Performance Analysis of Secure Unified Communications in the VMware-based Cloud

Aklilu Daniel Tesfamicael, Vicky Liu, William Caelli
Science and Engineering Faculty
Queensland University of Technology
Brisbane, Australia
aki.tesfamicael@hdr.qut.edu.au, {vicky.liu, w.caelli}@qut.edu.au

***Abstract*—Unified communications as a service (UCaaS) can be regarded as a cost-effective model for on-demand delivery of unified communications services in the cloud. However, addressing security concerns has been seen as the biggest challenge to the adoption of IT services in the cloud. This study set up a cloud system via VMware suite to emulate hosting unified communications (UC), the integration of two or more real time communication systems, services in the cloud in a laboratory environment. An Internet Protocol Security (IPSec) gateway was also set up to support network-level security for UCaaS against possible security exposures. This study was aimed at analysis of an implementation of UCaaS over IPSec and evaluation of the latency of encrypted UC traffic while protecting that traffic. Our test results show no latency while IPSec is implemented with a G.711 audio codec. However, the performance of the G.722 audio codec with an IPSec implementation affects the overall performance of the UC server. These results give technical advice and guidance to those involved in security controls in UC security on premises as well as in the cloud.**

Keywords— unified communications (UC), UCaaS, IPSec, cloud-based UC services, security for UCaaS

I. INTRODUCTION

The National Institute of Standards and Technology's (NIST) definition of cloud computing has been commonly referenced by many including the Australian Government [1]. NIST [2] defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." Rather than hosting unified communications services on-premises, Unified Communications as a service (UCaaS) is considered a cost-effective model for on-demand delivery of unified communications services in the cloud for meeting the needs of enterprise level IT services. The IT services that are hosted by UC services in the cloud provide "voice over IP" (VoIP), video conferencing, messaging and presence over the Internet. There are some enterprises adopting a hybrid model such that some of the UCaaS applications are integrated with some UC services on-premises. However, small and medium businesses may choose complete UCaaS for their unified communications solution to help in cost saving.

Though many businesses have shown great interest in UCaaS solutions, there is much work to be done in order to protect UCaaS services from security threats. In our previous paper [3] we presented an implementation and evaluation of UCaaS solutions to save the cost of deploying premises-based UC services. In this paper, we evaluate the protection of UCaaS traffic by implementing Internet Protocol Security (IPSec) and analyze the performance of such UCaaS services against those used without implementing IPSec. Numerous studies [4–9] use IPSec for securing network communications for premises-based VoIP services. However, this research focuses on protecting UCaaS traffic, particularly voice and video communications in a VMware-based environment. Undoubtedly, the UC traffic is more sensitive to latency, jitter and packet loss more than most network applications. Quality of service (QoS) is one of the critical success factors in the design and performance management of UC services. As such, when implementing UC over IPSec, it is crucial to analyze its performance to avoid service quality degradation that may be added by the overhead of IPSec. In this paper, we evaluate the latency of the voice and video traffic when IPSec is implemented. As these experiments are conducted in a closed network, it does not reflect any network delays observed in real wide-area telecommunications networks.

In our experiments, we use G.711 as a narrowband codec providing an effective pass-band of 200-3,300 Hz comparing to G.722 as a wideband codec giving a pass-band of 50-7,000 Hz. Both these codecs are international telecommunication union (ITU) standards for an audio codec operating at 64 kbit/s [10-11]. The G.722 codec may not be used widely, but it provides improved speech quality compared to the quality of that using the G.711 codec. A wideband codec uses double the sample rate to provide a higher fidelity voice quality, but requires more CPU and network resources.

To the best of our knowledge, at the time of writing this paper, no study has been found which discusses UCaaS over IPSec and the deployment of UCaaS in a VMware-based cloud. The contributions made in this paper include aspects of protecting UC traffic in the cloud environment, provision of understandable technical advice to business and service providers and details on the implementation of UCaaS in a specific VMware-based cloud environment.

