ChatApp: Instant messaging Application with End to End Encryption

Vaibhav Gupta, Dept. of Computer Science and Engineering, JIS College of Engineering, West Bengal, India

Anshu Kumar Mishra, Dept. of Computer Science and Engineering, JIS College of Engineering, West Bengal, India

Abhishek Thakur, Dept. of Computer Science and Engineering, JIS College of Engineering, West Bengal, India

Prithwish Kar, Dept. of Computer Science and Engineering, JIS College of Engineering, West Bengal, India

Amit Majumder, Dept. of Computer Science and Engineering, JIS College of Engineering, West Bengal, India

Abstract

ChatApp is based on instant messaging (IM) technology which is a type of online chat. This technology offers real-time text transmission with the help of the Internet. By 2010, instant messaging over the WebApplication was in peak, in favor of messaging features on social networks. With ever increasing users of the Internet and rise of digitalization. With the rise in demand of confidentiality over the Internet there is a new need for efficient end to end encryption to secure data from any attacker, or a curious administrator or the strict government. Moreover, instances of burst traffics are now more common and pre-deciding the maximum resource requirement is no more effective, thus there is a requirement of dynamic load balancing and resource allocation. Web applications always rely on servers to store its confidential information and to process it. Nevertheless, when anyone who gets access to the servers (e.g., any smart attacker, a curious administrator, or a strict government) there they can get all the stored data. This paper introduces ChatApp, a chat messaging platform that protects data confidentiality ChatApp stores server-encrypted sensitive data and decrypts the data only in browsers for users. While making this method work ChatApp faces three challenges. First, after encryption with a key, ChatApp server stores all data on the device and uses the same key before sending it to the client. Second, in the presence of an active adversary, ChatApp shares public keys securely with the users. Finally, even if the server is malicious ChatApp ensures that client-side application code is authentic. To handle bursty traffic ChatApp uses the concept of microservices and has a special server to monitor the health and traffic of different microservices and available hardware resources. Thus, creating or shutting down the instances of various microservices depending upon the pre-decided short circuiting hook. This project's main aim is to study, and design a pilot project as a proof of stated concepts. The main aim is to design an instant messaging application solving the problem as stated in the above paragraphs. This project studies various concepts of web application and in end design an instant messaging application with end to end encryption and self-healing servers.