CHAPTER 1
INTRODUCTION

1.1 ABSTRACT

This chapter presents an introduction to Cloud Computing concepts, the Cloud Architecture, Characteristics, Service and Deployment models. The chapter introduces Distributed Denial of Service attacks and software tools for executing the attacks. The chapter presents various methods adopted by cyber-criminals for Malware propagation and Ransomware attacks. Since Cloud computing involves user sessions and data transfers over unsecure circuits, the review of Cryptographic Algorithms for Cloud Computing is illustrated also in this chapter. A brief review is then presented along with the motivation and objectives of this research work.

1.2 INTRODUCTION TO CLOUD COMPUTING

Cloud Computing is well and truly the technology enabler for dynamic, on demand service delivery of Internet services and computing resources to corporates and end users. Cloud computing is referred to in different ways and approached from a variety of perspectives. As compared to traditional Information Technology services, Cloud services offer unlimited computing, storage and networking resources, with easy to pay options bundled with significantly enhanced service availability, reliability and reduced costs for infrastructure implementation and management. Cloud computing helps transform the services from being massive, cumbersome, high cost centers into proactive, agile, elastic services that can be utilized not just as IT Delivery, but also as a medium to conduct business globally.

Cloud Computing utilizes shared pool of resources comprising of Applications, Licenses, Operating systems, Virtualized Servers, Network and computing resources like CPU, Memory, Storage with minimum interaction from the Cloud service provider and the support teams. Hosting applications servers, deploying network devices or development platforms is swiftly provisioned and computing resources are released as per the end user demand. Cloud Computing includes five essential characteristics, four deployment models and three service models as shown by Jacobs (2012) and Qaisar (2012). With such a technology service features, it comes as no surprise that corporates,

government departments and small business enterprises plan to move their IT Service delivery and IT Infrastructure to the Cloud.

1.1.1 CLOUD COMPUTING ARCHITECTURE

Cloud Computing architecture relates to the components that are used for delivering Cloud services over the Internet. These components consist of the front end and the back end platforms, as referenced from Rolavideo Press book (2017). The Cloud architecture, network connectivity and the access process is a part of the cloud environment which comprises of the Internet as the delivery medium as illustrated below in Figure 1.1 and presented in the below section.

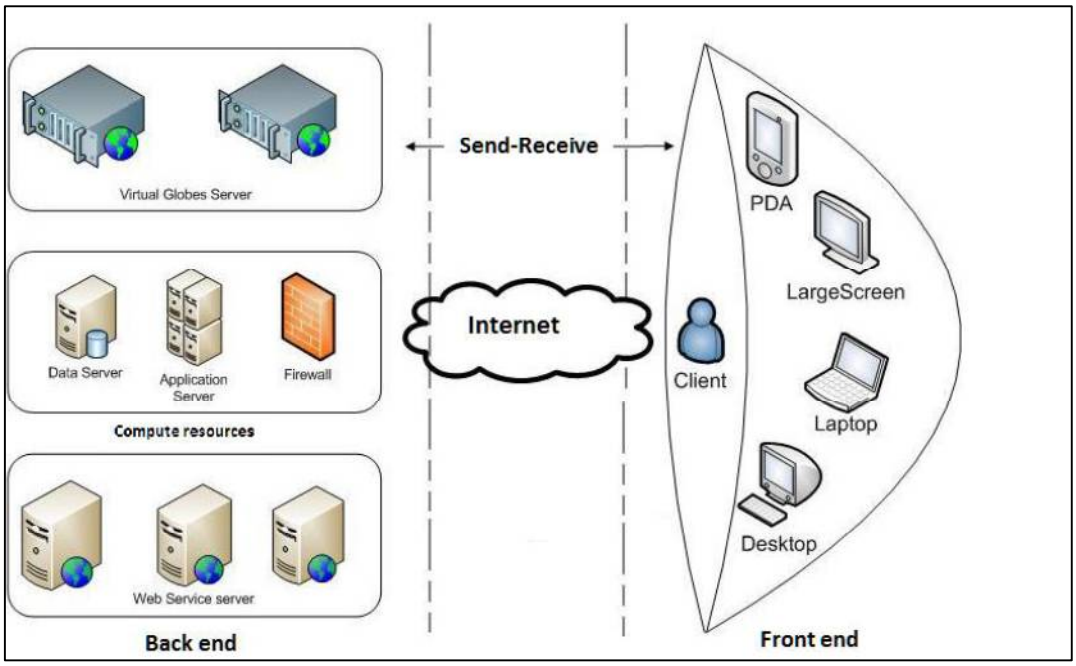


Figure 1.1: Cloud Computing Front End and Back End (Rolavideo Press Book 2017)

- **The Front End** consists of the client facing side running a thin client on the use system's web browser or executing a light weight application client on the user computer systems and mobile devices. This allows access to the cloud resources for the Cloud service consumer over a network which is usually the Internet.

- **The Back End** belongs to the Cloud service provider as part of a converged infrastructure consisting of network and hardware devices that comprise the 'Cloud' of computing environment providing the cloud based services. These devices are hosted in data centers as virtualized systems, application servers, backend databases, and storage and network devices. The back end application servers

consist of server operating systems, web portals and database software providing the 'Cloud Service' along with the central command servers. These administer the applications, monitoring the cloud traffic and cater to the cloud service consumer demands and ensure the Cloud service delivery runs smoothly.

Beyond these two main parts, the Cloud computing environment consists of the below mentioned sub-layers –

- **The Hardware Layer** consists of the physical hardware devices comprising of infrastructure components like Routers, Load Balancers, Network switches, Racks, Cabling, Power and Cooling systems running inside the data centers. Issues at this level include hardware failures, configuration issues, fault tolerance, power failures, air conditioning and heating.

- **The Infrastructure Layer** partitions the physical computing resources comprising of Servers, CPU, Memory and Storage using Virtualization. Dynamic computing resource management, allocation and commissioning or decommissioning of system tasks is performed here.

- **The Platform Layer** comprises of the software applications and operating systems running on the virtual machines for application deployment tasks which are utilized by developers for testing and hosting the cloud based applications.

- **The Application Layer** consists of the applications hosted in form of web portals accessed by the Cloud service consumers. These Cloud applications are provisioned and deployed in auto scaling mode using virtualized servers catering to the dynamic market and user demands. Unlike hosted web sites, Cloud applications leverage the auto scaling feature to achieve enhanced performance, maximum availability and offer low operating costs to the Cloud consumers.

1.1.2 CLOUD COMPUTING CHARACTERISTICS

To designate the data center hosted systems or web portal services on the Internet as a 'Cloud Service', five main characteristics are mandatory, as described by Philip (2015). These characteristics are explained as follows –

- Service on Demand

- Network Access over Virtual environment
- Resource Pooling
- Rapid Elasticity and Dynamic Scaling
- Measured Service

- Service on Demand is a Cloud consumer's option to use, rent and pay for Cloud services as required. Cloud vendors provide an application programming interface to enable use of the Cloud service as programmatically or automatically through a management application interface for the Cloud service consumer.
- Network Access over Virtual environment is the ability to provide computing infrastructure across users and being able to move user workloads, lower overheads and increase the quality of services for providing an efficient and on-demand infrastructure solution. This is accomplished by using virtualization over bare metal server systems running virtual machines with operating systems hosting web applications and services for Cloud delivery.

- Resource Pooling is the Cloud service feature to leverage applications and infrastructure while serving multiple consumers simultaneously in multi-tenanted mode. Cloud infrastructure requires investing a huge amount of capital expense along with an on-going operational cost. Cloud service provider implements the infrastructure to have the data center infrastructure, systems, licenses, applications available across as many consumers as possible.

- Rapid Elasticity and Dynamic Scaling the ability to commission and decommission computing resources on-demand in a dynamic manner. These resources are made available immediately and billed on monthly basis, so the Cloud service consumer pays only for the amount of services consumed.

- Measured Service is the Cloud provider's commercial entitlement for calculating the amount of computing resources utilized by consumers and charging then as part of the Cloud services offered to various end users.

1.1.3 CLOUD COMPUTING SERVICE MODELS

Cloud Computing Service Model is presented by Ubaidullah, et al. (2016) is illustrated in Figure 1.2 below is the adopted cloud Computing Service Model for Applications, Platforms and Infrastructure delivery.

