NEW AGE CYBER THREAT MITIGATION FOR CLOUD COMPUTING NETWORKS

Akashdeep Bhardwaj

Bentham Books

New Age Cyber Threat Mitigation for Cloud Computing Networks

Authored by

Akashdeep Bhardwaj

University of Petroleum and Energy Studies,
Cybersecurity & Digital Forensics
India

New Age Cyber Threat Mitigation for Cloud Computing Networks

Author: Akashdeep Bhardwaj

ISBN (Online): 978-981-5136-11-1

ISBN (Print): 978-981-5136-12-8

ISBN (Paperback): 978-981-5136-13-5

First published in 2023.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
80 Robinson Road #02-00
Singapore 068898
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

FOREWORD

To the Reader of this book:

In submitting the wonderful manuscript titled 'New Age Cyber Threat Mitigation for Cloud Computing Networks' in book form, I believe that a few words about the book author of this remarkable personality will be of interest.

I have known Dr. Akashdeep Bhardwaj for the past two decades, first as the IT manager of my organization, then as the IT Head leading the Data center teams for another organization. We have been in constant touch throughout as I reach out to him often for some IT-related security work projects that I deliver. With his passion for mentoring cyber warriors and give back his experience to society, Dr. Akashdeep ventured into academics, leaving behind a high profile and paying career in the Cybersecurity domain. My best wishes to him, and hoping he shares his experience in the form of these wonderful books with society.

Mohit Rampal
CTO Ramognee Pvt. Ltd., Gurgaon, India

PREFACE

Cybersecurity attacks have presented the highest priority to securing Cloud infrastructure by using encryption for cloud traffic and against new-age attacks. The use of encryption algorithms for security consideration to use for Cloud and network-based services that require critical data and link encryption. This book suggests the use of a network security framework to bridge the gap between high-level specification requirements and the low-level implementation phase for network infrastructure security using the network architecture model with the security policies associated with the network components required to be enforced. Increasing use of email security protocols with encryption, PKI-based cryptographic techniques, IP address verification, and DNS-based domain validation are discussed to mitigate spoofing and other email threats. This book provides global Cloud and Network engineers with new options and recommends new methodologies and feasible solutions that can be implemented to secure the Cloud architecture and IT Infrastructure, thereby securing end users. This includes designing and implementing solutions against new-age attacks on the cloud infrastructure and network services.

Akashdeep Bhardwaj
University of Petroleum and Energy Studies, Dehradun,
India

CHAPTER 1

Ransomware: Rising Threat of New-Age Digital Extortion

Abstract: What if someone stopped you from accessing your files or using your computer? What if they demanded an amount to get access back to you? Most financial and social interactions revolve around three critical aspects – firstly, the use of digital data and files; secondly, computer systems; and last, the insecure internet. This is where Ransomware using Bitcoin has become a major cause of concern in the form of a new-age digital extortion threat to home and corporate users. This chapter discusses Ransomware and the methods adopted by cybercriminals for holding ransom innocent users' digital data and systems and proposes a malware detection system. Crypto and Locker ransomware is reviewed for their propagation, attack techniques, and new emerging threat vectors, such as file Encryption Ransomware, Screen Lock Ransomware, Windows & Browser Lock, Pop Advertisements, and URL Redirection. The author proposed a Cloud-based malware detection system, performing comparison evaluation with and without the proposed anti-malware solution in the form of sandboxes, so even if the environment got compromised, it could be easily decommissioned and rebuilt from a fresh, clean virtual snapshot. Malware Behavioral environments were set up for analyzing malware before and after receiving malware payload files and logs from infected user devices. Malware Code Analysis gathered assembly code and memory dumps from memory and performed analysis on malware payload instructions. Reporting environment analyzed Web URLs proactively for malicious sites hosting malware code or payloads and checked the user system and devices for before and after analysis logs.

Keywords: Bitcoin, Crypto, Extortion, Locker, Malware, Ransomware.