Based on our test results, the paper reports the impact on the performance of a UC system operating on a cloud system while implementing IPSec.

II. Related Work

Recently, numerous studies [4–9] have discussed security for premises-based VoIP systems. This literature review is focused on the discussion of security for UCaaS over IPSec.

In 2009, Thanthry et al. [12] propose an alternate encryption scheme that uses a public key scheme for authentication and key exchange, and encrypts the voice traffic with a symmetric cipher scheme. They claim their approach is less complex while maintaining communication security. Kuhn et al. [13] assert the importance of the security for VoIP against packet sniffing and other eavesdropping attacks. They suggest using tunneling with the Encapsulating Security Payload (ESP) mode of IPSec for protecting communications between the "callee" and the "caller". Their studies were conducted more than a decade ago and only discuss VoIP.

Numerous studies [4–9] have also been conducted to report on the implementation of IPSec or alternative security measures to protect premises-based VoIP systems. This paper analyzes the performance factors when implementing IPSec on a UCaaS system.

III. UC Implementation in the VMware vCloud Director

VMware ESXi is an operating system-independent hypervisor used to run multiple virtual servers on a single physical server. It is based on the VMkernel operating system interfacing with agents that run atop it. VMware vCloud suite is an integrated solution for building and managing a complete cloud infrastructure that meet IT's most critical needs. It is installed on top of the VMware ESXi server that provides pools of servers, storage and networking with dynamically configurable security, availability and management services. VMware vCloud Director, a key component of VMware vCloud suite, is a layer of software building on a VMware vSphere server, which includes the vCenter (VC) Server and the ESX Hypervisor. It is a private or hybrid cloud software solution that is capable of enabling enterprises to build their own multi-tenant private clouds by pooling infrastructure resources into virtual datacenters. Users can access those services through web-based tools.

VMware vShield can provide comprehensive data and application security, improve visibility and control in a VMware-based cloud. We will be studying vShield in the future to understand its security services to protect voice and video communications in a VMware-based Cloud. Fig. 1 shows our proposed UC high level design before IPSec implementation.

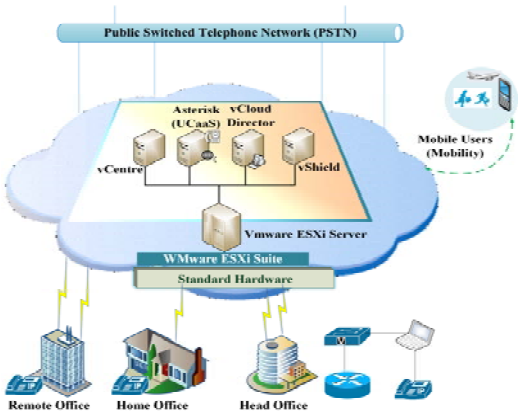

Fig. 1. A high level design of UCaaS

IV. UC Over IPSec in a VMware-based Cloud

IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols that helps protect communications over the Internet with encryption and/or authentication. IPSec supports transport and tunnel modes of packet delivery. In transport mode the protocols provide protection primarily for upper layer protocols; in tunnel mode, the protocols are applied to tunneled IP packets with the entire original VoIP or Video packets protected by IPSec. This means IPSec encapsulates the entire original packet inside a new IP packet, encrypts it and sends it to the other end [14].

IPSec provides two choices of security services, namely authentication header (AH) and encapsulating security payload (ESP). AH authenticates and ESP encrypts, and authenticates, the data over IP. The set of security services that IPsec can provide includes access control, connectionless integrity, data origin authentication, rejection of replayed packets (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality [14]. The ESP mode of IPSec implementation is selected as the operation mode for data authentication, integrity and confidentiality in this study as shown in Fig. 2. This study also uses the Internet Key Exchange (IKE) protocol v2 for performing mutual authentication and establishing a session key for data security. The encryption and integrity algorithms are based on the Advanced Encryption Standard (AES) with a 128-bit key length and Secure Hash Algorithm (SHA2-256) with 32-bit words, respectively. IPSec is implemented at the network layer to provide the security for UCaaS traffic security without any modifications to UC applications or related protocols.

