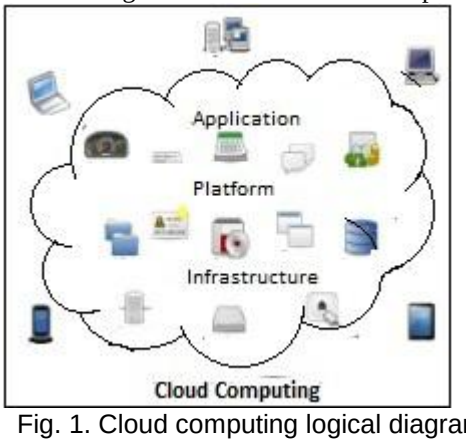

Fig. 1. Cloud computing logical diagram[1]

private company, such as their employer. Cloud computing works on a client-server basis, using web browser protocols. The cloud provides server-based applications and all data services to the user, with output displayed on the client device. If the user wishes to create a document using a word processor, for example, the cloud provides a suitable application running on the server which displays work done by the user on the client web browser display. Memory allocated to the client system's web browser is used to make the application data appear on the client system display, but all computations and changes are recorded by the server, and final results including files created or altered are permanently stored on the cloud servers. Performance of the cloud application is dependent upon the network access, speed and reliability as well as the processing speed of the client device.

1.2 SECURITY USING CRYPTOGRAPCHIC HASH FUNCTION

Cryptographic hash function is a hash function, that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded is often called the "message," and the hash value is sometimes called the message digest or simply digest[6]. The ideal cryptographic hash function has four main or significant properties:

I. It is easy to compute the hash value for any given message
II. It is infeasible to generate a message that has a given hash
III. It is infeasible to modify a message without changing the hash
IV. It is infeasible to find two different messages with the same hash

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital)fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.

The Secure Hash Algorithm is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). What is the Secure Hash Algorithm (SHA and SHA-1)? The Secure Hash Algorithm (SHA), the algorithm specified in the Secure Hash Standard (SHS), was developed by NIST and published as a federal information processing standard (FIPS PUB 180). SHA-1 was a revision to SHA that was published in 1994. The revision corrected an unpublished flaw in SHA. Its design is very similar to the MD4 family of hash functions developed by Rivest The algorithm takes a message of less than 264 bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5 (but the larger message digest makes it more secure against brute-force collision and inversion attacks.

1.2.1 Verifying the integrity of files or messages. An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).
For this reason, most digital signature algorithms only confirm the authenticity of a hashed digest of the message to be "signed." Verifying the authenticity of a hashed digest of the message is considered proof that the message itself is authentic.

1.2.2 Password verification. A related application is password verification. Passwords are usually not stored

n cleartext, but instead in digest form, to improve security. To authenticate a user, the password presented by the user is hashed and compared with the stored hash. This also means that the original passwords cannot be retrieved if forgotten or lost, and they have to be replaced with new ones. The password is often concatenated with a random, nonsecret salt value that is stored with the password. Because users have different salts, it is not feasible to store tables of precomputed hash values for common passwords.

2. Literature Survey

1. Traditional system :
The traditional communication uses the internet facility for communication. User can communicate using Personal computers and laptops. Availability of internet connection is the most important factor for the users. For eg two people chatting on gmail require to be having internet connection. The cost of using internet is pretty high and not affordable for every user. Due to high network traffic performance can degrade. Security is major concern. Hackers and illicit users can obtain password and other important information.

2. Current system :
Current system provides communication using Bluetooth technology. Two users can communicate using mobile devices or personal computer/laptops. The major concerns using this is the availability of service. For two users to communicate both the users should have Bluetooth active. If one user wants to mail his friend say for eg: Mr. X and X does not have his Bluetooth ON then X won't receive the mail. Second major concern is the coverage area. For all mobile devices the standard area coverage for bluetooth is 10m. So a user can communicate with anyone within that range, if a user beyond that range wants to communicate
it is not possible and cannot use the services. Power consumption is high.

3. Cloud based intra college information communication system using mobile clients :
To overcome the disadvantages of the current system we have proposed the CICCMC. The system uses wi_ technology which is the major advantage. The system provides high availability. Any user can use the services by turning on the wi-fi of its system. The users need not be login at the same time for communication. a user can send mail to his friend. The friend can see the mail when he logins. Incase of chat session one user logs off then the messages sent by the other person will be automatically stored in messages. Creation of groups and different users is much easier. The system provides high security using the SHA-1 algorithm. The coverage area is much higher than the current system which provides more portability. The users need not be present in front of eachother. The communication is cost e_ective and easy. comparing to the previous systems the CICCMC provides a new platform of communication.

3. Block Diagram

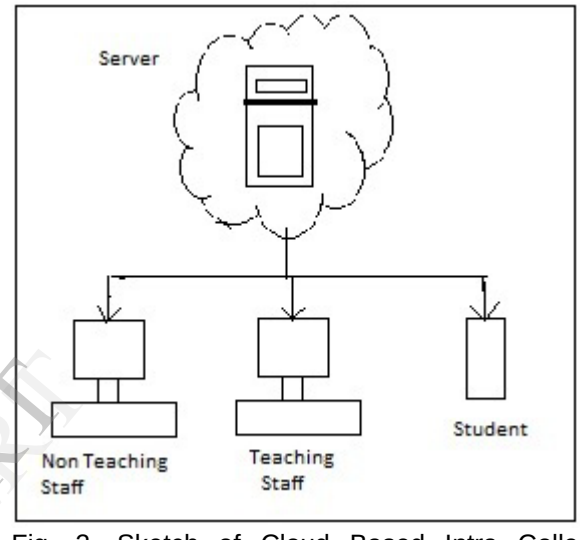

Fig. 2. Sketch of Cloud Based Intra College Information Communication System Using Mobile Client.