1. INTRODUCTION

The impact of Ransomware [1] has caused immense damage to end-users and corporates [2]. Access to authorized data being blocked and released only after the ransom demand has been made is a new age of digital extortion, which holds promise as a viable option against malicious attacks on user devices, including mobiles and handhelds. The recent explosion of the internet and personal computers have led to cybercriminals subjecting users to extortion on a massive scale never seen before. Ransomware is digital extortion by pushing a malware code to infect a user system from different infection vectors like browser exploit

Akashdeep Bhardwaj

kits, drive-by freeware apps, malicious email attachments, links offering free software, or advertisements offering free cash and incentives. The malware injects malicious code into the user system that installs randomly in the system location as an executable. This code then takes the user system hostage by preventing users from accessing their computer systems normally, stopping certain applications or input devices from running or encrypting user data files [3], and using scare tactics like asking the user to either do something like pay a ransom amount in the form of Bitcoin or fill in surveys [4] before releasing the system or data. The Ransomware malware has a high degree of capability inbuilt to run a 64 but code from its 32-bit TOR dropper; recent malware variants are known to switch the execution context of the processor from 32 to 64-bit on a WOW 64-bit environment [5].

Bitcoin is a network that allows a new form of monetary payment, medium of exchange and virtual Digital Cash. Individuals can purchase Bitcoins from online exchanges, direct sellers, or in-person with hard cash or credit cards. Bitcoin transactions are stored in a public ledger known as Blockchain, wherein money exchange is seen by the entire network almost immediately and recorded, making it difficult to identify the owners; however, the system is not anonymous [6]. These are not owned by any single company and are more like email exchanges where no one can block two entities from exchanging emails, details, or Bitcoins among themselves. Bitcoins are used for sending or receiving money with anyone, anywhere globally, at a very small transaction cost. The payments cannot be blocked or frozen. The rise in Bitcoin value has been phenomenal; about 25 Bitcoins are created every 10 minutes globally. In 2011, a single Bitcoin was under $1. Currently, 1 Bitcoin is worth 100s of US$. As Bitcoin's demand and popularity increase, Bitcoin might well be worth hundreds of thousands of dollars.

This chapter highlights the comparison of Signature-based antivirus scanning systems; the proposed malware detection and the alerting process have better mitigation results and advantages. The Anti-Malware scanning security [5], apart from being offered as a cloud service with the scanners operating from a secure cloud platform, showed far more resilience than other methods. Apart from having the advantages of being a cloud-based service that offers user-driven implementation, elasticity, and a pay-as-you-use model. This even helps save huge costs and promotes the concept of BYOD. The proposed Anti-Malware detection can be offered as a cloud service with specific customer blocking done so other users of the same application program benefit from the experience of other infected users. This system can be a pay-as-you-use model and dynamically elastic for capacity increase.

2. RANSOMWARE VARIANTS & PROPAGATION

Ransomware malware has been seen to have two major variants – the most common version is Crypto Ransomware which encrypts the files and data. In contrast, the other version is Locker Ransomware, which locks down the user system, applications, or input devices, preventing the target user from normal operations.

2.1. Crypto-Ransomware

This is a data locker. The malware, once injected into the user system, works in stealth mode to search for files and data. The attacked system continues to work normally as critical OS, and system files are not targeted, or the system's functionality is not tempered to raise any suspicion. Then, the malware encrypts the user files and data. This makes the files and data unusable to the user, forcing them to pay to obtain the decryption key. Crypto ransomware or Data locker, once injected into the user system, works in stealth mode to search for files and data with such extensions as FLV, RTF, PPT, CHM, TXT, DOC, CPP, ASM, XLS, JPG, MP3, MP4, CGI, KEY, MDB, PGP, PDF, and acts as a data locker. During this time, the system continues to work normally as critical OS and system files are not targeted, or the system's functionality is not tempered to raise any suspicion. Then the malware encrypts the user files and data. This makes the files and data unusable, forcing the users to pay to obtain the decryption key, as illustrated in Fig. (**1.1**).

Fig. (1.1). Crypto-Ransomware.