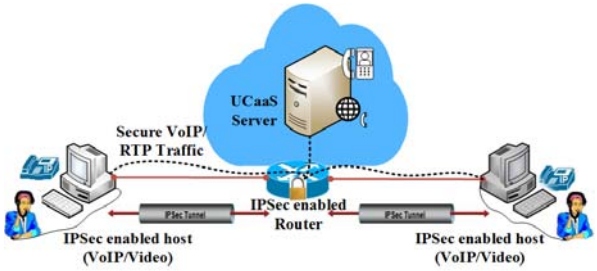

Fig. 2. Unified Communication over IPSec

V. TEST DESIGN AND RESULTS

To demonstrate the feasibility of the proposed UCaaS over IPSec implementation, we setup a cloud system based on the VMware vCloud Suite with a VMware ESXi server. The ESXi server acts as a core management tool to administer the entire virtual infrastructure for the provisioning, processing, storage, network and other fundamental computing resources.

Our experimental devices include a VMware ESXi server in a dedicated physical host. UCaaS, vCentre, vCloud Director and vShield are running on a virtual machine, and an IPSec enabled router on the cloud system. Our UCaaS system can provide services including VoIP, video conferencing, messaging and presence. We setup two dedicated client hosts, which are IPSec enabled clients. Another host, SIPp is setup as a traffic generator to send Real-time Transport Protocol (RTP) traffic. The experimental hardware devices are listed in Table 1.

TABLE I. HARDWARE SPECIFICATIONS OF EXPERIMENTAL DEVICES

	CPU	RAM	Operating System	
UC Client 1	Intel Core i7-3770 @3.4GHz x 8	16 GB	Ubuntu 14.04 LTS	
UC Client 2	Intel Core i7-3770 @3.4GHz x 8	16 GB	Ubuntu 14.04 LTS	
SIPp	Intel Core i7-3770 @3.4GHz x 8	16 GB	Ubuntu 14.04 LTS	
Cloud System	Intel Core i7-4470 @3.4GHZ x 8	16 GB	VMware ESXi Server on Windows Server 2012	UC Server on RedHat Linux 4.4.7-4
Router: Cisco 2911 Integrated Services				
Switch: Cisco Catalyst 3560 series				

As this experiment is conducted in a closed network the result revealed in this experiment is expected to be better in performance than in a real world scenario. In practice, there may be other factors, such as bandwidth limitations, which may affect end-to-end UC delay. As such, the overhead of the IPSec traffic may have an effect in the quality of UC communications. While some of the delays are tolerable for data traffic, it is critical for UC communications if delays occur. For example, the voice quality degrades (voice communications breaks) if the round-trip time delay (RTT), the time required for a signal to travel from the caller to callee and back again, exceeds about 250 milliseconds. The ITU G.114 specification [14] recommends no more than 150 ms end-to-end delay with one-way communication to maintain good voice quality. There are also other factors that can affect voice/video quality such as packet loss and jitter.

In order to measure the latency under this setting, the SIPp is used to generate RTP traffic. We create a simple setup using SIPp (1) to measure the call processing performance of our UC system running on the cloud system by using the following syntax for a SIPp command.

The experiment has been repeated three times and the results revealed in this paper are the mean (average) value of the three measurements, rounded to the nearest whole number.

sipp –sn uac –d “calls in milliseconds” –s “extension number” “IP address of a server”–l “number of simultaneous calls” (1)

That is, this command generates sip invites as a client with duration of calls in milliseconds, dials the IP address of our UCaaS server, and reaches the extension number with a limit to the given number of simultaneous calls. A high level design of our experiment is shown in Fig. 3.