4. Features

1) Manage notes:
- The staff members can upload notes of their respective subjects for the students.
- Students can upload their own notes to circulate them among their classmates.
- The user can modify,add,delete motes according to their requirements.
- This service has medium priority as it will be used on average basis by the users.

2) Create groups:
- The staff can create groups depending on branches,class,project ,practical batches etc.
- Every new user added should be assigned into some group.
- This feature has high priority.

3) Assign task:
- The HOD can assign the daily task to its department staff and manage it.
- Similarly teachers can assign their project task and subject assignments to students.

- Task assignment has medium priority.

4) Message/SMS:
- For communication in real time the system provides SMS service. The devices within wifi range can use the service free of cost as compared to the service provider SMS services which are charged.
- Priority: high.

5) Group-wise broadcasting:
- Notes and notifications can be broadcasted only to particular group.
- For eg: class teacher can send a notice only to its class students.
- Priority: low.

6) Email:
- Email service can be used by the users to mail and transfer information.
- The service is used free of cost.
- Priority: medium.

7) Manage notifications:
- Notifications would appear on mobile devices of students when a message or email is received.
- The users can be alerted with these notifications about important information.
- Priority: low.

8) Monitor student group:
- Staff can monitor the progress of their respective class or group.
- This will help them to schedule their work and assign tasks.

9) Staff-student communication:
- The main feature of the system is staff student communication that enables exchange of
- information between different users.
- Priority: high.
- This feature has maximum priority as communication is the base service of this system.

10) Event creation
- Events such as tech-fest at college level as well as cultural events information can be circulated.
- Events can be created and managed using this service.
- Priority: medium.

11) Resource/links:
- Important links can be uploaded for other users to use.
- These can be viewed by all users or group users depending on the access rights provided.
- Priority: low.

12) Request for group join/leave:
- Any student or staff can join a particular group.
- Eg: a student changes its project group then he can change its group.
- He can also leave a group.
- Priority: medium.

13) Manage to-do's:
- Students can create their to-do list which can be viewed by them any time which will help them to schedule their work or day.
- Priority:low.

4. Conclusion and Future Scope

In this paper the author has discussed various aspects and models related to cloud based communication. This system provides a brand new application which makes communication in daily life easy. The author has implemented software as a service (SaaS) architecture in the system. The system provides facilities of sms, email, notifications, to-do-list, and various other features which gives the user an user friendly interactive communication. The system provides high security ,data storage and authentication using hash algorithms. Theft of information and misusage of user's account is not possible. This creates a feeling of secured and safe communication in the users mind. Cloud based communication system can be implemented in various departments such as healthcare , corporate world, political and social world. It plays an important role in educational institutions by providing a platform for the students and staff for efficient and effective interaction. It is cost effective as communication is done using wifi technology. The availibility of low cost cell phones embedded with latest technologies , almost every other human can posses a cell phone. This makes the application widely and globally useful for future research and development.

5. References

[1] Cloud Computing for Mobile World Chetan S., Gautam Kumar, K. Dinesh, Mathew K. and Abhimanyu M.A.,Department of Computer, Science Engineering,National Institute of Technology,Calicut

[2] Aida Ghazizadeh, "Cloud Computing Benefits and Architecture in E-Learning," wmute, pp.199-201, 2012 IEEE Seventh International Conference on Wireless, Mobile and Ubiquitous Technology in Education, 2012

[3] International Conference on Information, Electronic and Computer Science (ICIECS 2010 E-BOOK)(pp 1542-1545)

[4] Andreas Klein, Christian Mannweiler, Joerg Schneider, and Hans D. Schotten. Access schemes for mobile cloud computing. In Eleventh International Conference on Mobile Data Management (MDM), 2010, pages 387-392, 2010.

[5] Srirama, S., Jarke, M., Prinz, W.: Mobile Web Service Provisioning. In: Int. Conf. on Internet andWeb Applications and Services (ICIW06), IEEE Computer Society(2006)
[6] ”Cryptographic Hash Function Basics: Definitions,Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and, Collision Resistance by P. Rogaway, T. Shrimpton,2004
[7] Balani, N.: Deliver Web Services to mobile apps. IBM developerWorks (2003)
[8] Jacson H. Christensen, ”Using RESTful web services and cloud computing to create next generation mobile applications,” in Proceedingsof the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications (OOPSLA), pp. 627-634, October 2009.
[9] Tian, M., Voigt, T., Naumowicz, T., Ritter, H., Schiller, J.: Performance considerations for mobile web services. Elsevier Computer Communications Journal 27 (2004) 10971105 [10] Web Services Activity, http://www.w3.org/2002/ws/,May 2006
[11] GSM World, GSM - The Wireless Evolution, http://www.gsmworld.com/technology/index.shtml, Jun 2006
[12] Srirama, S., Jarke, M., Prinz, W.: Mobile Host: A feasibility analysis of mobile Web Service provisioning. In: 4th International Workshop on Ubiquitous Mobile Information and Collaboration Systems (UMICS 2006), a CAiSE06 workshop, Springer LNCS (2006).