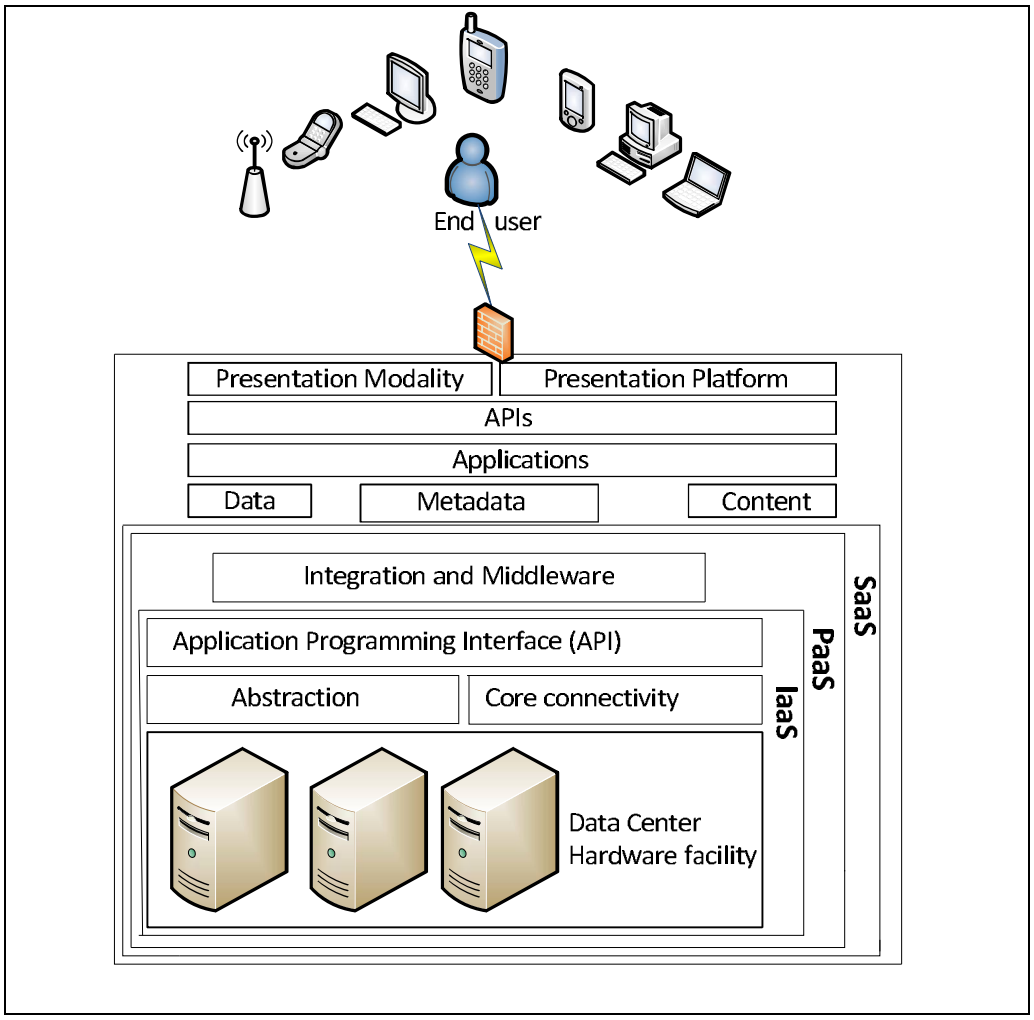


Figure 1.2: Cloud Computing Service Models

- **Software as a Service (SaaS)** targets end users and is concerned with on-demand delivery of applications by providing the Cloud application service subscribers access to application layer as shown by Huixin (2016). A physical copy of the software application is not required to be installed on user systems and accessed in form of a shared cloud product. The Cloud consumers are given access to the hosted application as per the service agreement but not to the application configuration or infrastructure implementation details. Some common SaaS examples are Salesforce On demand CRM, Web Conference on demand, Microsoft Office 365, Microsoft Sky Drive, Google Apps

- **Platform as a Service (PaaS)** targets the application developers and integrators by providing them with a pre-defined 'ready-to-use' environment in form of development framework platforms as a substitute to the on premise environment as described by Pratima, et al. (2015) and Bobák, et al. (2015). This service

incorporates the entire development requirements including coding, testing, hosting, deployment of web applications, databases and integration of different software applications. The Cloud provider grants a basic level of control to the developers for configuring the required resources and provisioning the developed platform. Some common PaaS examples are Google App engine, Microsoft Azure, Rack Space Cloud, Zoho Creator

- **Infrastructure as a Service (IaaS)** offers on demand dynamic provisioning of 'raw' computing infrastructure resources like virtual machines, hardware, software and storage. Here the subscribers outsource the resources requirements on a usage based pricing, paying only for the amount of IT infrastructure used and not having to worry about procurement of new hardware, maintaining them or facing any upgrade related issues. Dynamic scaling of infrastructure needs are done based on applications or resource demands as described by Shadha, et al. (2016) and Cash, et al. (2016). This service provides high level of control and responsibility over the configuration and utilization to the subscribers. IaaS examples are Amazon EC2, Rack Space, Attenda RTI, Eucalypt-us (Open source), Flexiscale

Apart from these delivery models, Anwar et al. (2015) described a set of specialized Cloud delivery models which are presented as follows.

- **Compute as a Service** provides on demand automated provisioning of virtual and physical computing resources, Servers, Operating systems, network devices like Firewalls, Routers and Load balancers. Access to these computing resources is provided via a management interface and can be shared or used individually.

- **Storage as a Service** eases the burden of data growth with data storage infrastructure on rent or lease. This service allows the administrators to own storage, have ability to transfer data to different storage tiers, send user or enterprise specific data sources to specific media locations such as SAN, disk or tapes. The service allows the ability to add or remove storage size as needed with virtually limitless capacity, all with an interactive self–service portal over the Internet.

- **Desktop as a Service** provides virtual desktop systems to setup and provision virtual machines on demand, as required. This service allows for optimum usage of the number of systems at any point of time and these systems can be accessed via

the Internet, logged to access data and run applications exactly as the office desktop workspace from any location.

- **Security as a Service** provides a portfolio for prevention, detection and resolution of Service services, skills, tools and processes as a subscription model. Security Incident Monitoring, Email Encryption, Identity and Access Management, Compliance Audits, Vulnerability Analysis, Digital Forensics, End point and Data Loss prevention, Network and Application Penetration Testing are some of the functions offered as in form of security services over the web. When leveraging security as a service, enterprises need to configure them as part of security of applications rather than creating and adopting security based on premise using standard algorithms for designing secure networks.

1.1.4 CLOUD DEPLOYMENT MODELS

Cloud Deployments models as described by Ziglari, et al. (2016) are implemented based on ownership, cost, access, security and size of the Cloud Computing environment are mentioned as follows –

- **Public Cloud** has no physical infrastructure hosted locally. The services, applications, storage and computing are offered commercially to end users by a Cloud Service Provider as described by Geetha, et al. (2016). The infrastructure environment and services are shared among multiple customers and managed by the third party. Organizations dynamically upload applications and provision resources through the Internet to an off-site Cloud provider. Wastage of computing resources is validated and limited as the Cloud service user only pay for whatever is used with access granted using an API over the Internet. Main characteristics that define a Public Cloud are Dynamic environment, pay as used, autonomy of self service and reliability. This makes the Public Cloud an obvious choice for those organizations with dynamic IT workload & applications like Email, Document or Image editors, Enterprise Resource Programs, working to develop applications for deployment, performing on collaborative projects or foresee sudden incremental capacity to cater to peak demands.

- **Private Cloud** has the infrastructure exclusively dedicated internally, available for the organization that manages itself or is large enough to share computing resources

and data between the departments within the same organization. The main characteristics that define Private Clouds are full control over user data, dedicated resources and enhanced security measures with greater level of customization. This model is an obvious choice for those seeking highest level of security along with data sovereignty and seeking control over consistency in IT Service delivery and deployments with priority to adhere to Compliance and efficiency at all times.

- **Community Cloud** involves having multiple groups with a common concern (compliance, security, jurisdictions) using the shared infrastructure. This Cloud environment is an obvious choice for Private HIPAA Compliance – health care organizations, Telecom companies which require to comply with FCC regulations or Government organizations that share classified data and resources among various ministries.

- **Hybrid Cloud** is an environment that deploys a combination of two or more Cloud models from private or public as described above. Here an integrated cloud service comprising of Public and Private Clouds is implemented. In this environment, application is deployed across environments with the front end being hosted on Public Cloud and the database is stored in an in-house or an on premise Private Cloud. Basic characteristics for this model are availability, optimal resource utilization, and data center consolidation. This ensures Hybrid Clouds are an obvious choice for enterprises seeking to use SaaS but are concerned about Security and Control. This is useful for environments seeking vertical market segment or have only Private Clouds for external access.

