Security Issues in VoIP and Solutions through Cloud Computing

A. R. M. Ahmed, D. K. S. Dematagoda, M. I. I. Ahamed, W. I. S. J. de Alwis, J. A. D. S. G. Jayasinhe, Dhishan Dammearachchi

Sri Lanka Institute of Information Technology

Abstract- VoIP Stands for Voice over Internet Protocol which is an alternative way of making telephone calls at a cheaper rate. Traditional telephone calls are replaced by VoIP rapidly as a result of cost efficient. The basic necessities of utilizing VoIP comprises of hardware and software such as a computer or any device which supports it, including microphone and speaker, with a relevant VoIP related software, and an active internet connection. VoIP transmits the sound that is received by the microphone over standard internet infrastructure using IP Protocol to the particular recipient(s). In order to establish a complete VoIP system for making calls from one person to another person, a VoIP service provider is compulsory, which can also be known as a central nervous system resembling to passing of messages to and fro in the human body. Cloud computing is another concept which has risen far well in the enterprises. Cloud computing helps functioning the organizations and their systems while upgrades are taken place without affecting the system. In a layman's term, everything is connected to a system where users can also gain access to additional systems other than the main system which is indirectly connected to the main system. In this research, we discuss the reliability of VoIP in terms of Bandwidth dependency, Power dependency and Security threats and also how to overcome the dependencies and threats through cloud computing**.**

Index Terms- VoIP; Reliability; Security issues; cloud computing

I. INTRODUCTION

Cloud Computing", a rising concept throughout the years in the industry, is derived from the technical terminology called storm from its birth. Wikipedia describes the cloud computing as a paradigm of computing in which is dynamically scalable and rapidly virtualized resources are provided as a service throughout the internet." In the context of VoIP, the Cloud is actually a means by which is carrying and service providers can give infrastructures component and application platforms to customers economically whilst being beneficial and as required or which are on demand. But how is hype differentiated from reality? And, is the Cloud truly relevant in the services of telecommunications industry?[10] Inside the VoIP industry, companies which are based on cloud technology, go to security infrastructure and policies which the Software as a Service (SaaS) provider has implemented can minimize market using a suite of services created to fit their target consumers' and enterprises' procured requirements. From collocation services in premium sites all over the world to Class four wholesale and Class five retail infrastructure, to platforms and software around the world, it is essential to understand the challenges of sourcing the cloud elements of these types of services. There are actually three relevant categories. [1]

1.1 Infrastructure as a Service (IaaS)

Resources that are delivered by means of service such as power, hardware, bandwidth and core components of network, are fundamental requisites in providing services and 'cloud' infrastructure. Items like UPS, CPU, generator options, network components,data storage and disaster recovery procedures, etc., must be evaluated. Further, clientele may be offered accessibility in order for Cloud Network components analysis to achieve more transparency [2]

1.2 Platform as a-Service (PaaS)

Choosing the platform on which VoIP services will be launched is vital to the security and reliability of the cloud-based offering. An acknowledged trending manufacturer will deliver a scalable, reliable and redundant platform in conjunction with tech support process and ongoing engineering and expertise to ensure stability. VoIP Logic depends and varies on several experienced hardware and software vendors. The quality of known platform vendors is achieved through their established records. These connections among us, enables to score relatively higher in end-user satisfaction [2].

1.3 Software as a Service (SaaS)

These applications are accessed on the web via browsers. Policies are generally set in place by the operator which provides the necessary flexibility and reliability. For example, in a scenario such that the user ponders about the significance of the satellite communication along with cloud based VoIP. This research paper discusses vulnerability to fraudulent, adequate protection for security such as denial of service (DOS) attacks, IP addresses or domain addresses hijacking, unauthorized traffic, etc. it can be another substantial consideration. It is pragmatic to partner with an IaaS, PaaS and SaaS provider when a service provider has extensively researched their own requirements including the capabilities of their network, the platforms as well as the managed services provider. It is beneficial to offset not owning and operating your own infrastructure. Various configuration decisions can be made having a better cloud service whereas the responsibilities will nevertheless require active attention along with a full comprehension of all facets of a VOIP (Voice Over IP) service offerings.[10]