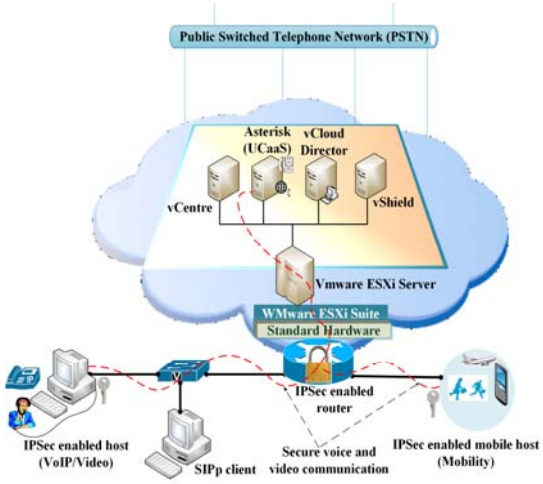

Fig. 3. Host-to-site IPSec communications

A. G.711 codec Performance measurement (Latency) of VoIP traffic without IPSec

In this experiment we run a latency test on the plain VoIP traffic without IPSec (no encryption). Using the SIPp command with the syntax **sipp 10.0.0.2 -sn uac -i 10.0.0.155 -s 5555 -m 100 -l 100 -r 30 -d 30000** we discovered how the system performs with increased stress levels without IPSec enabled as shown in Fig. 4. Basically, the system receives calls at a rate of 30 calls per second, with a limit of specified open calls. The purpose of this experiment is to find the total maximum simultaneous calls the server can handle to determine its capacity and the time it takes to process and

complete the call. For instance, in the case of 100 simultaneous calls, we run the following SIPp command to observe the results of the "response time repartition" to obtain the value of the total time it takes to complete the call. In order to determine the maximum capacity of the UCaaS server, we tune the parameters that define the traffic levels.

For instance, if we take 100 simultaneous calls, the latency of all the 100 calls (the mean value of 100 calls in the first experiment, 99 calls in the second and third experiments) is below 10 milliseconds (ms), which is within the acceptable performance for voice traffic. However, when we run 1200 simultaneous calls, we observed that about 18 calls are dropped (timed out), as it takes more than 200 ms to complete the call. Based on this experiment, the UCaaS system without IPSec, the UC server hosted on the cloud system can handle about 1100 simultaneous calls within the acceptable latency range for VoIP.

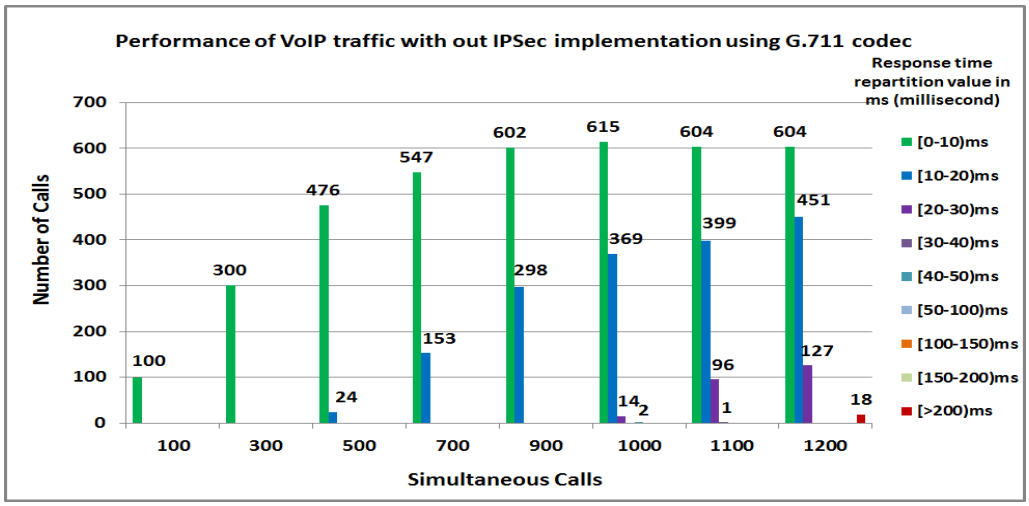

Fig. 4. Performance of VoIP traffic without IPSec using the G.711 codec

B. *G.711 codec Performance measurement (latency) for UC traffic with IPSec*

In this scenario we enabled our IPSec gateway for UC traffic and the results shown in Fig. 4 were obtained.

