International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 07 | July - 2021 ISSN: 2582-3930

# REAL TIME MESSAGING SYSTEM BASED ON WEB

**Rekha S[1], Shreevatsa N[2], Yellappa S[3]**

*[1]Assistant Professor, Department of Computer Science & Engineering, Atria Institute of Technology, Bangalore, India*

*[2,3]Student, Department of Computer Science & Engineering, Atria Institute of Technology, Bangalore, India*

---

**Abstract -** The 21st century is also called "The age of the Internet" due to rapid growth of communication among people and its uses in workplaces. Thereby reduces time and effort which it used to take before for long distance sharing of information and enabling faster completion of works and increasing efficiency. Communication often requires the installation of software or any other dependencies which is time and space consuming therefore causes hesitancy among users. This paper accord the solution of Real Times Messaging System(RTMS) to bring people together by communicating with no installation of any software or dependencies by offering only pure web experience. It achieves persistent real time messaging through websockets and provides users with one-to-one or group communication. It introduces the system architecture of RTMS, illustrates the function of the persistent communication system, and describes the realization of three key technologies (such as Web Sockets, Server, MongoDB, Encryption)

***Key Words***: Real Time Messaging, Point-to-Point Communication, Websockets, Encryption.

## 1. INTRODUCTION

In recent years, the need for communication between people is increasing and has become part of our daily life. Information exchange in all fields from students to professional use has become rampant. With the rise of mobile users and affordable internet, more and more people are adopting to communication through the web. With the rise of HTML5 and other front-end technologies, there is a strong demand from users for a real-time messaging system. The simplification of technologies has only helped developers in fulfilling these user demands. The proposed method provides low cost usage, efficient use of network resources and requires no installation of software or any application on the client side, overcoming the differences between the operating systems providing a cross-platform real-time messaging experience. So this system can adopt the way of the web to complete real time messaging, and whether it is a computer, mobile phone or tablet, it can communicate well. The application of web real time messaging has a very high significance to enhance the user activity and the interactivity of the website.

## 2. LITERATURE SURVEY

A considerable number of Real Time based on Web applications are developed and deployed in domestic computers. It mainly includes Tencent, Taobao and Renren. The Real Time Messaging is used in Taobao in a relatively early time. [1] Demonstrated that it is possible to implement a pure web based instant messaging system with relatively strong login methodology. It uses the method that adopts loading the third party SDK and achieves high quality communication between users. Real Time Messaging is mainly applied to the buyer and the seller to communicate in the Taobao page, Taobao uses a long polling based on AJAX to achieve the Comet[2]. The web chat of Renren is mainly used in instant communication between users. Renren uses the Iframe and htmlfile stream mode to achieve Comet. For Tencent and Web QQ use Comet technology is used to achieve instant chat at first, but the goal of Tencent is not only applying Comet technology to instant chat, but also using the Real Time Web technology as a foundation to achieve a lot of specific application model. Tencent will build the Web QQ as the core platform of a new B/S generation [3]. So, Real Time Messaging is very important to domestic enterprises. [4] This system is a Web application based on B/S structure, follows the software engineering design method and realizes the user login, examination question management, database maintenance, examination paper generation of examination question database, online examination management, examination score management, and other functions.[5] The RSA encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting.

## 3. SYSTEM ARCHITECTURE

The system architecture of RTMS[Real Time Messaging System] is composed of a user layer, RTMS service layer and database layer as shown in fig. 3.1.

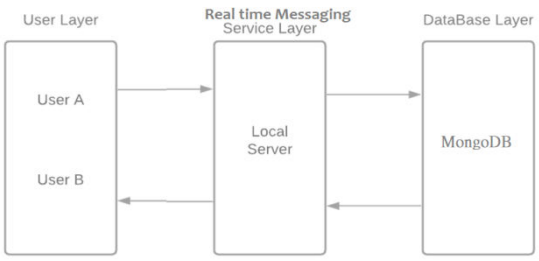


**Fig -1**: System Architecture

Among them, the user layer includes individual users with their own namespace, the RTMS service layer is responsible for interacting with all user space and the database space. It is also responsible for creating a websocket among users for communication channel. It also mainly realizes the data processing of the user's friends and groups real-time

messages. The database layer is used for storing, retrieving and listing real-time messages.

System Functions:
The system includes login module, point to point communication module and group communication module.

A. Login Module:
The module mainly realizes the functions of user register, user login. Users can log in, create, fill the personal information including their username, password and phone number after registration, so that making other users understand their own.

B. Point to Point communication module:
This module mainly realizes the user's text messages between two friends. After the friend's contact has been saved into the friend list. User can send and receive text messages.

C. Group communication module:
This module mainly realizes the group creating and joining. After joining group, user can send text messages to all friends in the group. With all of them receiving these text simultaneously.

## 1. KEY TECHNOLOGIES

A. Socket.io:
Socket.IO is a library that enables real-time, bidirectional and event-based communication between the browser and the server. The client will try to establish a Websocket connection if possible, and will fall back on HTTP long polling if not. Websocket is a communication protocol which provides a full-duplex and low-latency channel between the server and the browser.

B. MongoDB Atlas Database:
MongoDB Atlas is the global cloud database service for modern applications. Deploy fully managed MongoDB across AWS, Google Cloud, and Azure with best-in-class automation and proven practices that guarantee availability, scalability, and compliance with the most demanding data security and privacy standards.

C. RSA Encryption:
RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private Key is kept private.

### Algorithm:

1. Select two large prime numbers, x and y.
2. Calculate n = x * y
3. Calculate the totient function; phi(n) = (x-1)(y-1)
   According to totient function: if x is a prime number, phi(x) = x – 1.
4. Select an integer e, such that
   A) e is co-prime to phi(n) i.e gcd(phi(n) and e) = 1
   B) 1 < e < phi(n)
5. Calculate d such that e.d = 1 mod phi(n)
6. PUBLIC_KEY = ( e, n )
7. PRIVATE_KEY = ( d, n )
8. Encryption : C = M^e * mod(n)
9. Decryption : P = C^d * mod(n)

## 2. CONCLUSIONS

This paper proposes a solution of RTMS, because it achieves high quality communication between users. We don't need to deal with the tedious bottom business, the solution shortens the development cycle of the system, reduces the difficulty of system development and saves the development cost.

After the system running, it has basically achieved the above functions, and the effect is good. It provides reference for the development of other Real Time Messaging systems.

The shortcoming of the system is that requiring the browser version, only support Google browser (38, 44, 45, 46 stable version) in the HTTP environment, and supports all versions of above Chrome38 (recommended to use more than Chrome47 version) and the latest version of Firefox in the HTTPS environment.

## REFERENCES

1. J. Wang, B. Zhang, J. Guo and H. Wang, "The design of instant messaging system based on web," 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2017.
2. Xin Yang, "Research on real time communication system and key technology based on Web," Beijing University of Posts and Telecommunications, 2013.
3. Wenting Yang. "Research and implementation of message push platform based on HTTP long connection," Huazhong University of Science and Technology, 2012.
4. Li Zhang, "Design and implementation of network examination system based on B/S architecture," Jilin University, 2014.
5. Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, 2011.