VoIP in Cloud communications

Cloud communications are Internet-based voice and data communications where telecommunications applications, switching and storage are hosted by a third-party outside of the organization using them, and they are accessed over the public Internet. Cloud services is a broad term, referring primarily to data-centre-hosted services that are run and accessed over an Internet infrastructure. Until recently, these services have been data-centric, but with the evolution of VoIP (voice over Internet protocol), voice has become part of the cloud phenomenon. Cloud telephony refers specifically to voice services and more specifically the replacement of conventional business telephone equipment, such as a Private branch exchange (PBX), with third-party VoIP service.

II. BACKGROUND AND RELATED WORKS

At the beginning of the research the development team studied various research papers and documents from various sources. There is no similar existing system for this system. Summary of the findings is follows;

Cloud based VoIP Application in Aircraft Data Networks [3] is a Research that talked about the importance of the satellite communication along with cloud based VoIP. In this research paper it discussed about the different VOIP protocols named Session Initiated Protocol (SIP), Skinny Client Control Protocol (SCCP) and H.323. Proposed architecture of this research referred to as Cloud based VoIP ADN Architecture (C-VoIP ADNA). First requested data from the flight send to the satellite then the satellite send the request to the ground station situated on the earth. Nearest ground station receives the signal and sends it to the VoIP application running on the cloud. The data is fetched from the cloud; and it is send back to the Storage Area Network (SAN) from where the ground station receives data; then the data is fetched from the cloud, it is send back to the SAN from where the ground station receives it. Using a high speed link all the ground stations are connected to the SAN.

Metamorphosis in VOIP Cloud Computing Services Used in VOIP [4] using different servers transfer the voice over data network in the traditional VoIP. The servers located on the different geographical areas that hard to transfer the voice over the internet. Over the cloud Voice or data calls can transfer. Using different ISP (Internet Service provider) business servers route the calls to the remote/home office or to the enterprises. To transport voice over data network in the traditional VoIP human voice must be “packetized”. When transferring the voices in traditional VOIP using different servers it automatically increases the cost of communication and decreases the graph of quality of service. This research discussed about the way that to provide the good quality service to transfer the voice over the network.

Security and Privacy in Cloud Computing: A Survey [1] this is a survey for identifying the security and privacy status of cloud computing. This research investigates the security and privacy concerns current cloud computing systems. Cloud computing used to refer both applications delivered as services over the internet. Most of the users haven’t correct idea about the security of the cloud computing, it allows providers to develop some functions such as scalability, availability, reliability, performance and etc. for make it more user friendly.

Cloud Computing Security – Trends and Research Directions [1] this research divides the common security issues around the cloud computing into four main categories as follows. Cloud infrastructure, platform and hosted code- This category discussed about possible virtualization, storage and networking vulnerabilities. And this covered vulnerabilities that may be contained in the cloud software hosted code and platform stack, which gets immigrated to cloud and also the physical data- center security aspects.

Data- In this category concerns about the function as follows; data remanence, data integrity, data lock in data provenance, data confidentiality and user privacy.

Compliance- According to its size and disruptive influence, cloud is tempting attention from regulatory agencies, especially around data location and security audit.

Access – This includes the content around cloud access, user identity management and encrypted data communication.

Cloud Computing: Issues and Challenges [5] This research discussed about the current adoption associated with numerous challenges in Cloud Computing named Costing Model, Service Level Agreement, multi-tenancy model, what to migrate and Charging Model. A number of cloud computing are essential to the level difference. Before choosing the best IT resources and assets needed to keep an organization. In - house IT assets and capabilities to perform their basic functions and activities related to the outsourcing of cloud while. Data Security and Privacy Protection Issues in

Cloud computing [6] according to this research can identified the many security issues related with cloud computing. Some of the safety issues can be mentioned as follows; long-term viability, data segregation, Privileged user access, investigative support, regulatory compliance, data location and recovery. Traditional data security and privacy protection is similar to the content of data security and privacy protection in cloud. And also is related in every stage of the data life cycle.

