Journal of Engineering Science and Technology
Vol. 14, No. 3 (2019) 1398 - 1405


# PERFORMANCE EVALUATION OF VoIP SYSTEMS IN CLOUD COMPUTING

MOSLEH M. ABUALHAJ[1,*], MAYY M. AL-TAHRAWI[2], SUMAYA N. AL-KHATIB[3]

[1]Networks and Information Security Department, Faculty of Information Technology, Al-Ahliyya Amman University, 19328, Amman, Jordan
[2]Computer Science Department, Faculty of Information Technology, Al-Ahliyya Amman University, 19328, Amman, Jordan
[3]Software Engineering Department, Faculty of Information Technology, Al-Ahliyya Amman University, 19328, Amman, Jordan
*Corresponding Author: m.abualhaj@ammanu.edu.jo

## Abstract

In the last decade, cloud computing and Voice over Internet Protocol (VoIP) technologies have been exceeding propagated. Whereas, the cloud computing technology is deployed in more than 60% of the companies around the world. On the other hand, VoIP technology generated more than 1872 petabyte of data in the year 2015. The conjunction of the two technologies, cloud computing and VoIP, has been implemented by a considerable number of the organisation. However, VoIP systems are facing numerous types of attack. In this paper, we are investigating the performance of VoIP technology over cloud computing, when protected against attack. Particularly, we will investigate the Session Initiation Protocol (SIP) VoIP protocol Registration Request Delay (RRD) in cloud computing with security layer protection. In order to achieve that, we have deployed SIP server on the cloud (Microsoft Azure's datacenter) with security layer protection. The implementation of SIP VoIP server on cloud computing showed that the RRD delay was increased when adding a security layer in comparison to the implantation without a security layer. Whereas, the increment of the RRD delay was between 29% and 42%, in the tested scenario. Therefore, protecting the SIP VoIP server on cloud computing with the security layer negatively impact the performance of the SIP VoIP server.

Keywords: Cloud computing, Cloud Security, SIP delay, VoIP, VoIP threats.

## 1. Introduction

Cloud computing provides worldwide access to almost infinite types of services and resources through the Internet, with pay-as-you-go pricing. These resources and services are to three different models, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [1]. Cloud computing has grown tremendously in the last few years. According to Rapid Value Solutions [2], cloud computing is big business, already, generated around $100 billion a year in 2012. It is forecasted to increase up to $270 billion by the year 2020. In addition, more than 60% of enterprises will have at least half of their infrastructure on cloud-based platforms by 2018. There are many drivers behind this tremendous adoption of cloud computing, including; cost saving, on-demand scalability, superior performance, high security, etc. [2].

Meanwhile, in a diff erent context, Voice over Internet Protocol (VoIP) is spreading rapidly everywhere. VoIP is a technology to make a voice call through the Internet Protocol (IP) network [3]. According to Abualhaj et al. [4, 5], the amount of VoIP traffic running over the Internet around 156 petabytes per month in the year 2015. In addition, 214 billion minutes of VoIP calls were run on Skype application alone in the year 2013. The main driver behind this tremendous adoption of VoIP is that VoIP calls are very cheap and even sometimes are free. With this distribution, the deployment of VoIP over the cloud is an attractive solution that gains considerable popularity in all sectors [6]. This paper analyses the Session Initiation Protocol (SIP) VoIP protocol performance in cloud computing, while protected against attack. Specifically, this paper investigates the SIP protocol Registration Request Delay (RRD) in cloud computing with security layer protection. The security layer represented by the Intrusion Prevention System (IPS), whereas, the SIP requests are checked and dropped before passing to the SIP server if they are malicious.

The remaining of the present paper is arranged as follows. Section 2 highlights some issues that are related to this work, including; VoIP protocol and VoIP security threats, in addition, it discusses the related works. Section 3 demonstrates SIP testing network architecture. Section 4 displays and discusses the results. Section 4 concludes the paper.

## 2. Background and Related Works

This section highlights some issues that are related to this work, including; VoIP protocol and VoIP security threats, in addition, it discusses the related works.

