EXECUTIVE SUMMARY

Cloud Computing has become the global technology enabler for corporate businesses and home users relying on IT services today. Cloud Computing offers unlimited flexible computing resources, storage and network capacity to seamlessly meet the service demands offering rental models, hosting options, virtual infrastructure, maximum utilization and availability. Cloud computing also benefits technology organizations, service providers and the home users in reducing the capital expenditure and setup costs on a regular basis. Access to high speed links and Internet availability has further led to the increase in adoption of Cloud based services by global corporates working in offices or from remote locations as well as the home users.

Since Cloud Computing utilizes the Internet as the primary communication medium, traffic from unsecure Internet locations flow into public data centers, on premise corporate systems and home computers. This exposes data and computing resources to external threats and cyber-attackers. To realize the full potential of Cloud Computing and be successful, security threats and challenges need to be addressed and managed. To counter these, Cloud service providers and organizations deploy firewalls and intrusion detection systems in data centers, while home users install antivirus and personal firewalls on desktops and laptops.

However, when receiving and sending traffic to the unsecure Internet, inbound access to the corporate web portals, hosted applications, email servers and computing systems is essential. Cloud service providers and corporate organizations open access to ports on the edge and network devices. In doing so, the corporate resources, devices and data is again exposed to the cyber threats at network and application level. Data centers, systems and infrastructure devices are constantly targeted by cyber attackers and remain under constant threats primarily from Malware and Distributed Denial of Service attacks. Even though these attacks are not unique threats in itself, the detection and mitigation continues to be the top security challenge. These attacks constantly evolve into a new threat levels impacting the security solutions implemented in Cloud and On Premise hosting environments. Every segment is vulnerable to the DDoS and malware attacks which continue to increase in size, sophistication and frequency. Thus there is an immediate need to have a secure security architecture that can detect and mitigate

the network layer attacks and the application layer attacks to help normalize the web traffic and ensure the hosted applications are available at all times.

This Thesis focuses primarily on designing a comprehensive infrastructure architecture for mitigating the Distributed Denial of Service attacks on Hybrid Clouds and presents a Malware detection system to mitigate Ransomware attacks. The Researcher first performed a survey to understand security issues and the impact of cyber-attacks on Cloud Computing environments. The Researcher reviewed research papers and manuscripts published between January 2012 and December 2016 on Cloud Computing, Denial of Service attacks and Malware detection and mitigation approaches. The Researcher also reviewed existing solutions to mitigate the Distributed Denial of Service attacks as well as Malware attacks. The Researcher then designed and implemented Cloud based system to detect malware for mitigating Ransomware attacks. The Researcher then designed and implemented the secure infrastructure architecture to mitigate Distributed Denial of Service attacks on Hybrid Cloud environments. Network and Application level attacks are performed on the proposed infrastructures and the results compared with single tier data center architecture design. Future research directions are also outlined in this Thesis.

THESIS ORGANIZATION

The main security challenges impacting Cloud based services and environments are the Distributed Denial of Service and Malware attacks. The present research work is carried out to design and implement secure architecture to mitigate Distributed Denial of Service and Malware attacks, the entire work is organized in terms of eight chapters.

The First Chapter gives a brief introduction about Cloud Computing, presents the top security issues regarding Distributed Denial of Service attacks and Malware attacks impacting Cloud environments. Tools required for performing the cyber-attacks are illustrated in this chapter along with a brief overview on the cryptographic algorithms for Cloud security. A brief review of the Thesis is then presented along with motivation and objectives of the work.

The Second Chapter contains the various literature reviews. Since the aim of the work is on designing secure architecture to mitigate the Distributed Denial of Services attacks on Hybrid Clouds and detecting and blocking Ransomware, hence the parameters for determining effective countermeasure strategies are reviewed in this chapter. A new DDoS Classification Taxonomy is also introduced in this chapter.

The Third Chapter presents the latest cyber-attack trends regarding the recent DDoS attacks on Cloud environments. In order to understand the research topic in detail, the Researcher conducted a cyber-security survey on cyber-attacks and security issues faced by various organizations. The outcome of the survey pointed to Ransomware and Distributed Denial of Service attacks as the topmost security related threats faced by the organizations. This chapter presents strategies and existing solutions for mitigating DDoS attacks on Cloud based environments.

The Fourth Chapter deals with Ransomware as the new age digital cyber threat. The different methods adopted by cyber criminals for propagating malware are discussed in this chapter. The Researcher designed and implemented the Malware detection system in form of virtual environment with sandboxes hosted on the Cloud and presents the comparison evaluations to determine the effectiveness of the proposed anti-malware solution.

The Fifth Chapter deals with the analysis of Cryptographic Algorithms for Cloud environments. Since the user data flows on network circuits and devices with session encryption between the Cloud application systems and Cloud service consumers, the emphasis is primarily on reviewing the algorithms to use for security systems and devices that utilize Cloud based applications and services.

The Sixth Chapter presents the implementation of proposed infrastructure design for mitigating DDoS attacks Hybrid Cloud environments. The Researcher designed and implemented two infrastructure designs, the first as single tier architecture and the second as three tier architecture. These infrastructure simulated Cloud hosted service applications by using Windows Server hosting the web application portal and running IIS with SQL Server Database as the backend.

The Seventh Chapter is dedicated to validation of the work presented. The Researcher executed DDoS simulating network and application layer cyber-attacks on the Single Tier infrastructure and the proposed Three Tier infrastructure. The results are then analyzed taking into account the key performance parameters based on 'real user monitoring' and compared for Cloud application responses.

The Eighth Chapter has the concluding note about the work with future scope. At the end of this Thesis a detailed relevant bibliography is reported that deals with the reported work in the area of Distributed Denial of Service attacks.