1.3 INTRODUCTION TO DDoS ATTACKS

Ensuring safety and security of information and communication technology and infrastructure has become a persistent race between the cyber attackers or black hats and the ethical hackers or defenders. With the rise of cyber-attacks on Cloud systems, service providers, web hosting and Internet data carriers are required to ensure the highest consideration to the novel challenges posed by cyber-attacks like Distributed Denial of Service and Malwares. With new attack vectors and novel threats are on the rise, corporates enterprises are required to protect IT infrastructure from the advanced attack methods being employed. Cyber-attacks today take on a variety of patterns and sizes. Because of increased botnet accessibility, large attacks are more common, as even

20 Gbps events have been reported. In addition to an increase in frequency, attacks have also become more sophisticated and stealthy. Critical resources like network links, session capacity, application service capacity or back end database response are affected. For example, Layer 7 application attacks are much more targeted and often consist of what appears to be legitimate traffic, making them more difficult to detect. In recent times, Malware and Distributed Denial of Service attacks have developed to be the main security threats as described by Choi, et al. (2010).

1.3.1 DENIAL OF SERVICE ATTACKS

DDoS attacks are executed to disable networked circuits, server systems by limiting access to them and termed as DoS attacks. These deny users the access to applications like Email, Chat, Ecommerce or Banking, or hosted Cloud services like SaaS, PaaS or IaaS Cloud services and computing resources like Network or VoIP infrastructure. The attacks are performed from a single source address as described by Deshmukh, et al. (2015) and illustrated in Figure 1.3 below.

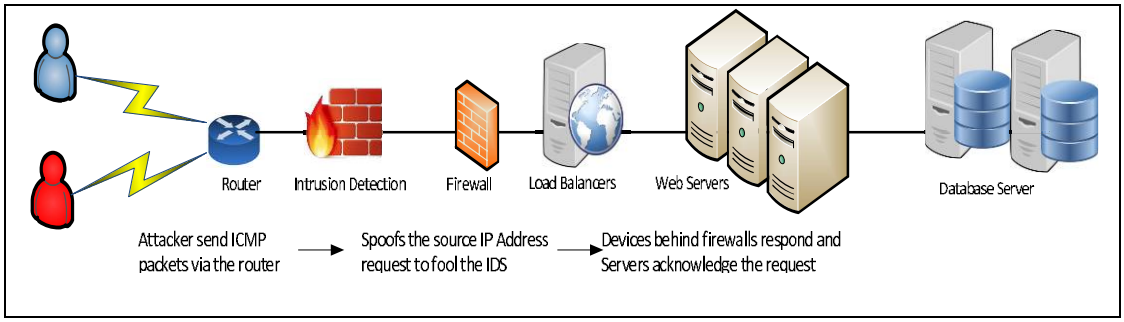


Figure 1.3: Denial of Service attack process

1.3.2 DISTRIBUTED DENIAL OF SERVICE ATTACKS

DDoS based attacks started with cyber-attacks on Gaming and Gambling web sites, the new cyber-attacks are now used for political reasons, financial gains and even as diversionary tactics to steal intellectual property and data. These cyber-attacks then amplify the Denial of Service attack by launching a flood assault from several thousand nodes by bombarding the target with malformed information requests and data packets in order to overwhelm the infrastructure and disrupt normal operations. These attacks are termed as DDoS attack, as described by Mishra, et al. (2011) and Anwar, et al. (2014).

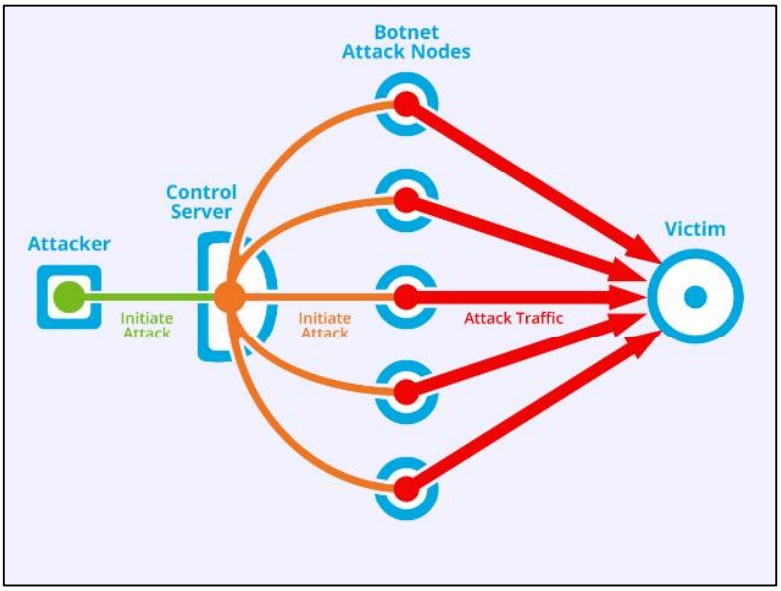


Figure 1.4: DDoS attack using Botnet nodes

Figure 1.4 above illustrates the use of Botnets sending amplified requests and turning the DoS attack into a DDoS flood attack. The attacker exploits vulnerable systems across geographies by compromising them with a malicious payload. This payload infects the end user systems with a malware application which enables the attacker to gain remote access with command and control capabilities. This is performed without the knowledge of the users with the intent to have the target services, hosted web applications unavailable to the authorized users as well as unavailability and security issues for Cloud computing services. This is presented by Zargar, et al. (2013) and Wong, et al. (2014) with DDoS attacks being performed by sending a flood of network packets, data or transaction requests over the Internet. These are sent from multiple locations and multiple systems at the same time. The infected and compromised user systems or nodes are referred to as Zombies or Bots which further compromise other user systems. The flood of compromised systems working as a group is known as Botnets and also controlled by a single attacker performing the attack sequence as shown in Figure 1.5. DDoS attacks present a high priority risk for Cloud service providers and Cloud service consumers with regards to the hosted infrastructure for managing the Service Level Agreements, Cloud service delivery, Cloud availability and avoiding any collateral damages.

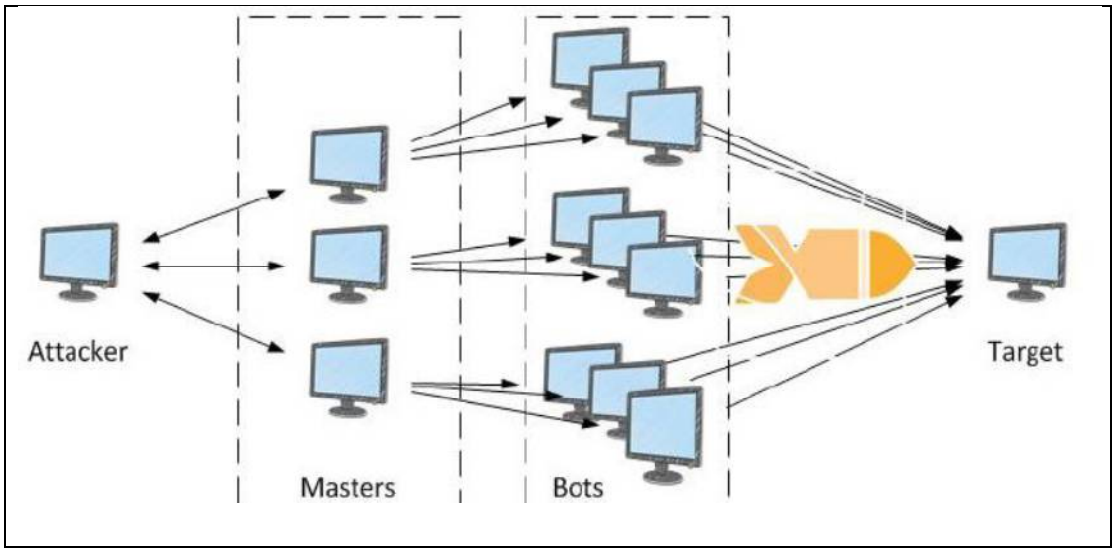


Figure 1.5: Distributed Denial of Service attack process

Besides having the cloud infrastructure and services being unreachable to actual consumers resulting in rental losses, increased delivery cost and harm to reputation, which further lead to legal and financial consequences, DDoS attack directly impacts the cloud providers and cloud service consumer in the below mentioned ways.