VoIP Security [7] A VoIP deployment faces a various threats from different networking layers and trusted areas within the network. According to this research attacks that VoIP network faced can be categorized as follows:

VoIP Application Level Attacks, Eavesdropping, Call Hijacking, Message Integrity, Toll Fraud, Resource exhaustion and Denial of and etc. Non Trusted Identities, VoIP Protocols Design Flaws, Functional protocol testing or Fuzzing, Availability, Attacks against the underlying VoIP devices’ Operating System, Configuration Weaknesses in VoIP devices, Physical access are some of other attacks that VOIP network faced.

Security Challenges in Cloud Computing According to this research in cloud computing there are two major challenges named security and privacy. Virtual environment of cloud computing lets user access computing power that violate that contained within their physical world. User has to transfer data throughout the cloud for entering this virtual environment. There are several areas in Information security can be discussed, such as Losing control over data, Data Integrity, Risk of Seizure, Incompatibility Issue, Constant Feature Additions, Failure in Provider’s Security, Cloud Provider Goes Down are some of

Information security issues can be faced. And there are network security issues also with the cloud computing when transmitting the data. The issues can listed as follows; Distributed Denial of Service (DDOS) Attack, Man in the Middle Attack, IP Spoofing, Port Scanning, Packet Sniffing and etc [8].

A Review on Cloud Computing: Design Challenges in Architecture and Security in this Research paper discussed about the design challenges in cloud computing architecture and the security challenges that can faced.by using the cloud computing most of the business companies deducted their It cost. But most of the times the cloud based computing environment easily hacked by the other users [3]. As a solution Most of the times it can be encrypt the data. But in cloud computing it's hard to encrypt it. So no security for the system users who used the cloud based computing environment [9].

A Survey on Security Issues in Cloud Computing in this research Define and analyze the several unresolved issues threatening to the Cloud computing. Cloud servers deny the access to data lying in the cloud in any sort of internet breakdown. Sometimes the whole system had been down for hours. There are several network attacks in cloud computing environment such as DNS attacks, SNIFFER attacks, Issue of Reused IP Address, BGP prefix hijacking. In Application level security this research discussed about Security concerns with the hypervisor, Denial of service attacks, Distributed denial of service attacks, Cookie poisoning, Hidden field manipulation, Backdoor and debug options and etc. This research discussed about the various solutions against to this attacks [4].

III. Results and Discussion

In Voice over Internet Protocol (VoIP) the voice is transmitted as compressed packets and delivered by a decompression algorithm and this has to be taken place in a very short amount of time maybe milliseconds if this is not done properly the quality of the VoIP is affected sometimes the sender may echo his own voice. VoIP is highly dependable on the Bandwidth, VoIP normally does not work over a dialup connection, and it works great on a mobile broadband or a wireless network or a cellular connection.

VoIP does not work if there is no active internet connection it means that if there is no internet then the user cannot communicate through VoIP. Poor connection is also a major disadvantage, when using VoIP if the connection quality is not good the user will not be able to communicate with the other party and the user will end up hating the technology and the network provider. Using a shared connection in VoIP also affect the quality of the VoIP calls, if the user is connected over a high speed broadband connection its effect will be minimum also if there are several users connected through the connection each user will be using the bandwidth and it leaves the user a little bandwidth which will not be enough to reach the quality VoIP calls.

To communicate through VoIP it also needs electrical power, if there is a power interruption the modem, router will not work so the user will not be able to use the service, although UPS (Uninterrupted Power Supply) is available it will allow the user to connect to the internet only for a certain period of time.

There are several security threats concerned to VoIP theft of the service is a threat where the hacker steals the service while the cost is passed to another person, Eavesdropping or interception of calls is also a major security threat where the hacker steals confidential information about the users and uses them for his needs, DOS attack Denial Of Service is an attack on a network, the hacker floods the target network and disrupts the service of the user, through this the hacker gained the control of administration privileges of the service. Call tampering involves the tampering a call in progress in this the hacker send noise packets to the network and affects the quality of the VoIP call it causes a long silent in calls and delayed response from the receiver from the other end. Man in the middle is also a security threat where the hacker alters the signal by sending SIP (Session Initiating Protocol) messages and possibly altering the communication between two parties who think that they are directly connected to each other .The above security threats can be overcome, as a counter measure the user can use encryption, use secure wireless network, physical security like firewall or use a authentication method in VoIP protocol.