CHAPTER 2

Design A Resilient Network Infrastructure Security Policy Framework

Abstract: The information security policy development lifecycle tends to lack focus on the use of standard terms and semantics. This results in blurred outlines for monitoring, evaluation, and enforcement of the security policy for the employees confusing adhering to and implementing it, which leads to a lack of a process of publishing from the security policy, end-user awareness, translation of high-level policy to lowest level component configuration plans and actions to take in time of crisis. This leads to the critical need to design an empirically tested, comprehensive security policy. This chapter proposes bridging the gap between the high-level information security policy descriptions and low-level network infrastructure security implementation. With new and innovative technologies, such as Cloud, Remote Computing, Enterprise Mobility, and e-commerce on the rise, network security has remained an ever-increasing challenge. This chapter presents a security framework to bridge the gap between high-level specification requirements and the low-level implementation phase for network infrastructure security using the network architecture model with the security policies associated with the network components required to be enforced. An architectural model and a set of design-level security policies are considered to achieve the framework design. Also discussed are the advantages and desired characteristics of the model, relating to existing processes worked in the design area, and future research directions are pointed.

Keywords: Information Security Policy, Network Architecture, Network Firewall, Network Infrastructure, Security Policy, Web Application Firewall.

1. INTRODUCTION

With the ever-growing increase in the use of computer systems, applications on the cloud with the internet for data exchange and communication, the need for secure computing and a well-designed network security architecture is essential for all types of organizations ranging from corporates, academic or government entities or geographically spread end-users, different roles, and profiles as well as the use of different computing devices, communication channels [1]. This varied range introduces many new challenges to traditional approaches to designing network infrastructure architectures. This manuscript focuses on new and advan-

Akashdeep Bhardwaj

ced network infrastructure security systems defined as the setup of network devices, software, and integration technologies that help collaborate and implement the organization's network security. The current information security policy development lifecycle tends to have a few disadvantages, the most critical being the overall lack of view of the policy. Typically, a narrow view can be found when focusing only on the development of the security policy documents and not including the actual practices for implementation or even maintenance of the security policies. This process does not address how the security policy would be developed, enforced, or even evaluated. The lifecycle designs usually focus on policy for development instead of focusing on the development process of the information security policy.

They are utilizing a Hybrid cloud architecture design so that internet-facing tiers tend to be public clouds and internal secure applications and databases tend to be private clouds. This change in network architecture helps take on the volumetric network and application layer DDoS attacks to ensure the traffic reaching the internal network tiers is free from such attackers. Using Rate controls, built-in intelligent WAFs, and Client Reputation monitoring be used in combination as part of a comprehensive defense against all types and sizes of cyber threats. To understand the security landscape and grasp the areas affecting network security architecture, Fig. (**2.1**) provides a general representation of the various attack types and their mitigation approaches.

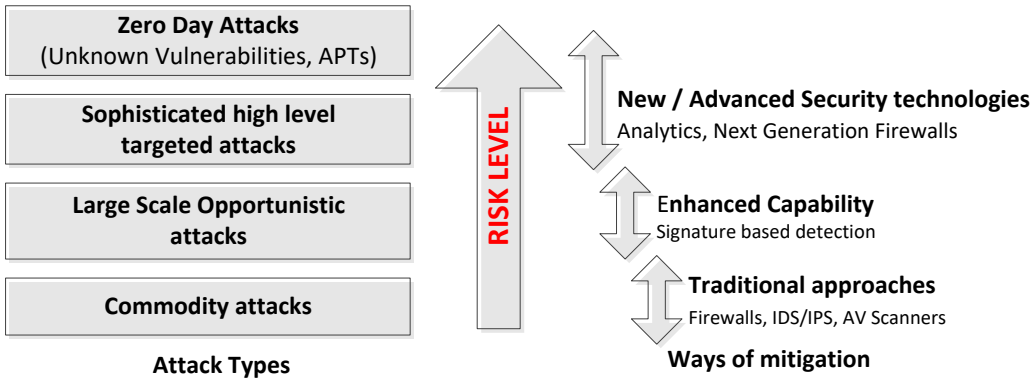

Fig. (2.1). Attack types and Mitigation Approaches.