### 2.1. VoIP protocols

Generally, VoIP systems use two categories of the protocol to handle the call. The first category is media transfer protocols, such as Real-time Transport Protocol (RTP), which are used to carry the voice data between the caller and callee. The second category is signalling protocols, which are used to establish a call between caller and callee. H.323 and the Session Initiation Protocol (SIP) are the two standard signalling protocols. Though H323 was the first standard, SIP overtook H.323 and dominate the VoIP systems [7]. This is due to the numerous advantages of SIP protocol, which suit the current propagation and environment of the of VoIP technology. One of the main advantages of the SIP protocol is that it may work

with any of the transport layer protocols, such as TCP or UDP. Another vital advantage that is SIP able to be extended, by allowing the developers to add new features that providing new services. In addition, SIP is a simple protocol that uses only a few messages to set up a call, unlike H.323, which requires several messages to set up a call. SIP Call Setup Delay (CSD) composed of Registration Request Delay (RRD) and Session Request Delay (SRD) [8]. RRD is the time taken by the SIP client to become registered. Figure 1 shows the SIP RRD process.

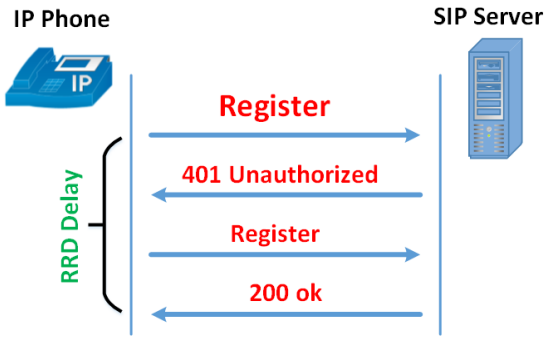


**Fig. 1. SIP client registration process.**

## 2.2. VoIP security threats

VoIP systems are experiencing a rapid increase in SIP security threats. A report published by Nettitude in 2015 stated that the number of attacks against the VoIP services, specifically SIP, represented 67% of all attacks recorded against our UK based servers [9]. Figure 2 shows the overall services being targeted. There are different types of attack can be done against SIP, including; Denial of Service (DoS) attacks, eavesdropping, packet spoofing, replay attacks, message integrity, session teardown. Therefore, a security layer should be implemented to protect a SIP server. Cloud computing can protect the SIP server by using different tools including, antivirus, firewall, Intrusion Detection Systems (IDS), and IPS [10, 11]. Implementing a security layer impose additional processing time and, thus, increase the delay of the signalling process [12].

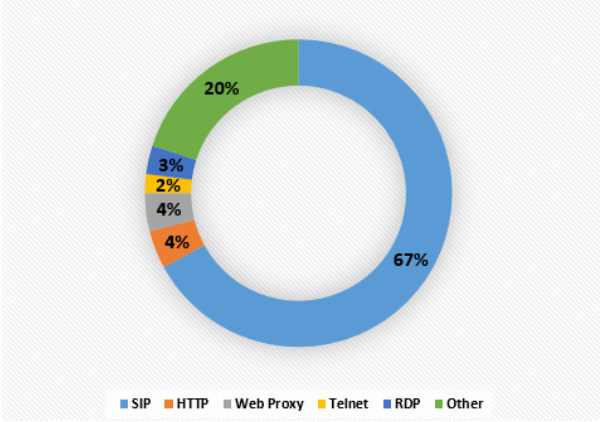


**Fig. 2. Attacks against VoIP services.**

## 2.3. Related works

There are several researchers have been investigated the performance of SIP. This section brief some of these researches.