- Resource exhaustion like over whelming and consuming the bandwidth capacities of Internet pipes or making the Server CPU and memory to exceed the capacity
- Triggering Fallbacks to have the Intrusion Detection systems or Web Application Firewalls alter from their filer-mode to log-only-mode.
- Exploitation of end user accounts with lockouts by repeatedly attempting logon access with invalid credentials
- Cloud Portal access disruption by crashing the web application process by attacking vulnerabilities in the application code or altering user types to an invalid type and making it incorrect to input data for the legitimate user
- Camouflage the real attack motive by diverting the Security team attention acting as a smoke screen to steal data or hijack other services
- Pushing malware which affects the user access and data by opening up sockets and triggering errors in the micro codes

1.3.3 TYPES OF DDoS ATTACKS

DDoS attacks are broadly categorized into three main types of attacks depending on the area of Cloud infrastructure on which the cyber-attack is focused. These attacks are described in the below section as –

- Network or Volumetric DDoS attack
- Application layer DDoS attack
- Reflector DDoS attack

- **VOLUMETRIC DDoS ATTACKS** are network bandwidth attacks attempting to overwhelm the target by saturating the network bandwidth capacity (Giga bites per second). These originate from a botnet at most times over the Internet. Internet consists of a vast number of individual networks, interconnected to each other with the large, well connected networks providing access to smaller networks. The connections between these networks have a finite amount of bandwidth capacity. This capacity is often fixed due to technical or contractual limitations. Regardless of the limitation, most links cannot be trivially upgraded to a higher capacity without incurring substantial cost in terms of both time and money. Volumetric DDoS attacks are possible due to the relatively small network capacity of a target compared to the overall capacity of all Internet connected devices. These attacks are performed on layer 3 and 4 protocol layers by flooding and consuming the network bandwidth to the point where access to the hosted resources is rendered inaccessible. TCP/UDP/ICMP floods and spoofed packet attacks are typical examples of such attacks and these are referenced as mentioned below from the Incapsula DDoS Attack glossary (2017).

    - TCP Flooding starts by spoofing IP Address in SYN packet header of the data packet sent to the attacked server. TCP handshake process is exploited by the attacker sends half open connections seeking response from the server, whose SYN-ACK never reach the destination. Servers keeps the unestablished connections in queue for a period of time before discarding the packets (Linux OS leaves such connections open for 3 minutes each).

- UDP Flooding is initiated by excessively high volume of UDP datagrams IP network packets with MTUs ~1500 bytes being sent to random ports of the targeted servers or devices. The connectionless and non-mandatory packet transfer reliability feature of UDP packets makes these fake packets unable to be reassembled. This causes the server resources to be consumed quickly which results in the target device being unavailable ultimately.

- ICMP Flooding is performed by redirecting ICMP echo requests to overload the target with requests which results in the server spending all its resources to respond to those requests and consumes the network bandwidth ultimately.

- **APPLICATION LAYER DDoS ATTACKS** exploit application and server vulnerabilities by generating low-slow rate traffic, which looks legitimate and mimics human user behavior. These attacks overload the server and application resources and disrupt transmission of data between systems and hosts for the web application. These attacks are executed by introducing typical race conditions by requesting multiple computationally intensive GET/POST HTTP Flood requests and monopolize transactions. This impacts the web portal performance, client reputation and Quality of Service. XML and HTTP Floods are some types of application layer attacks.

  - HTTP Flood targets web application servers and the web architecture flaws and vulnerabilities using Slowloris and RUDY to send malformed HTTP packets in slow bandwidth traffic flow, sending partial requests, attempting to exceed the maximum concurrent connection pool that causes the web server to deny any more connection attempts from legitimate users or sending specialized HTTP GET or POST requests that exhaust the target server connection table.

  - XML Flood employs the X-DoS markup language which is used for Cloud communications with user and providers starts with SOAP messages. These are written in XML and these user validation requests get exploited by simple XML tag changes. This allows unauthorized entry to the Cloud services.

- **REFLECTION or PROTOCOL DDoS ATTACKS** involves sending large number of requests similar to volumetric attacks which get amplified by redirecting from more such bots hosts using spoofed IP Address as shown by Arukonda, et al.

(2015). This leads to flooding of requests on the target, exhausting the connection state tables of the servers and the intermediate equipment by consuming the resources. In this attack the request sent to a server, has the response larger than that of the request. State Exhaustion, SYN Floods, DNS Protocol Flood, Smurf attacks and Fragmented packet attacks are typical Reflector DDoS attack examples and this is measured in Millions of packets per seconds.

- State Exhaustion DDoS has the attacker targeting the firewalls, routers or server hosts to overwhelm and exhaust the maximum finite simultaneous connections which the server or network devices can support. These attacks target vulnerabilities in servers, operating systems and holes in the network infrastructure to significantly impact the availability of some or all of the infrastructure devices and impact multiple tenants.

- Protocol DDoS Attacks: Targeting protocols like DNS or NTP is becoming a concern for Cloud providers. DNS Amplification can be done by targeting a misconfigured DNS server and sending a 64byte while UDP dig request from a spoofed IP. The command returns 3-4Kbyte (50 times the request). NTP Amplification attacks also have UDP as the attack vector.

1.3.4 DDoS ATTACK TOOLS

This research work required use of software tools in order to perform DDoS attacks. These tools are reconfigured for the attack purpose and are described in this section.

- Low Orbit Ion Canon or LOIC launches floods of garbage requests of TCP, UDP and HTTP packets to overwhelm the target web server and disrupt its services by a single attacker. Figure 1.6 illustrates the LOIC attack targeting web server ports by increasing the inbound user requests in low packet rate attacks as shown by Bhuyan, et al. (2015).

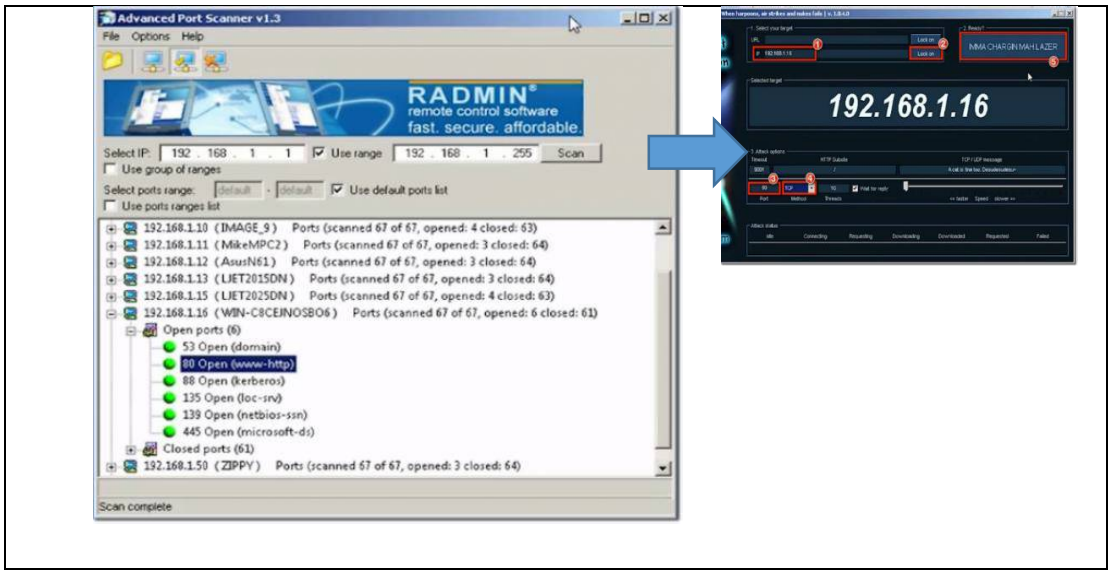
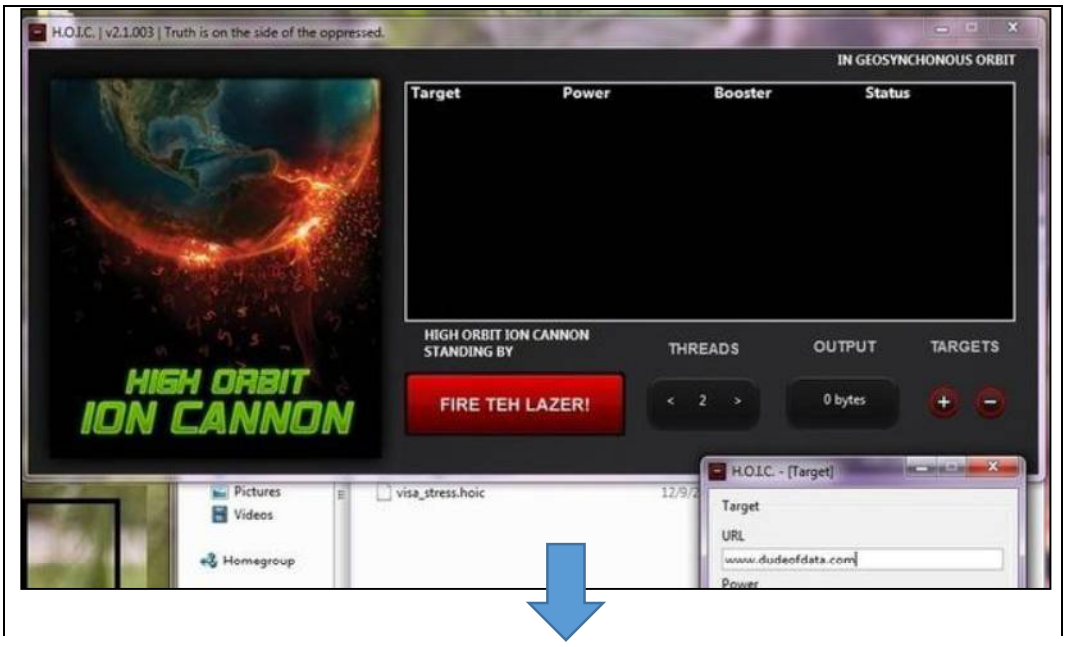