As the security risk levels increase, the security needs of organizations become complex. Network Security system architecture with legacy traditional approaches like single-tier design and firewalls must undergo several design changes before acceptance [2]. Some of the changes essential to move from the traditional levels (like firewalls, IPsec, VPN) to enhanced levels include turning data centers into

auto-scaling clouds, virtualization-based software-defined networks, open stack network architecture, and multi-tenant-aware provisioning networks. Usually, the design of network security systems follows three standard phases, with the security policy (high level) being documented with some controls (like ISO, PCI) and guideline manual, followed by the formulation of security requirement specifications, and finally implementation phase (low level) that integrates and combines the security design. The problem with this approach is the gap between the high-level security specification requirements and the low-level implementation phase. The IT Security team receives the high-level description and goes directly to implement the security design, however complex and multiple network components and mechanisms involved. These network devices and components sometimes have completely different configuration setups [3] and features with little or no integration mechanisms.

This causes errors and improper enforcement of the actual security design, leaving security holes and vulnerabilities with a false sense of security. The Information Security Policy aims to provide a framework for information security management across the enterprise. This applies to everyone with access to the enterprise information systems (including employees, contractors, third-party consultants, and visitors) and devices and systems attached to the enterprise computer and telecom network. The policy addresses the processing of information by the enterprise for its operational business purpose, regardless of being on paper or in electronic form. The policy also covers services provided by external parties as consultants to the enterprise, as described in Fig. (**2.2**).

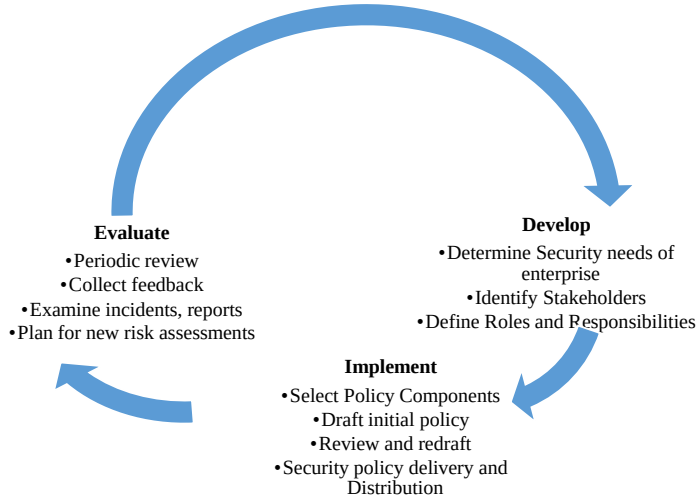

Fig. (2.2). Information Security Model.

CHAPTER 3

Security Algorithms For Cloud Computing

Abstract: With growing awareness and concerns regarding Cloud Computing and Information Security, there is growing awareness and usage of Security Algorithms in data systems and processes. This chapter presents a brief overview and comparison of Cryptographic algorithms, with an emphasis on Symmetric algorithms should be used for Cloud-based applications and services that require data and link encryption. In this chapter, we review Symmetric and Asymmetric algorithms with an emphasis on Symmetric Algorithms for security consideration on which one should be used for Cloud-based applications and services that require data and link encryption.

Keywords: Asymmetric, AES, Cryptography, 3DES, MD5, RSA, RC6, Security Algorithm, Symmetric.

1. INTRODUCTION

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 an 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 [1] can be seen as a method of storing and disguising confidential data in a cryptic form so that only those for whom it is intended can read it and can 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 what is referred to as clear text and converting it into Ciphertext [2] and then performing decryption which is reverting to the original plain text as presented in Fig. (**3.1**).

Akashdeep Bhardwaj

Fig. (3.1). Encryption and Decryption process.

With this ability, Cryptography is used to provide 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, and its implementation for computer systems that store user data, processes, or retrieve that data.
- Authentication for determining whether someone or something is 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.

In pure science terms [3], Cryptography is the science of using mathematics to make plain text information (P) into an unreadable Ciphertext (C) format called encryption and reconverting that Ciphertext back to a plain text called 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 Ciphertext. This can be interpreted as Ciphertext C = E {P, Key} and Plain text C = D {C, Key}.

