PriMera Scientific Engineering
Volume 2 Issue 6 June 2023
ISSN: 2834-2550

PriMera Scientific Publications

Security Protocols for Cloud Based Communication

Type: Editorial
Received: May 08, 2023
Published: May 24, 2023

Citation:
Varun Prakash Saxena. "Security Protocols for Cloud Based Communication". PriMera Scientific Engineering 2.6 (2023): 01-02.

Varun Prakash Saxena*

Department of Computer Engineering, Government Women Engineering College Ajmer (Raj), India

***Corresponding Author:** Varun Prakash Saxena, Department of Computer Engineering, Government Women Engineering College Ajmer (Raj), India.

Over the past decade, cloud computing is the most emerged fast growing and widely accepted concept for information exchange. This is smartly designed for information exchange paradigm which builds around the core concepts of data encryption, data transmission, media transmission and communication with different remote login.

In highly programmable and high performance cloud based network, the central remote server or data centres are used for the storage of information in secure manner. They monitor everything and help the end user to retrieve the information without breaking its integrity, confidentiality and access controllability.

This task to manage and maintain the security at highest level in cloud is, inherently challenging. These cloud network are operated by many security level protocols to provide the efficient and secure service to end user who often lack of technical knowledge about the security mechanism and threats in a network.

On the other side, when sensitive information is stored on a cloud server, which is not in a direct control of end user, then the risk for the information is increased dramatically. Many unauthorised users may try to intercept secure data to compromise data centre server. Therefore in cloud communication, cloud provider will help to provide complete security measures for user to user communication but at the end cloud protection is not a network protection. Network level threads can compromise the security of information, so to provide the protection of information from intruders, security shield at the different level of cloud network is required.

We need three layers of security shield in cloud based network (1) Connectivity Level (2) Storage Level (3) Application Level. Cloud based protocol provide a broad set of policies and technologies to control these attack.

1. In *connectivity level*, when the real world communicate with multiple data centres and multiple end users in a cloud network, we have to consider all aspects of infrastructure including computer centre, data centre and cloud network to overcome the challenges related to architecture, performance , reliability, security, maintainability and virtualization as well.
   As the information move between the communication channels, end to end encryption and authentication with no data leakage is mostly needed. During this transmission to protect our cloud network, Host Identity Protocol is used for authenticate IPv4, IPv6 client server cloud network from the intruders. MQTT and HTTP Protocol provide a core support for device con-

nection and communication. In general MQTT is supported by embedded devices and for machine to machine interaction. In HTTP protocol based devices do not maintain a connection to IoT cloud, however it maintain a half duplex TCP connection where transmission is connectionless.

At this level some standardized protocol like connectionless network protocol, Secure Shell protocol, Spanning Tree Protocol, Equal Cost Multi-Pathing Protocol and many more are used. In these protocols some are communication protocols which are used for message failure detection, message monitoring and data unit identification.

2. In *storage level*, privacy plays an important role for the cloud service customer. Cloud service provider must ensure that the information and identity of client service customer will not disclose in any case. On the other hand, most pressing issue is that the data must be encrypted so no one, even administrator can't see the information without permission of customer. It is a duty of customer service provider to make sure the customer that no duplicate copy of keys (Private /Public) is generated and data form stored in is in encrypted multiple safe locations.

   Since the cloud is a very vast storage and it deals with a large amount of data information, the service provider should provide a separate address space to each customer with their individual memory space. This virtual isolation is provided with the help of dedicated virtual machines. Some time cloud deploys firewalls to protect the data and to overcome it Session Initiation Protocol (SIP) is used on VoIP based communication. This protocol helps the cloud for protecting their network by attacks like Denial of service, IP traffic management, Toll fraud protection and encryption of data.
3. In *application level*, cloud provides a facility to the end user to design their own application as per their requirement and the platform provided by service provider. Each cloud has its own different platform to execute user idea. The application must be tested and verified by the cloud service provider. The complete testing and module checking are done at the cloud service provider level before application being made available for the end user. There are some chances that attacker can also create a malicious application on cloud and launch it with attractive features to attract new user in a network. Application security protocol can handle all these malicious application service provider and user also. In addition, Cloud service providers have their own application firewall for monitoring incoming and outgoing traffic.

In these days, Equal Cost Multi-Pathing protocol is widely adopted by the cloud computing because it has the ability to create multiple load balanced paths which play a very important role for providing variable bandwidths depending upon the requirement of the application. Moreover, Extensible messaging and presence protocol (XMPP) can be used for public subscribe system and file transfer.

To conclude, there is no doubt that Cloud computing is the latest field in communication and for technology friendly users which promises immense benefits. Most of the Information technology giants like IBM, Cisco, Google and Microsoft have adopted it and continuously working in this area to handle security and privacy issues. It is expected that the use of cloud computing would exponentially increases in the upcoming days and simultaneously we all will face new challenges in cloud security. Hacking and various attacks to cloud infrastructure and cloud network would affect multiple clients even if only one site or one machine is attacked. These risks can be mitigated by using most secure protocols, security applications, most dynamic encrypted file systems, minimum data leakage and recovery software, and buying security hardware to track unusual behaviour across servers. However, there a lot of research work by the experts is still required in cloud area because many of the concerns related to security and privacy issues are not been answered yet.

Dr. Varun Prakash Saxena (BE, ME, PhD) is presently Assistant Professor, Department of Computer Engineering, Government Women Engg. College Ajmer since 2012. He has 10 year of teaching and research experience. He has published more than 18 research paper and 5 research article in national/International journal of repute. He is a member of 5 national/ international professional societies. His interest includes cryptography, Networks and programming. He is also guiding more than 10 PG students.