Figure 1.6: LOIC attack process

- XOIC is designed to perform network DDoS attack on specific IPs, multiple URLs, user selected port or user selected protocol. This software has the ability to cause HTTP flood with low number of bots and supports 'booster files' to increase the magnitude of the attack, configurable VBScript modules to randomize HTTP headers of attacking systems as shown in Figure 1.7 below.



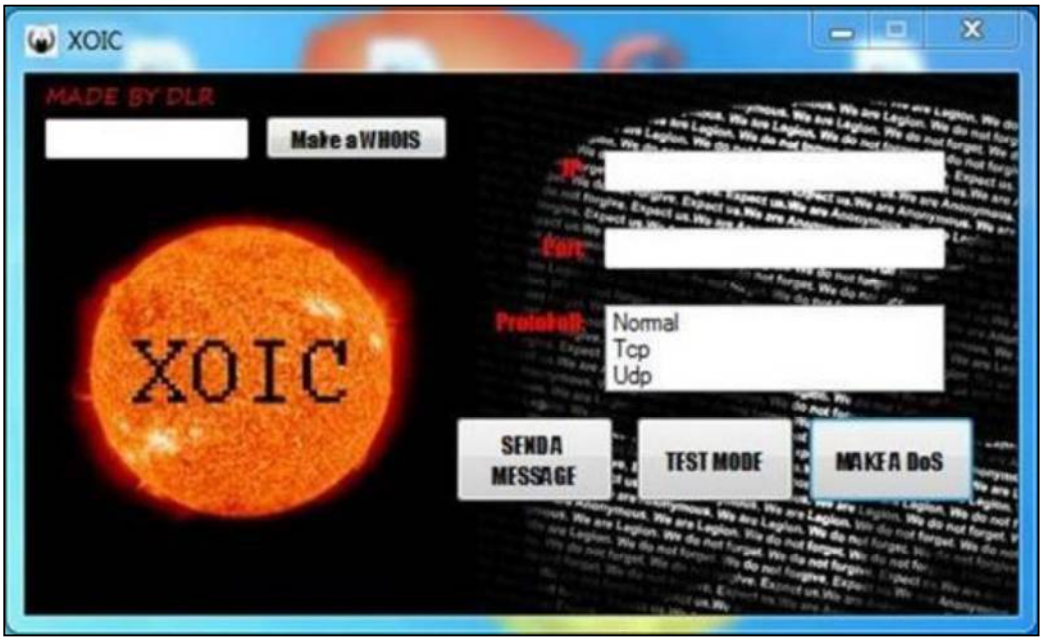


Figure 1.7: XOIC attack process

- DDoSIM creates bots and zombies operating on Layer 7 with spoofed IP Addresses as shown in Figure 1.8 below with data packets having in-built TCP, UDP and HTTP, ICMP messages creating full TCP connection (SYN-SYN or ACK-ACK).

Figure 1.8: DDoSIM attack process

- Slowloris simulates an application layer attack by using slow read, HTTP POST and Apache range header attacks, these end up consuming significant memory and CPU of the application servers. This tool runs on Lunix as shown in the Figure 1.9 below.

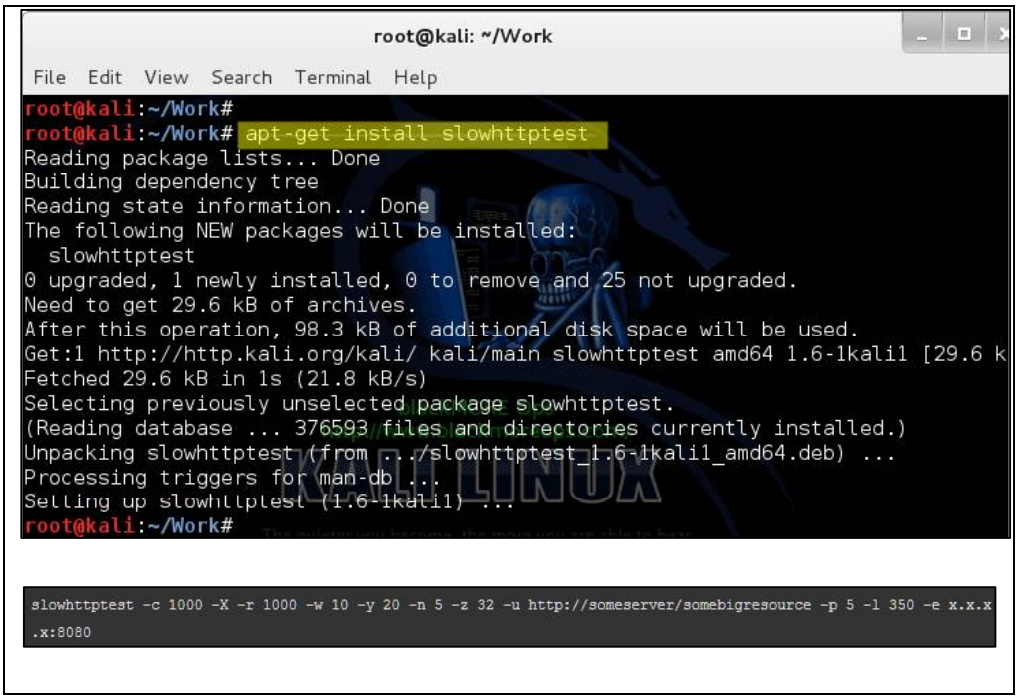


Figure 1.9: Slowloris attack process

- Pyloris tool has ability to actually own HTTP request headers during an attack, keeping the connection open as long as required for exhausting the resources of the target server. Figure 1.10 below describes the attack parameters for of threads, requests and time between threads.

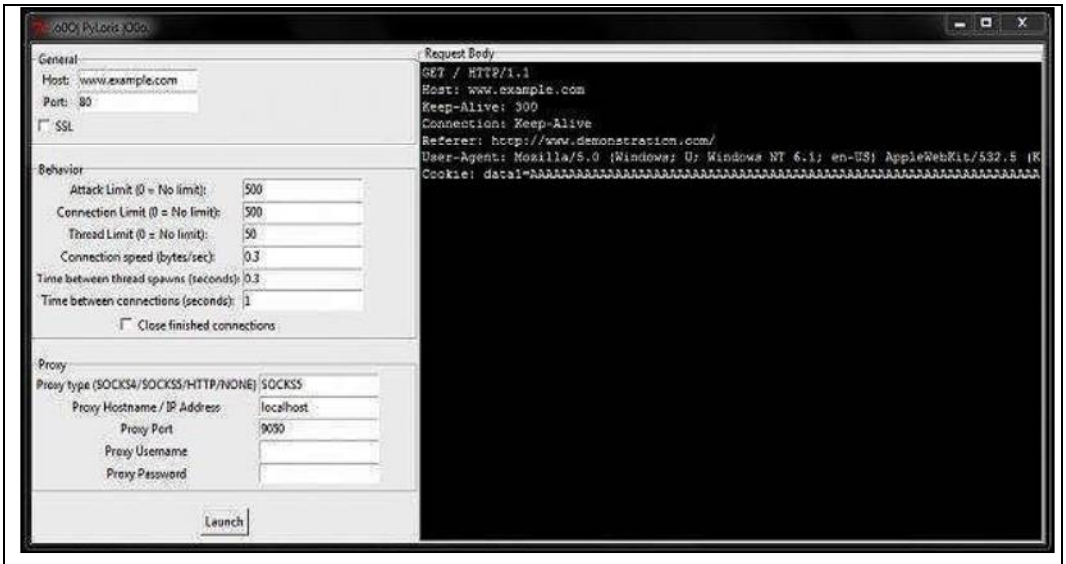


Figure 1.10: Pyloris attack process

- RUDeadYet or RUDY is a HTTP POST attack software which performs long field submission attack using POST method allowing the attacker to select forms and

fields to use for the POST attack for connections to open with timeout and content length as shown in Figure 1.11 below for a Slow POST attack on a web site.