Defining some terms used in Cryptography:

- The plaintext is the original intelligible source information or data that is input to algorithms
- The Ciphertext is the scrambled message output as a random stream of unintelligible data
- The encryption Algorithm substitutes and performs permutations on plain text to Ciphertext
- Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the Ciphertext to produce the original plain text
- Keys are used as input for encryption or decryption and determine the transformation
- Sender and Recipients are persons who are communication and share the plaintext

Concerning Cloud computing, the security concerns [4] are 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. Various security issues 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 insecure 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 a single secret key is used for encrypting a large amount of data and are have a fast processing speed. These algorithms use a single secret key that is known to the sender and receiver. RC6, 3DES, Blowfish, and 3DES are some prime examples of these algorithms.
- Public Key / Asymmetric Algorithms: Use a key pair for the cryptographic process, with the public key for encryption and the 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 and DH
- Hash Algorithms: Compress data for signing to a standard fixed size. Examples include: MD5, SHA
- Other ways of classifying Algorithms based on their processing features as illustrated in Fig. (**3.2**).

With several Cloud services, Servers, and hosted applications under IT management, most Cloud providers have no defined process to ensure the security of data from threats and attacks [5]. Cyber attacks this target the end-user data, 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 Ciphertext from the plain text. When the key length is

CHAPTER 4

Solutions for DDoS Attacks on Cloud Environment

Abstract: The internet has become the key driver for virtually every organization's growth, brand awareness, and operational efficiency. Unfortunately, cyber terrorists and organized criminals know this fact too. Using a Distributed Denial of Service attack, they can deny corporates and end-users internet access, make the website go slow, and deny access to corporate networks and data, making them unable to service legitimate users. It is not just these that are vulnerable; DDoS attacks are diversions. Due to the increased attack volume, collateral damage is becoming a major cause of concern – packet loss, delays, and high latency for internet traffic of those whose network traffic traverses the WAN saturated by a DDOS attack. DDOS attacks disrupt services and distract security resources, while other attacks, like fraudulent transactions, are attempted. Adaptive DDOS attacks are prevalent – attackers attack traffic on the fly to avoid identification and confuse mitigation plans. Reflective and Amplification attacks are most common – leveraging misconfigured DNS, NTP, and other network resources by spoofing source IP addresses. The bitter reality is that for cloud computing to be useful, it has to be exposed to insecure WANs and the public internet. With Cloud services presence being advertised and the interfaces defined, unauthorized attacks would always look to target the services.

Keywords: Cloud Computing, Cloud Security, CSP, Denial of Service, Scrubbing.

1. INTRODUCTION

Denial of Service attacks [1] is a cyberattack method to deny legitimate users access to online web applications (Email, Chat, Ecommerce, and Banking), SaaS, PaaS, or IaaS Cloud services and computing resources like network resources or even VoIP infrastructure with a single attack address as illustrated in Fig. (**4.1**).

Distributed Denial of Service attacks or DDoS attacks [2], as presented in Fig. (**4.2**), amplify the effects of a DoS attack by using thousands of machines to launch their assaults and disrupt operations at a large scale by bombarding the target web applications and network devices with information requests that overwhelm the server.

Akashdeep Bhardwaj

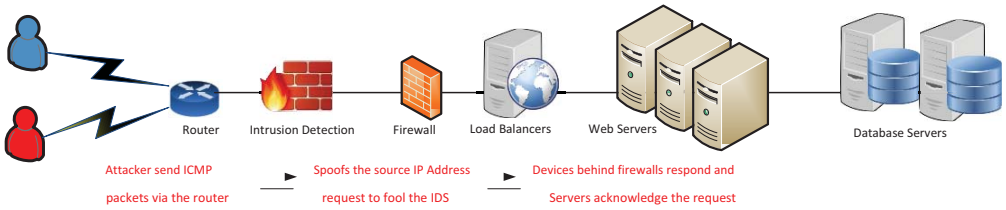

Fig. (4.1). Denial of Service Attacks.