Eyers and Schulzrinne [13] studded the CSD of SIP and compared and with that of. The simulation result showed that the delay of H323 significantly increases compared to SIP during high error periods. McDonald [14] studded the CSD of SIP in Third Generation Partnership Project (3GPP) network. The simulation result showed further researches are needed to improve SIP CSD in the 3GPP network. Fathi et al. [15] investigated the SIP CSD using a Markovian model to capture the burstiness of the channel. The result showed that Transport Control Protocol (TCP) imposes 30% extra delay compared with User Datagram Protocol (UDP). In addition, the result showed that SIP CSD outperforms H.323 CSD. Alshamrani et al. [16] Investigated SIP CSD over IPv6 Mobile Ad-hoc Network (MANET) and compared it with IPv4 MANET. The result showed that the SIP CSD when using IPv6 over MANET has underperformed the SIP CSD when using IPv4 over MANET. Shen et al. [17] investigated SIP CSD using Transport Layer Security (TLS) instead of UDP. The result showed that the SIP CSD when using UDP outperformed the SIP CSD when using TLS, due to the extra delay imposed by RSA (Rivest, Shamir and Adleman) when using TLS. Sher, et al. [12] investigated the SIP CSD under TLS and IDS. The result showed that increases the number of SIP requests increase the delay imposed by IDS. Kulin et al. [18] investigated the secured SIP CSD over TLS and compared with SIP CSD over UDP. The experiment, on the Asterisk open source SIP server, showed that TLS increases the delay up to four times compared to UD.

As we can see, there are many researchers have been done on testing the delay of SIP under different environments and security options. However, none of the previous works has investigated delay of SIP under the cloud environment. Therefore, the purpose of this paper is to investigate the delay of SIP signalling under cloud environment with a security layer added. Particularly, in this study, we try to investigate the impact of the security layer on SIP RRD under cloud environment.

## 3. Proposed SIP Testing Network Architecture

The proposed architecture places the SIP server on the cloud with security layer protection. The security layer represented by IPS which deny the malicious traffic before passing to the SIP server. The advantage of adding security is that the packets are checked against attacks before entering the network to prevent malicious traffic. However, this imposes an additional delay on the traffic, which may reduce the performance of some applications such as SIP applications [12]. In our proposed architecture the security layer was enabled at the server side in the cloud. Basically, the security layer checks the incoming requests to the SIP server against the attack. If suspicious requests found the request is cancelled, otherwise; the request forwarded to the SIP server. Figure 3 shows the proposed architecture with the place and the role of the security layer. We placed our SIP server at Microsoft Azure's datacentre under sipksa.cloudapp.net domain. We used Windows 2012 server as a guest machine with 8 Core CPU 2.6 GHz and 56 GB of RAM and implemented SIP server with more than 50 users. The clients reside at our internal network. The clients' SIP requests travel through the internal network to the edge router then through the internet to reach the SIP server at the Microsoft Azure's cloud.

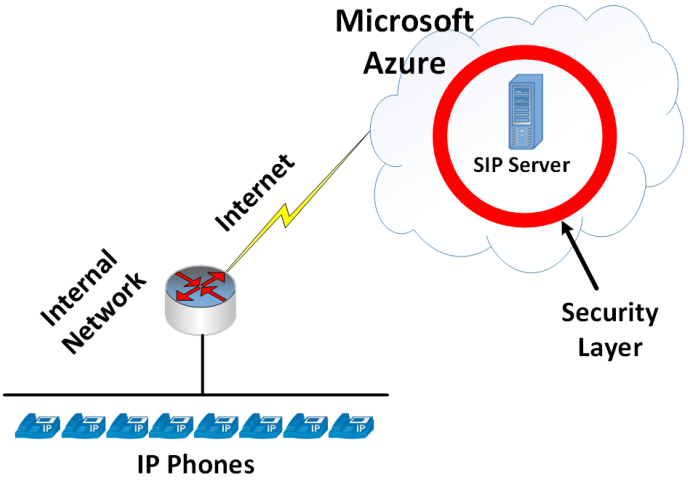


**Fig. 3. Proposed SIP architecture.**

## 4. Results and Discussion

The Network Microsoft Azure's datacentre was utilised to evaluate the performance of a SIP server in the cloud environment with security protection. The RRD to the SIP server with security protection was investigated and compared with that of SIP server without security protection, as shown in Fig. 4. The better (less) delay was observed when using a SIP server without security protection. This is because applying security protection enforce buffering the SIP packets for processing and checking whether they are malicious packets or not. This imposes additional delay that is increasing with the number of SIP packets. Figure 5 shows the difference in delay between the two scenarios. The result showed that the imposed delay when checking the SIP packets against attack is between 29% and 42%, in the tested cases. As we can see from Fig. 5, the delay has fluctuated when increasing the number of calls. This is due to the bursty nature of the network traffic, which fluctuate the load on the network, thus, fluctuate the delay.

