CHAPTER 8

CONCLUSION

8.1 CONCLUSION

As Cloud Computing technology adopts and advances towards embracing Cloud services, DDoS attacks have only increased in the past few years and show no signs of abating in volume, complexity or magnitude. The traditional IT defense systems on premise DDoS solutions or taken from ISPs can hardly be expected to take on the wide range of new types of dynamic attacks.

The author introduced Cloud Computing, DDoS and Ransomware in the first chapter and then reviewed research papers on DDoS and Ransomware in chapter 2, proposing a new DDoS Attack Classification, Parameters for DDoS Detection and a new DDoS Countermeasure Taxonomy.

Current Cyber Security threats and latest trends are illustrated in the second chapter, which also includes the DDoS based Survey performed by the author for gaining further insights. This lead to learnings that Ransomware and DDoS are among the top concerns for organizations. Existing DDoS mitigation solutions ranging from On-Premise, ISP DDoS Service offerings to Data Scrubbing are reviewed and the author proposed a secure architecture design for mitigating DDoS Attacks.

In the fourth chapter, the author investigated if malware can be detected using a Cloud based setup against Ransomware and if it can be better than the existing signature based anti-virus and scanners. The results indicate the performance of the proposed system is better than existing anti-malware solutions. The proposed system is illustrated in detail in this chapter.

With Cloud Computing emerging as a new thing in technology industry, public and private enterprise and corporate organizations are either using the Cloud services or in process of moving to the Cloud. Since network devices and servers employed cryptographic algorithms for data and traffic flow, the author analyzed Symmetric algorithms in the fifth chapter and AES is found to be a good candidate for key encryption while MD5 is faster when encoding. A combination of these algorithms can be implemented for securing end user data when using Cloud based applications.

The author implemented a secure infrastructure design in form of a three tier architecture in chapter six. DDoS attacks were performed on this infrastructure and compared with a single tier standard architecture. The results obtained from the DDoS attacks are presented in chapter seven of this which clearly indicate that by providing multiple tiers of network and web application security in form of defense layers, it is possible to protect the availability, data integrity and the performance of critical web applications, leading to higher customer confidence and lowering risks of under provisioning the security and network devices. This the main undertaking of this so that individuals and security administrators could make knowledgeable judgements regarding the emerging threats and attacks using the proposed three tier infrastructure design.

8.2 SUGGESTIONS FOR FUTURE WORK

Security is a major concern for distributed systems and services. Cloud computing has inherited all these security issues from its predecessors. The new technological challenges introduced by Cloud Computing like Multi Tenancy, Licensing, Resource Sharing, Computation Outsourcing, and external data warehousing, has increased compliance and data privacy concerns and made Cloud Computing platforms prone to newer security issues and threats. Therefore, security in cloud based solutions is highly crucial and may be considered as one of the most significant barriers to widespread adoption and acceptance.

Cloud Computing not only introduces additional risks and challenges but also adds various complications to deploying and maintaining the existing security standards. Widespread mobile device access and the on-demand services offered by Cloud providers amplify the security concerns and threats even further. Table below lists some of the known attacks and their consequences.

Attack Type	Category	Consequence
Denial of Service	Cloud Infrastructure	Service availability issue
Malware	Cloud Infrastructure	Service availability issue
Cross VM side-channel	Cloud Infrastructure	Information theft & leakage
Targeted shared memory	Cloud Infrastructure	Cloud malware injection
Phishing	Access Control	Unauthorized access
Botnets	Access Control	Unauthorized access
VM Rollback attack	Access Control	Brute force launch, info leakage

Table 8.1: Known Attacks in Cloud Computing Infrastructure

Given the various layers of Cloud Computing, Security threats and DDoS attacks can be contained at different layers in the Cloud computing environment. There are system level threats, where an intruder bypasses the security to get unauthorized access, as well as Cloud infrastructure and network level threats. Each component of a Cloud should be separately addressed and requires equal attention to protect a Cloud Computing platform as a whole. The potential challenges in Cloud Computing can be categorized into the following four categories shown in the Table 20 below.

Category Type	Areas Targeted
Cloud Infrastructure	Virtual Machines, Network & Platform level
Access Control	User & Resource level authentication
Data Outsourcing	Storage, Transfer & Data migration
Security Standards	Cloud Service Agreements, SLA, Implementations

Table 8.2: Cloud Computing Categories and Target Areas

These categories are closely related in various aspects and whenever one category is vulnerable to a certain attack, the other categories tend to fail ensuring the desired level of security. Thus, use of right set of security management design and level of precautions for a category can help strengthen the other categories a lot more and may eliminate the subsequent threats. As a result, security research in Cloud computing should address the complete set of issues in a holistic approach, instead of an iterative or categorical resolution of threats and the distributed denial of service attacks.

Thus DDoS mitigation has now become the topmost security priority for Cloud server providers and cloud service consumers and there is a need for a systematic, verifiable, and reliable Cloud service delivery framework for cloud computing delivery to be sustainable. Given the complex operational structure of Cloud Computing frameworks, secure provenance of Cloud based data and services will be always be a prominent research area in near future. Cloud Computing has become the leading computational model for online application delivery. Due to the significant benefits in terms of flexibility, performance, and efficiency, Cloud computing is slowly but steadily being adopted by almost all sectors. As more sectors migrate to Cloud computing platforms, it becomes very important for Cloud based services to be fully ready for not only performance expectations but also for all types of potential security issues, risks, and challenges.