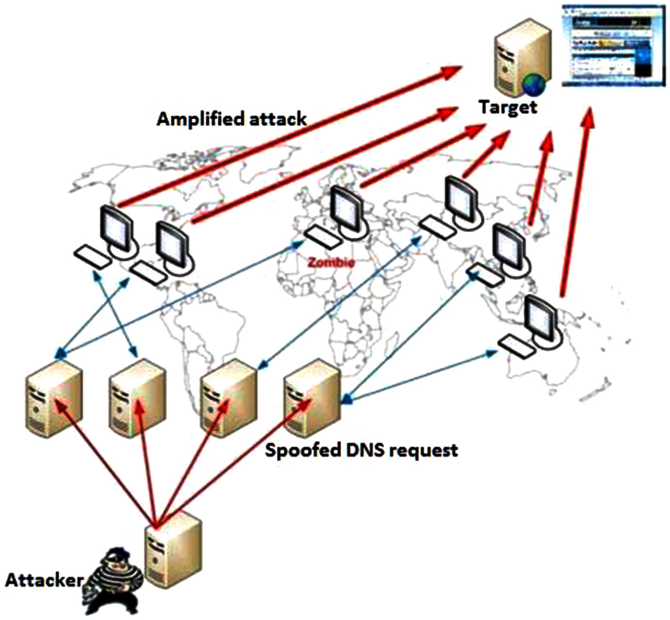

Fig. (4.2). Distributed Denial of Service Attacks.

Attackers exploit vulnerable systems across geographies, compromising them by infecting them with a Trojan virus. This is a small application that enables remote access to command-and-control capabilities of the user systems without their knowledge to attack the intended target servers in an attempt to make one or more services like Cloud services or hosted web applications unavailable to the intended users by sending a flood of network packets, data or transaction requests over the network from multiple systems at the same time. These are called Zombies or Bots [3]. These infected systems or Bots further compromise others, with the compromised systems working as a Botnets group. The problems faced by the users range from:

- Resource exhaustion, like over-utilizing and consuming the WAN pipes, or server CPU time

- Exploitation for user accounts lockout by repeatedly attempting with invalid credentials
- Process disruption by crashing a web application process by attacking a vulnerability in the code
- Pushing malware that affects processors opens sockets to trigger errors in computer micro-codes
- Corrupting data by altering user types to an invalid type, making it incorrect to input data

2. REPORTS AND TRENDS

As per F5 Denial of Service and Cloudflare trend reports, Figs (**4.3** to **4.9**) illustrate the dismal state of security on the Internet and cloud domains regarding various cyberattacks.