.

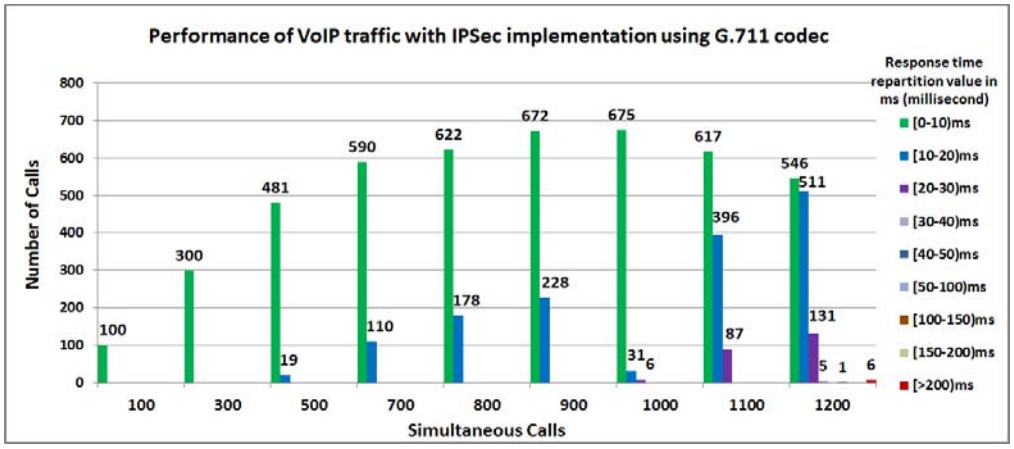

Fig. 5. Performance of VoIP traffic with IPSec using the G.711 codec

When IPSec is implemented, we noticed a slightly better performance in terms of VoIP latency than that of plain voice traffic. For instance, as shown in Fig. 4, when we run 900 simultaneous calls in a plain VoIP (no encryption) situation the latency for about 602 calls out of 900 was less than 10 ms and for 298 calls between 10 to less than 20 ms. However, in the case of encrypted voice traffic as shown in Fig. 5, when

we run 900 simultaneous calls we observed a higher number of calls completed below 10ms. About 672 calls out of the 900 completed in less than 10 ms and about 228 calls between 10 to less than 20. From these two experiments, surprisingly, we observed that the UC server with encrypted VoIP can process more calls in less time than that of unencrypted VoIP. However, both setups are identical, in terms of the total number of calls the server can handle with in the acceptable performance for VoIP traffic

C. *G.722 codec Performance measurement (Latency) of VoIP traffic without IPSec*

With this test, we analyse the UC server in terms of the voice/video latency using the G.722 codec. G.722 provides improved speech quality comparing to that of the narrowband speech coder, G.711, due to a wider speech bandwidth of 50–7000 Hz operating at a bit rate of 24kbps or 32kbps. G.722 codec has higher speech quality than G.711 however it is not widely used. We use this codec in our experiment as "Asterisk", our UCaaS server, supports the implementation of this codec.

Fig. 6 shows the result for voice latency when using the G.722 audio codec without IPSec implementation.