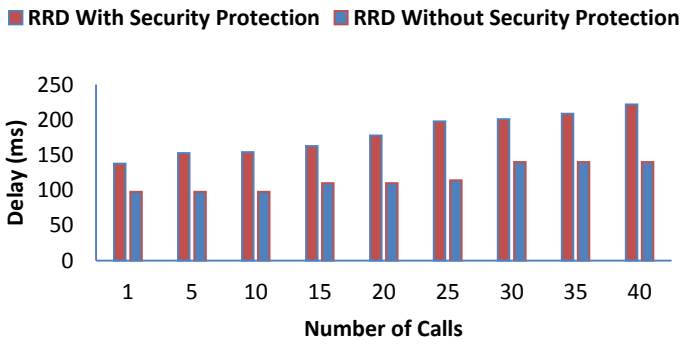


**Fig. 4. RRD delay of SIP server.**

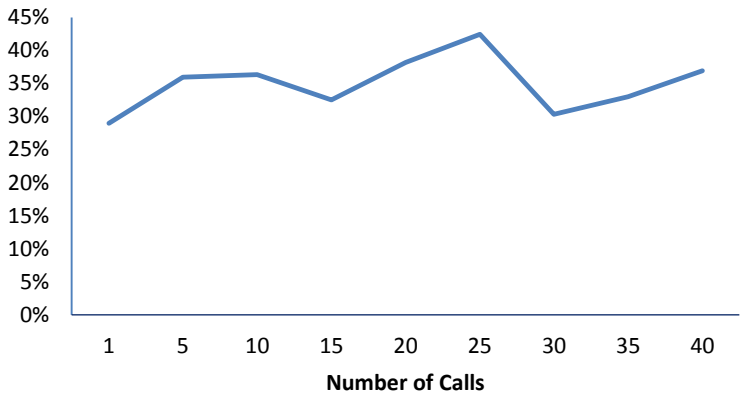


**Fig. 5. Imposed delay of security layer.**

## 5. Conclusions

Cloud computing hosts, almost, all types of services. One of the well-known services is Voice over Internet Protocol (VoIP). VoIP is a technology to make a voice call through the IP network. Session Initiation Protocol (SIP) is the dominant signalling protocol in VoIP technology. Due to that, it faces several types of attacks such as DoS attacks, eavesdropping, packet spoofing, and many other types of attacks. In this paper, we have implemented a SIP server in cloud computing with security layer protection. We have measured the RRD delay, as part of the SIP protocol delay. The result showed that the RRD delay was increased by up to 42% in the tested scenarios when adding a security layer in comparison to the implementation without a security layer. As future work, we will investigate the performance of other VoIP signalling protocols, such as Inter-Asterisk eXchange (IAX) and H323 in cloud computing with security layer protection. The performance of the three protocols (SIP, IAX, and H323) will be compared with each other. In addition, the performance of these protocols will be investigated under different security layer components in different environment specifications.

### Nomenclatures

| | |
|---|---|
| *CSD* | Call setup delay, ms |
| *RRD* | Registration request delay (Fig. 4), ms |
| *SRD* | Session request delay, ms |

### Abbreviations

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| DoS | Denial of Service |
| IaaS | Infrastructure as a Service |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| MANET | Mobile Ad-hoc Network |
| PaaS | Platform as a Service |
| RSA | Rivest, Shamir and Adleman |

| | |
|---|---|
| RTP | Real-time Transport Protocol |
| SaaS | Software as a Service |
| SIP | Session Initiation Protocol |
| TCP | Transport Control Protocol |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| VoIP | Voice over Internet Protocol |