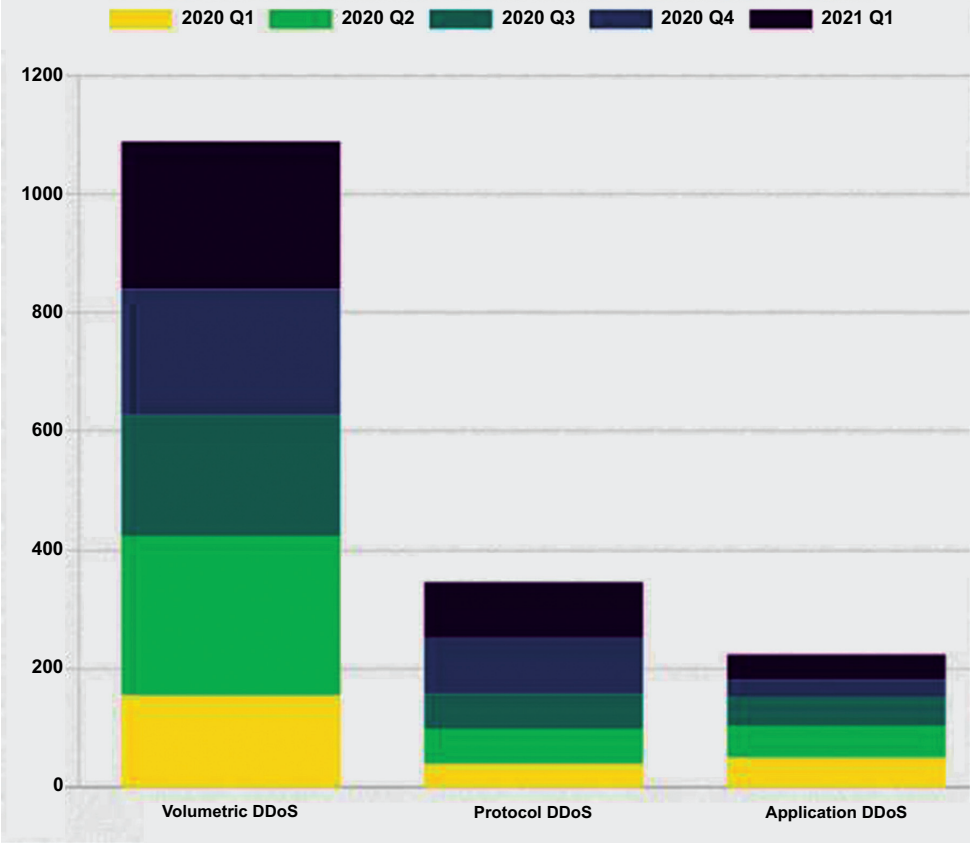

Fig. (4.3). Frequency of DDoS Attack Types.

CHAPTER 5

Three-tier Network Architecture to Mitigate DDoS Attacks on Hybrid Cloud Environments

Abstract: With the rise of cyber-attacks on cloud systems globally, Cloud Service Providers, Data carriers, and hosting providers are forced to consider the novel challenges posed and requirements for attacks and, more specifically, DDoS protection in large hosting environment setups. This chapter proposes using a multi-tiered network design based on a Hybrid cloud solution comprising an On-premise solution and a public cloud infrastructure capable of handling hurricane-sized DDoS storms.

Keywords: DDoS, Hybrid Cloud, Multi-tier, Network Firewall Three-tier, Web Application Firewall.

1. INTRODUCTION

While DDoS attacks began within gaming and gambling Websites, newer attacks are being used for political reasons, financial gain, and as a diversionary tactic to steal intellectual property. With new vector attacks and threats on the rise, corporates and enterprises must protect their IT infrastructure from advanced attack methods. Today's attacks take on a variety of patterns and sizes. Due to increased botnet accessibility, large attacks are more common, and 20Gbps events have been reported.

2. DDoS IMPACT ANALYSIS

To ascertain the DDoS impact and trend, the authors contacted 350 industry professionals, including Cloud experts (30%), CXOs (10%), IT Managers (30%), and engineers involved in DDoS mitigation (30%). They performed a survey collecting data and details on DDoS effects on organizations, with the survey meant for those respondents who were responsible and in charge of IT and DDoS Security within their roles. Below are the survey results from the data gathered and a list of questions that were asked:

Akashdeep Bhardwaj

- Does your organization have the ability to block and prevent DDoS attacks?
- Is your organization prepared to deal with and respond to DDoS attacks in your data centers?
- Did you face downtime due to DDoS attacks?
- Has a DDoS attack ever resulted in downtime for your Cloud-hosted services?
- Rate and prioritize areas as a result of a DDoS attack.
- What are the barriers that prevent DDoS mitigation implementation?

Figs. (**5.1** to **5.4**) illustrate the outcome of the responses received in the survey.

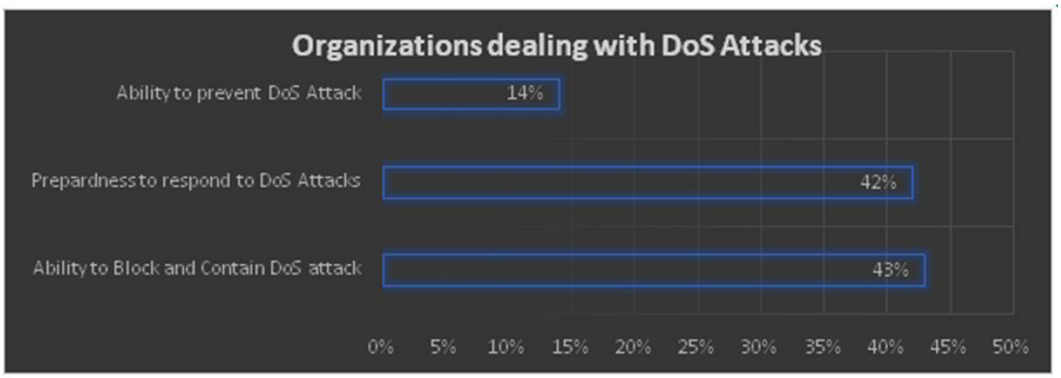

Fig. (5.1). Ability to block/prevent DDoS attacks.