When looking the mentioned problems regarding the reliability of VoIP systems, Backup power is important for an uninterrupted network connection this will help to retain the internet connection in the router or the broadband device if there is a power failure. Broadband bonding is joining multiple bandwidth lines to increase the bandwidth of the connection and also acts as a backup in case one connection fails. Using a dedicated network for VoIP connection allows the user to be secure from any virus or attacks, by connecting it to a firewall the user can allow only the specific protocols required for VoIP communication and block the others. Using separate lines for internet and voice will allow the user to use VoIP with high quality bandwidth.

IV. Conclusion

As a conclusion, we've briefly discussed in this research paper about VOIP and Cloud computing, several dependencies in VOIP such as Bandwidth and Power and the security threats and how to overcome these issues by using Cloud Computing technology. Literature review emphasizes mainly about cloud based VOIP applications, the importance of the VoIP services and traditional methods of VoIP, Classifying Cloud computing into four parts and the Data security of Cloud computing and VoIP security. By doing the background research works of the Literature review, we briefly discussed about the importance of the above topics, as well as the problems which can be solved using our new system. Furthermore, we discussed how Cloud computing could affect VoIP as infrastructure, platform and software categories. Therefore, it is important to know that by using the Cloud computing, especially Cloud communications in VoIP could help to deduct the dependencies in VoIP and reduce the risk of current security threats in VoIP. This would be a vital concern in future and by solving these, it would help to get the maximum benefit out from the VoIP system using cloud computing.

V. Future Work

VoIP Bandwidth

VOIP Bandwidth consumption naturally depends on the codec used. When calculating bandwidth VOIP, one can't assume that every channel is used all the time. Normal conversation includes a lot of silence, which often means no packets are sent at all. So even if one voice call sets up two 64 Kbit RTP streams over UDP over IP over Ethernet the full bandwidth is not used at all times.

VoIP Threat

1) Social threats are aimed directly against humans. For example, misconfigurations, bugs or bad protocol interactions in VoIP systems may enable or facilitate attacks that misrepresent the identity of malicious parties to users. Such attacks may then act as stepping stones to further attacks such as phishing, theft of service, or unwanted contact (spam).

2) Eavesdropping, interception, and modification threats cover situations where an adversary can unlawfully and without authorization from the parties concerned listen in on the signaling (call setup) or the content of a VoIP session, and possibly modify aspects of that session while avoiding detection. Examples of such attacks include call re-routing and interception of unencrypted RTP sessions. [11]

3) Denial of service threats have the potential to deny users access to VoIP services. This may be particularly problematic in the case of emergencies, or when a DoS attack affects all of a user's or organization's communication capabilities (i.e., when all VoIP and data communications are multiplexed over the same network which can be targeted through a DoS attack). Such attacks may be VoIP-specific (exploiting flaws in the call setup or the implementation of services), or VoIPagnostic (e.g., generic traffic flooding attacks). They may also involve attacks with physical components (e.g., physically disconnecting or severing a cable) or through computing or other infrastructures (e.g., disabling the DNS server, or shutting down power)

4) Service abuse threats covers the improper use of VoIP services, especially (but not exclusively) in those situations where such services are offered in a commercial setting. Examples of such threats include toll fraud and billing avoidance.[12]

5) Physical access threats refer to inappropriate/unauthorized physical access to VoIP equipment, or to the physical layer of the network (following the ISO 7-layer network stack model).

6) Interruption of services threats refer to non-intentional problems that may nonetheless cause VoIP services to become unusable or inaccessible. Examples of such threats include loss of power due to inclement weather, resource exhaustion due to over-subscription, and performance issues that degrade call quality.