## References


1. Saqib, M. (2017). Cloud monitoring: A survey. *International Journal of Advanced Research in Computer Science*, 8(2), 8-11.
2. Rapid Value Solutions. (2015). The adoption of cloud technology by enterprises – Trends, benefit and future. Retrieved May 25, 2018, from https://www.rapidvaluesolutions.com/the-adoption-of-cloud-technology-by-enterprises-trends-benefits-and-future/.
3. Abualhaj, M.M. (2015). ITTP-MUX: An efficient multiplexing mechanism to improve VoIP applications bandwidth utilization. *International Journal of Innovative Computing Information and Control*, 11(6), 2063-2073.
4. Abualhaj, M.M.; Kolhar, M.; Qaddoum, K.; and Abu-Shareha, A.A. (2016). Multiplexing VoIP packets over wireless mesh networks: A survey. *KSII Transactions on Internet and Information Systems*, 10(8), 3728-3752.
5. Abualhaj, M.M.; Al-Khatib, S.N.; and Baklizi, M. (2018). Multiplexing VoIP packets over internet telephony transport protocol (ITTP). *Proceedings of the 5th International Conference* on *Computer Science and Technology (CST)*. Dubai, United Arab Emirates, 75-81.
6. Abu-Alhaj, M.; Kolhar, M.S.; Halaiyqah, M., Abouabdalla, O.; and Sureswaran, R. (2009). MuxComp - A new architecture to improve VoIP bandwidth utilization. *Proceedings of the International Conference of Future Networks.* Bangkok, Thailand, 212-215.
7. Abu-Alhaj, M.M.; Manjur, S.K.; Sureswaran, R.; Wan, T.-C.; Mohamad, I.J.; and Manasrah, A.M. (2012). ITTP: A new transport protocol for VoIP applications. *International Journal of Innovative Computing, Information and Control (IJICIC)*, 8(3), 1879-1895.
8. Kolhar, M.; Alameen, A.; and Gulam, M. (2018). Performance evaluation of framework of VoIP/SIP server under virtualization environment along with the most common security threats. *Neural Computing and Applications*, 30(9), 2873-2881.
9. Nettitude R&D. (2015). VoIP attacks on the rise. Retrieved July 7, 2018, from https://www.nettitude.co.uk/wp-content/uploads/2015/06/VoIP-attacks-on-the-rise-Jules-Pagna-Disso.pdf.
10. Lee, J.; Cho, K.; Lee, C.; and Kim, S. (2015). VoIP-aware network attack detection based on statistics and behaviour of SIP traffic. *Peer-to-Peer Networking and Applications*, 8(5), 872-880.
11. Yang, X.; Zhou, S.; Ren, G.; and Liu, Y. (2018). Computer network attack and defense technology. *Information and Computer Security*, 1(1), 35-41.

12. Sher, M.; Wu, S.; and Magedanz, T. (2006). Security threats and solutions for application server of IP multimedia subsystem (IMS-AS). *IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation*. Tubingen, Germany, 38-44.
13. Eyers, T.; and Schulzrinne, H. (2000). Predicting internet telephony call setup delay. *Proceedings of the 1st IP Telephony Workshop*. Berlin, 1-11.
14. McDonald, C. (2003). *Converged networking- data and real-time communications over IP* (1st ed.). Berlin/Heidelberg, Germany: Springer Science + Business Media.
15. Fathi, H.; Chakraborty, S.S.; and Prasad, R. (2006). On SIP session setup delay for VoIP services over correlated fading channels. *IEEE Transactions on Vehicular Technology*, 55(1), 286-295.
16. Alshamrani, M.; Cruickshank, H.; and Sun, Z. (2014). A cross-layer approach to enhance the call setup performance of sip-based VoIP over AODV MANET. *Proceedings of the Eighth International Conference in Next Generation Mobile Apps, Services and Technologies (NGMAST)*. Oxford, United Kingdom, 241-247.
17. Shen, C.; Nahum, E.; Schulzrinne, H.; and Wright, C. (2010). The impact of TLS on SIP server performance. *Proceedings of the Principles, Systems and Applications of IP Telecommunications*. Munich, Germany, 59-70.
18. Kulin, M.; Kazaz, T.; and Mrdovic, S. (2012). SIP server security with TLS: Relative performance evaluation. *Proceedings of the 9th International Symposium on Telecommunications (BIHTEL)*. Sarajevo, Bosnia and Herzegovina, 1-6.