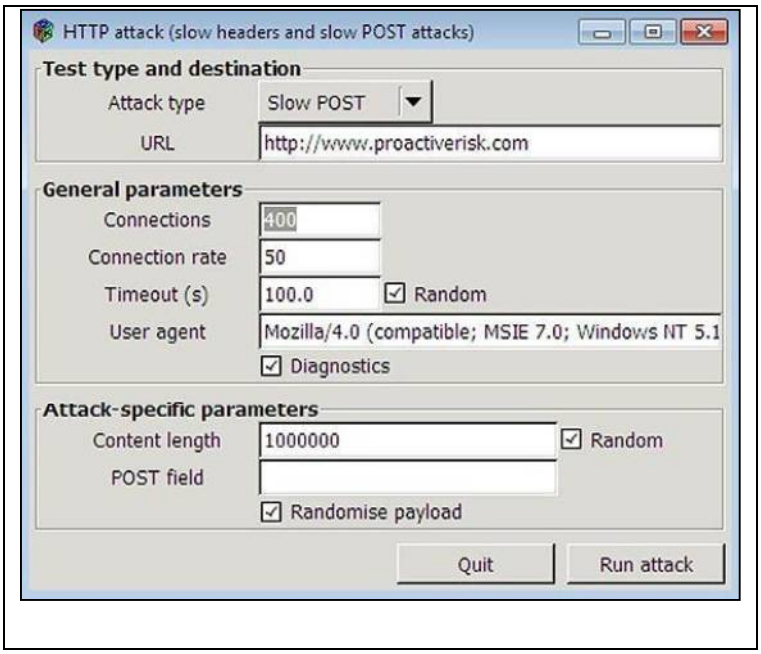


Figure 1.11: RUDY attack process

- Hulk or HTTP Unbreakable Load King generates unique requests to the target web servers. This attack software perform referrer forgery to bypass cache engines hitting the web server resource pool and avoids detection from IDS via known patterns as shown in Figure 1.12 below for requests sent and responses received.

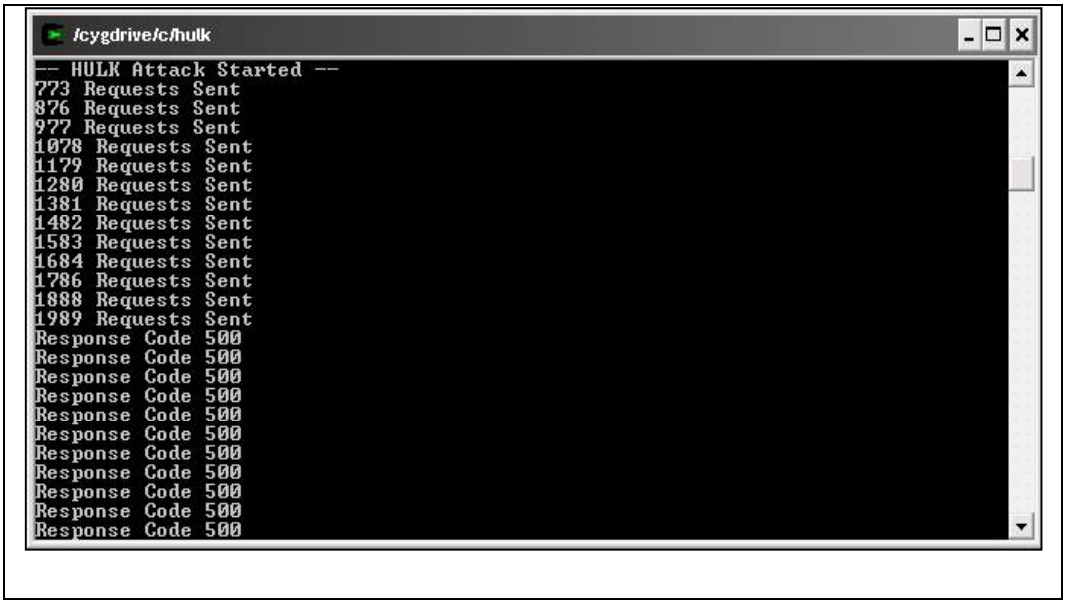


Figure 1.12: HDoS attack process

1.4 INTRODUCTION TO RANSOMWARE

Imagine what would happen if you were stopped from accessing your own files or accessing your own computer system. Now imagine further if to get back the access someone demanded ransom amount from you. Use of personal computing systems, hand held devices and mobiles have provided cyber-criminals an easy window of opportunity to preform malicious activities which impact the end users resulting in digital extortion on a scale never seen before.

Apart from DDoS, Ransomware is the top security threat in the information technology world. Ransomware is defined as a digital extortion conducted by using a malware having malicious code that infects the end user systems using different impact infection vectors. These range from browser exploits, freeware apps, email attachments or advertisements offering cash and incentives to lure innocent victims, as presented by Moore (2016) and Nolen, et al. (2016). Ransomware malwares are known to have high capability inbuilt into them to be able to run on 64-bit code from a 32-bit dropper or be able to switch execution context of the computing processor from 64-bit to 32-bit and visa-versa on 64-bit Windows or Linux environment. Ransomware propagation methods followed by cyber-criminals is presented below.

- **Botnets and Social Engineering** methods are employed by having first entering into user systems by way of free applications like software games or tools and then download the malware payload code inbuilt into these application installers.

- **Traffic Redirection** is performed by redirecting the user to the attacker's server or by luring the end user with malicious advertisements offering free upgrades or downloadable games. These sites actually host malware and exploits in the applications that are unknowingly downloaded by the users with the malicious payload installing itself in the user's systems and exploiting vulnerabilities in the user operating system and files.

- **Ransomware as a Service** is being offered by cyber criminals to perform malware attacks on payment for profits and running the ransomware attacks in form of a corporate mafia business from the Cloud as a service.

- **Email attachment** traps users into opening attachments or clicking on links with malware from friends or legitimate authorities ranging from bills for electricity, insurance, tax, legal notifications to job offers as displayed in the Figure 1.13 below.

Figure 1.13: Spam Email containing payload

Malware propagation methodology by criminals is illustrated in Figure 1.14 and presented in this section. Firstly by having users download a malware payload, the attacker injects a malicious code into the end user computer or mobile. The payload is installed in a random location as an executable application hidden from the device owner. This malicious code when executed takes over the end user device preventing access in various forms like blocking, encrypting of the computer system and data which would have been available in a normal environment. This is capable of stopping critical applications, disabling the physical input devices, hampering their working or simply encrypting data and files.

Figure 1.14: Malware propagation methodology

With the aim of preventing the victim from performing normal operations and access to data, the demand is for 'ransom' in this attack. The common ransomware variants are Crypto Ransomware which encrypts user data and files and Locker Ransomware which performs a lock down of the user systems, applications and even the input devices. These variants are presented in this section below.

- **Crypto Ransomware** is a data and file locker malware which once injected in user systems, executes silently searching for user data and files as described by Orman (2016). The infected system continues to work as usual, since the critical operating system files and applications are not modified and system functionality is not impacted, so no suspicion is raised. Data lockers are designed to search for end user files and data with extensions as FLV, PDF, RTF, MP3, MP4, PPT, CPP, ASM, CHM, TXT, DOC, XLS, JPG, CGI, KEY, MDB and PGP.

Figure 1.15: Crypto Ransomware Data Encryption

The malware silently encrypts the end user data and files making them useless for the owner and then demands a ransom for the decryption key as shown by Liao, et al (2016) and illustrated in Figure 1.15 above.