Acknowledgment

We would like to acknowledge with gratitude to every single personal who supported us to discover about Cloud computing, VOIP and every related topic. Special thank will be given to Mr. Dhishan Dhammearatchi who supervised us on this research to have a successful outcome.

References

[1] Z. Tari, "Security and Privacy in Cloud Computing," in IEEE Cloud Computing, vol. 1, no. 1, pp. 54-57, May 2014. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6848730&isnumber=6848686[Accessed:20.02.2016].

[2] A. Behl and K. Behl, "An analysis of cloud computing security issues," Information and Communication Technologies (WICT), 2012 World Congress on, Trivandrum, 2012, pp. 109-114. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6409059&isnumber=6409038 [Accessed:20.02.2016].

[3] "Analysis of Security Issues in Cloud Computing", INTERNATIONAL JOURNAL ON Advances in Information Sciences and Service Sciences, vol. 5, no. 5, pp. 493-500, 2013. Available at: http://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5 [Accessed:20.02.2016].

[4] A. Jasti, S. Mohapatra, B. Potluri and R. Pendse, "Cloud computing in Aircraft Data Network," Integrated Communications, Navigation and Surveilance Conference (ICNS), 2011, Herndon, VA, 2011, pp. E7-1-E7-8. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5935273&isnumber=5935117

[Accessed:20.02.2016].

[5] SA Patinge, PD Soni, "Metamorphosis in VOIP Cloud Computing Services Used in VOIP" ,vol 2, issue 2, February 2013, Available at: http://ijaiem.org/Volume2Issue2/IJAIEM-2013-02-28-057.pdf [Accessed:20.02.2016]

[6] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, Perth, WA, 2010, pp. 27-33. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5474674&isnumber=5474664.

[Accessed:20.02.2016].

[7] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, Hangzhou, 2012, pp. 647-651. Available at: http://xa.yimg.com/kq/groups/2584474/417972861/name/NDU-1.pdf [Accessed:20.02.2016].

[8] DC Sicker, T Lookabaugh, VoIP Security,2004,Available at: http://146.163.150.3/~wwhite/Caballero/Sicker_ACMQueue2004.pdf [Accessed:20.02.2016].

[9] "Cloud Computing - voip-info.org", Voip-info.org, 2016. [Online]. Available: http://www.voip-info.org/wiki/view/Cloud+Computing. [Accessed: 18.03.2016].

[10] "nexogy", nexogy, 2016. [Online]. Available: https://nexogy.wordpress.com/. [Accessed: 20- Mar- 2016].

[11] T. Saadawi and L. Jordan, "Full text of "Cyber Infrastructure Protection"", Archive.org, 2016. [Online]. Available: http://archive.org/stream/CyberInfrastructureProtection_112/10-Cyber_djvu.txt. [Accessed: 19- Mar- 2016].

[12] A. Keromytis, "A Comprehensive Survey of Voice over IP Security Research", IEEE Communications Surveys & Tutorials, vol. 14, no. 2, pp. 514-537, 2012.

Authors

First Author – A. R. M. Ahmed, Undergraduate, Sri Lanka Institute of Information Technology, Email: mushtaq.ahamed.ar@gmail.com

Second Author – D. K. S. Dematagoda, Undergraduate, Sri Lanka Institute of Information Technology, Email: kris.sanjeewa@gmail.com

Third Author – M. I. I. Ahamed, Undergraduate, Sri Lanka Institute of Information Technology, Email: ijaazops@gmail.com
Fourth Author – J. A. D. S. G. Jayasinghe, Undergraduate, Sri Lanka Institute of Information Technology, Email: shanikajayasinghe90@gmail.com
Fifth Author – W. I. S. J. de Alwis, Undergraduate, Sri Lanka Institute of Information Technology, Email: isurudealwis@gmail.com

Sixth Author - Dhishan Dhammearatchi, Lecturer at Sri Lanka Institute of Information Technology and Network Engineer, Sri Lanka Institute of Information Technology, Email: dhishandhammearatchi@gmail.com

Correspondence Author – A. R. M. Ahmed, Undergraduate, Sri Lanka Institute of Information Technology, Email: mushtaq.ahamed.ar@gmail.com