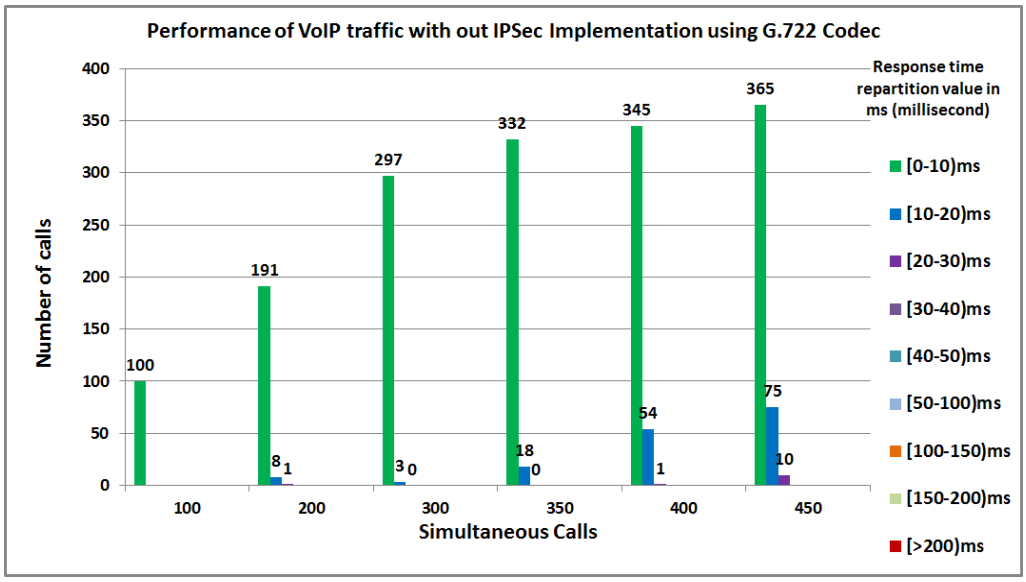

Fig. 6. Performance of VoIP traffic without IPSec using the G.722 codec

D. *Performance measurement (Latency) of VoIP traffic with IPSec implementation using G.722 codec*

Similarly, we ran tests for VoIP latency with IPSec implemented using the G.722 codec and the result is shown in Fig. 7.

Surprisingly, what we have observed from this experiment is that there is not much difference in UC performance in terms of latency whether VoIP traffic is encrypted or not using the G.711 codec. The reason could be that we used an Intel Core i7 CPU processor @ 3.4GHZ x 8 for our performance tests. That can implement some of the complex and performance intensive steps of the Advanced Encryption Standard (AES) algorithm using hardware and thus accelerates the execution of the AES algorithm. However, when we test the latency using the G.722 as the audio codec we observed the performance of the UC server, in terms of the VoIP latency, to be impacted when IPSec is implemented. What we have observed from the results shown in Fig. 6 and Fig. 7 is that the UC server can handle 100 fewer concurrent calls when IPSec is implemented than that of the UC server with plain VoIP traffic. Based on the experiment we note that the selection of the audio codec is crucial when considering IPSec implementation for VoIP traffic encryption.

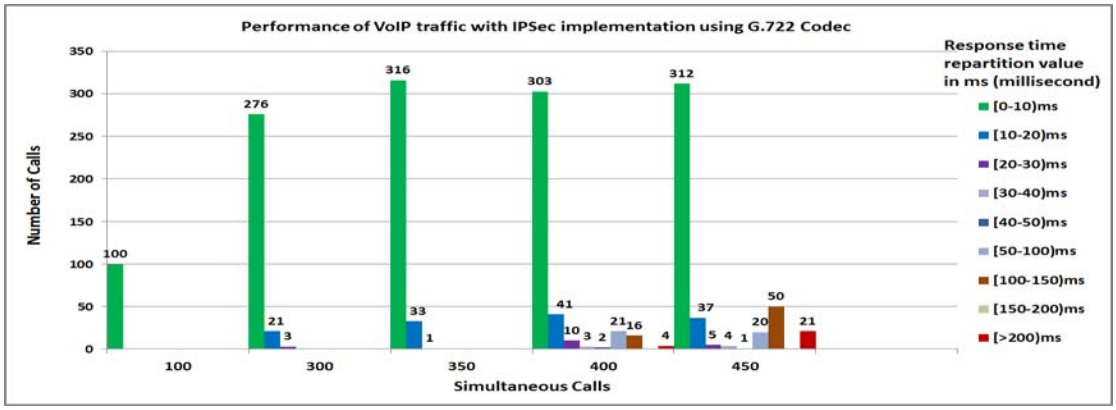

Fig. 7. Performance of VoIP traffic with IPSec using the G.722 codec

VI. Conclusion and Future Work

The paper presents different experimental results highlighting the impact of security on performance. The empirical tests are valuable for those seeking UCaaS provisiong and other forms of communications, and this did extend the discussion of such issues to include performance. The research presents new information regarding this issue and allows cloud providers the clarity to move more rapidly to secure cloud systems.