Locker Ransomware impacts computing devices like the user systems, mobile devices or the input interface devices, keyboard and mouse by controlling their access and locking the systems and devices. This control method is executed in order to deny access to the system owner as shown by Khouzani, et al. (2011). The malware flashes a Ransom page on the monitor screen as shown in Figure 1.16

below, allowing limited functionality access to user functions like moving the mouse or keeping only the numeric keyboard keys enabled for the user victim to input the amount and pay the ransom before restoring normal access. This malware can however be removed by restoring the system to its original state and such malware threats can be resolved relatively easily as compared to data locker malware.

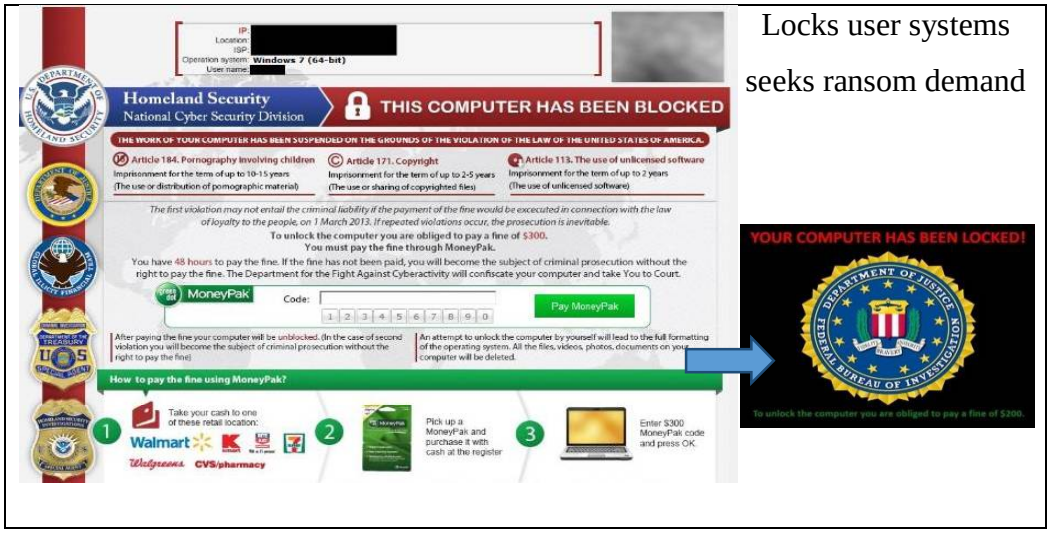


Figure 1.16: Locker Ransomware System Lockout

In a nutshell, Ransomware involves use of various scare tactics say getting the end user to either pay amount as ransom in form of Bitcoins or the end user is forced to buy items before releasing the user system and data. In order to protect data and have secure session connections, the Researcher also reviewed Cryptographic Algorithms for application systems and network devices inside Cloud computing environments. A brief of Symmetric and Asymmetric algorithms is presented in the section below.

1.5 ALGORITHMS FOR CLOUD SECURITY

Imagine two people who share critical secret information have to split up. This requires them to share and communicate their data and information from a distance, even as there lays a threat of eavesdropper having the ability to stop, interfere or intercept their communications and seeks that same information. They decide to lock their information in a box using a lock that only the other knows the combination to and has the key to open it. The box is locked and sent over to the other user who uses the combination key to unlock the box and read its contents. In simple terms, Cryptography can be seen as a method of storing and disguising confidential data in a cryptic form as described by

Devi, et al. (2012) so that only those for whom it is intended can read it and are able to communicate information in the presence of an adversary and the security algorithms mitigate security issues by use of cryptography, authentication and distributing keys securely. Cryptography is thus the science of making data and messages secure by converting the end user data to be sent into cryptic non-readable form and encrypting or scrambling the plaintext by taking user data or that referred to as clear text and converting it into cipher text as shown by Simranjeet Kaur (2012) and then performing decryption which is reverting back to the original plain text. With this ability, Cryptography is used for providing the following security:

- Data Integrity: information has value only if it is correct, this refers to maintaining and assuring the accuracy and consistency of data, its implementation for computer systems that store use data, processes, or retrieve that data.
- Authentication for determining whether someone or something is, in fact, who or what it is declared to be.
- Non Repudiation: is the assurance that a party, contract or someone cannot deny the authenticity of their signature and sending a message that they originated.
- Confidentiality: relates to loss of privacy, unauthorized access to information and identity theft.

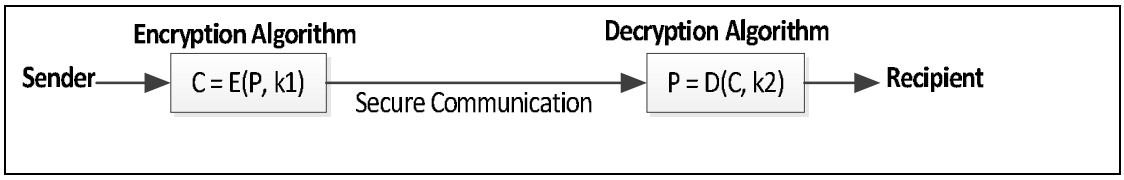


Figure 1.17: Encryption and Decryption process

In pure science terms, Cryptography as described by Kurtz, et al. (2010) is shown in Figure 1.17 above is the science of using mathematics for making plain text information (P) into an unreadable cipher text (C) format called encryption and reconverting that cipher text back to plain text called as decryption with the set of Cryptographic Algorithms (E) using encryption keys (k1 and k2) and the decryption algorithm (D) that reverses and produces the original plain text back from the cipher text. This can be interpreted as **Cipher text C = E {P, Key} and Plain text C = D {C, Key}**

With respect to Cloud computing, the primary security concerns relate to end user data security, network traffic, file systems, and host machine security which Cryptography can resolve to some extent and thus helps organizations in their reluctant acceptance of Cloud Computing. There are various security issues that arise in the Cloud:

- Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end user control of where the resources are hosted.
- Ensuring Secure Interface: integrity of information during transfer, storage and retrieval needs to be ensured over the unsecure Internet.
- Have Separation of data: privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.
- Secure Stored Data: question mark on controlling the encryption and decryption by either the end user or the Cloud Service provider.
- User Access Control: for web based transactions (PCI DSS), web data logs need to be provided to compliance auditors and security managers.

Security Algorithms are classified broadly as:

- Private Key / Symmetric Algorithms: Use single secret key are used for encrypting large amount of data and are have fast processing speed. These algorithms use a single secret key that is known to the sender and receiver. RC6, 3DES, Blowfish, 3DES are some prime examples of this algorithms.
- Public Key / Asymmetric Algorithms: Use a key pair for cryptographic process, with public key for encryption and private for decryption. These algorithms have a high computational cost and thus slow speed if compared to the single key symmetric algorithms. RSA and Diffie Hellman are some types of public key algorithms.
- Signature Algorithms: Used to sign and authenticate use data are single key based. Examples include: RSA, DH

- Hash Algorithms: Compress data for signing to standard fixed size. Examples include: MD5, SHA

- Other ways of classifying algorithms based on processing features as displayed in Figure 1.18.

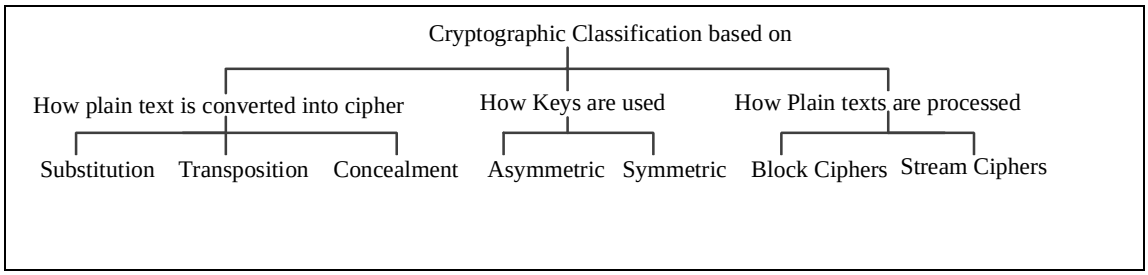


Figure 1.18: Classification of Algorithms

With several Cloud services, Servers and hosted applications under IT management, most Cloud providers have no defined process to ensure security of data from threats and attacks. Cyberattack these target the end user data for which the Cloud Service providers seek to try and secure by using Cryptographic algorithms whose primary goal is to make it as difficult as possible to ensure decrypting the generated cipher text from the plain text. When the key length is long, that makes it harder to decrypt the cipher texts, which in turn make the algorithms efficient and effective. For Cloud based web applications or portals needing real time or time sensitive data, an algorithm that might be taking a long time to long to run would prove a hindrance for the real time application as it may render the results to be useless. Such in efficient algorithm might end up needing lots of computing power or storage to execute over the Cloud, making the algorithm useless in that environment.