The significance of this research is based upon the provision of detailed technical advice and guidance to those involved in planning, designing and managing security controls of unified communications security on premises as well as in the cloud, viz. in public, hybrid and private cloud structures.

Implementing security in UC systems is necessary, but performance may have to be considered in the light of delivery priorities. Additionally, the performance and the manageability of network security controls both need to be considered in large-scale enterprise deployments. This research is able to provide detailed technical advice and guidance on appropriate security metrics for UC traffic confidentiality and integrity parameters which may be needed to secure confidential conversations in transit, in a variety of situations. The advice and recommendations provided from this research are affirmed by the results of performance testing. In conclusion, the potential security benefits of IPSec deployment should be balanced against performance and manageability parameters.

UC traffic is more sensitive to latency, jitter and packet loss than most network applications. As such, this research will continue to investigate and evaluate the overall quality of service factors for UC implementation in terms of its latency, jitter and packet loss.

Acknowledgment

Our VMware ESXi, UCaaS and IPSec implementation and performance testing has been conducted on a networking laboratory with student-formed teams. The authors appreciate the contributions from Jiexi Li, Xiaoxiang Ma and Keng U Fung.

References

[1] Australian Government. (2014, October). *Australian Government Cloud Computing Policy (3rd ed.)*. [Online] Available:http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Inst. of Stan and Tech., Gaithersburg, MD, Sep. 2011.

[3] A. D. Tesfamicael et al., "Design and Implementation of Unified Communications as a Service based on the Openstack Cloud Environment," in IEEE International Conference on Computational Intelligence and Communication Technology., Ghaziabad, 2015, pp. 117-122.

[4] W. B. Diab et al., "VPN analysis and new perspective for securing voice over VPN networks," in Fourth International Conference on Networking and Services., Gosier, 2008, pp. 73–78.

[5] N. Kazemi et al., "Evaluation of IPsec overhead for VoIP using a bare PC," in 2nd International Conference on Computer Engineering and Technology., Chengdu, 2010, pp. 586–589.

[6] A. Nascimento et al., "Can i add a secure VoIP call?," in International Symposium on a World of Wireless, Mobile and Multimedia Networks., Buffalo-Niagara Falls, NY, 2006, pp. 435–437.

[7] J. Oetting and K. King, "The impact of IPsec on DoD Teleport throughput efficiency," in 2004 IEEE Military Communications Conference., Monterey, CA, 2004, pp. 717-721.

[8] Y. C. Sung and Y. B. Lin, "IPsec-based VoIP performance in WLAN environments," IEEE Internet Comput., vol. 12, no. 6, pp. 77–82, Dec. 2008.

[9] T. Yildirim and P. J. Radcliffe, "VoIP traffic classification in IPSec tunnels," in 2010 International Conference on Electronics and Information Engineering., Kyoto, 2010, pp. 151–157.

[10] ITU-T. (1990, June 28). G.711 : Pulse code modulation (PCM) of voice frequencies. [Online]. Available: http://www.itu.int/rec/T-REC-G.711-198811-I/en.

[11] ITU-T. (1990, June 28). ITU-T Recommendation G.722. [Online]. Available: http://www. itu.int/rec/T-REC-G.722.

[12] N. Thanthry et al., "Alternate encryption scheme for VoIP traffic," in 43rd Annual 2009 International Carnahan Conference on Security Technology., Zurich, 2009, pp. 178–183.

[13] D. R. Kuhn et al., "Security Considerations for Voice Over IP Systems" National Inst. of Stan and Tech., Gaithersburg, MD, Jan. 2005.

[14] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," BBN Corp., Cambridge, MA, Nov. 1998.