1.5.1 ASYMMETRIC ALGORITHMS

Asymmetric Algorithms as described by Khader, et al. (2015) involves a pair of related keys, one key for encryption called the Public key and a different but inter related key for Decryption called the Private keys when performing transformation of plain text into cipher text. The main asymmetric algorithms are ECC, Diffie-Hellman and RSA.

- RSA: is best suited for data traveling to/from Web and Cloud based environments. The end user data is first encrypted, transported and then stored on the Cloud application systems. When the data is required, the end user simply needs to place a request to the Cloud Service provider for accessing the data. For this the Cloud

service provider first authenticates the user to be the authentic owner and then delivers the data to the requester using RSA Asymmetric Algorithm.

- Diffie-Hellman Key Exchange (D-H): is a method for exchanging cryptographic keys by first establishing a shared secret key to use for the inter communication and not for encryption or decryption. This key exchange process ensures the two parties that have no prior knowledge of each other to jointly establish a shared secret key over unsecure Internet. Transformations of keys are interchanged and both end up with the same session key that looks like a secret key. Then each can calculate a third session key that cannot easily be derived by attackers who know both the exchanged values. This key encrypts the subsequent communications using a symmetric key cipher but is vulnerable to the Man-in-the Middle (MITM) attack. This key exchange is not used for exchanging real large data unlike RSA.

1.5.2 SYMMETRIC ALGORITHMS

Symmetric algorithms as described by Mewada, et al. (2016) involve a single shared secret key to encrypt as well as decrypt data and are capable of processing large amount of data and from computing standpoint are not very power intensive, so has lower overhead on the systems and have high speed for performing encryption and decryption. Symmetric algorithms encrypt plaintexts as Stream ciphers bit by bit at a time or as Block ciphers on fixed number of 64-bit units as mentioned in the Figure 1.19 below.

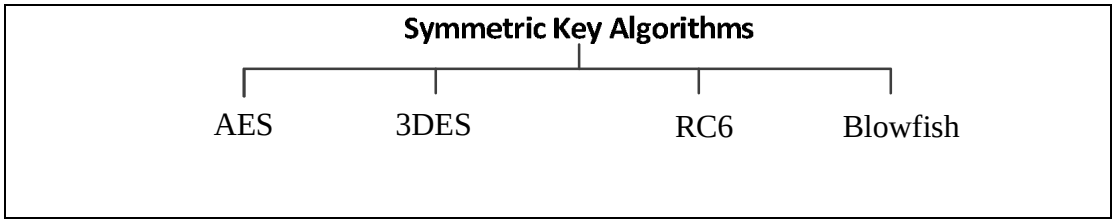


Figure 1.19: Symmetric Algorithms

There are however few problems with Symmetric Algorithms:

- Exchanging Shared Secret Key over unsecure Internet - Symmetric-key algorithms share secret keys required by the sender and receiver during encryption or decryption process. In case a third person gains access to the secure secret key, cipher text messages can easily be decrypted. The fact of having one single secret key algorithm is the most critical issue faced by Cloud service providers when dealing with end users who communicate over unsecure Internet. The only option

is to have that secret key be changed often or kept as secure as possible during the distribution phase.

- Problem if the content is altered or actually sent by the claimed sender - If a hacker has the secret key, decrypting the cipher text, modifying the information being sent with that key and send to the receiver. Since a single key is involved during the crypto process, either side of the transactions can get compromised. Such data integrity and non-repudiation issues however need to involve the use of Digital signatures or Hashing functions like MD5.

- Tools for cracking Symmetric encryption - By use of Brute force by running hacking tools that have the ability crack the combinations and keys to determine the plaintext message and perform Cryptanalysis where the attacks are focused on the characteristics of the algorithm to deduce a specific plaintext or the secret key. Then hackers are able to determine the plaintext for messages that would use this compromised setup.

1.6 RESEARCH OBJECTIVE

This research Thesis aims to understand the research subject in detail, seeking solution for cyber-attacks related to Malware and Distributed Denial of Service attacks and also reviews cryptographic algorithms for Cloud environments. The research proposes a Malware detection cloud based system, designed and implemented a secure architecture design to mitigate DDoS attacks on Hybrid Cloud Computing environments with sub objectives as:

i. Identifying the Security issues and Vulnerabilities in Cloud Environments.

ii. Explore existing DDoS Attacks and trends on Cloud Data Centers

iii. Design and implement Ransomware Malware mitigation system

iv. Study Algorithms with emphasis on Security for Cloud Computing.

v. Design Secure Architecture to mitigate DDoS attacks on Hybrid Clouds.

vi. Setup and validate the proposed secure architecture against DDoS attacks.

1.7 RESEARCH METHODOLOGY

This research is based on DDoS attacks on single and three tier architectures as well as on secondary DDoS Survey. The research methodology phases for the research Thesis is presented in Figure 1.20 below.

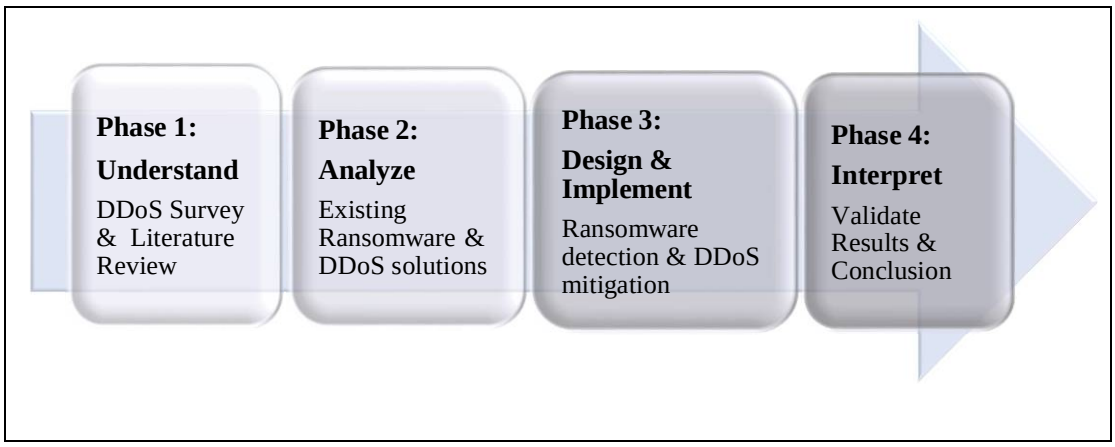


Figure 1.20: Research Methodology

Phase 1: Understand - DDoS Survey and Literature Research

- Perform DDoS Survey to understand Denial of Service and attack trends
- Review Literature research on Distributed Denial of Service, Cloud Computing and Security Algorithms to understand the security issues and vulnerabilities

Phase 2: Analyze – Study existing Ransomware issues and DDoS mitigation solutions

- Perform DDoS Survey, study existing mitigation solutions and current trends
- Analyze existing mitigation solutions for DDoS on Hybrid Clouds and Ransomware
- Review Security Algorithms for Cloud Computing environments

Phase 3: Design & Implement – Ransomware and DDoS mitigation solutions

- Design Ransomware detection and mitigation system
- Design Secure Architecture to mitigate DDoS attacks on Hybrid Clouds
- Perform DDoS Attacks on proposed architecture and single tier architecture

Phase 4: Interpret – Validate Results and Conclusion

- Compare results for the proposed Ransomware detection and mitigation system
- Compare metrics and parameters for single tier and three tier architecture designs
- Validate results and draw conclusions

1.8 RESEARCH CONTRIBUTION

This research work focuses on developing a secure infrastructure design to mitigate DDoS attacks on Hybrid Clouds, presents a Cloud based Ransomware mitigation system. By comparing the DDoS mitigation work in the literature, this proposed work is different as suggested below.

Firstly, the proposed network architecture design defends the DDoS attacks utilizing network and application defenses at physically different data centers mitigating specialized cyber-attacks and having asynchronous routing for outbound traffic.

Secondly, the proposed secure architecture mitigates network and application attacks in a phased multi-tiered manner, handling the inbound traffic with improved security and response.

Thirdly, the proposed architecture design is a combination of network level and application level defense mechanisms, both of which are working independently of each other, thus the proposed three tier architecture comes across as a resilient design for DDoS attacks.