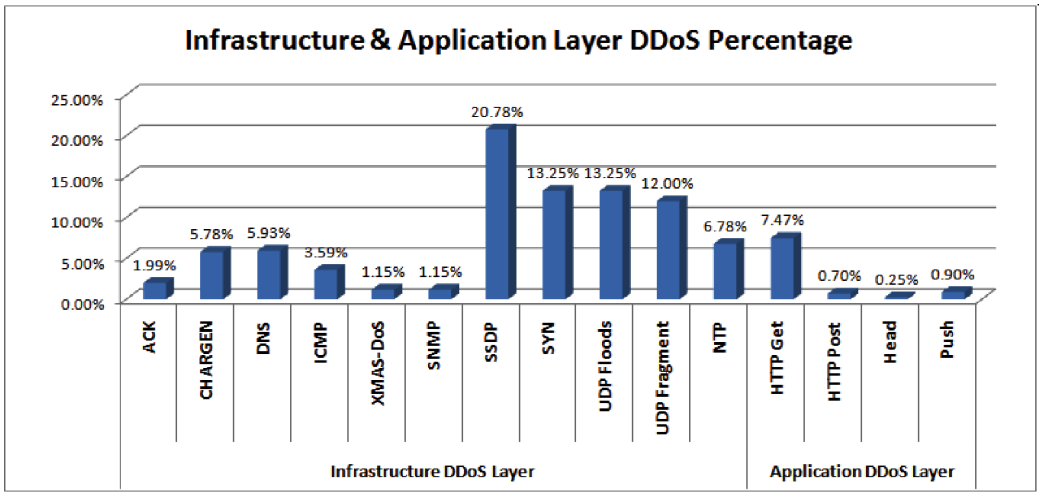

Fig. (5.2). Infra & Application Layer Attacks.

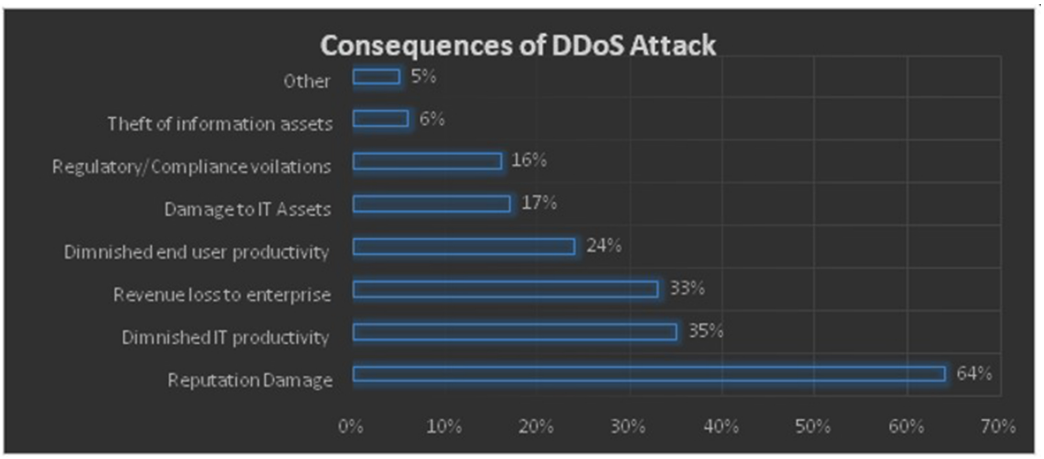

Fig. (5.3). DDoS Attack on organizations.

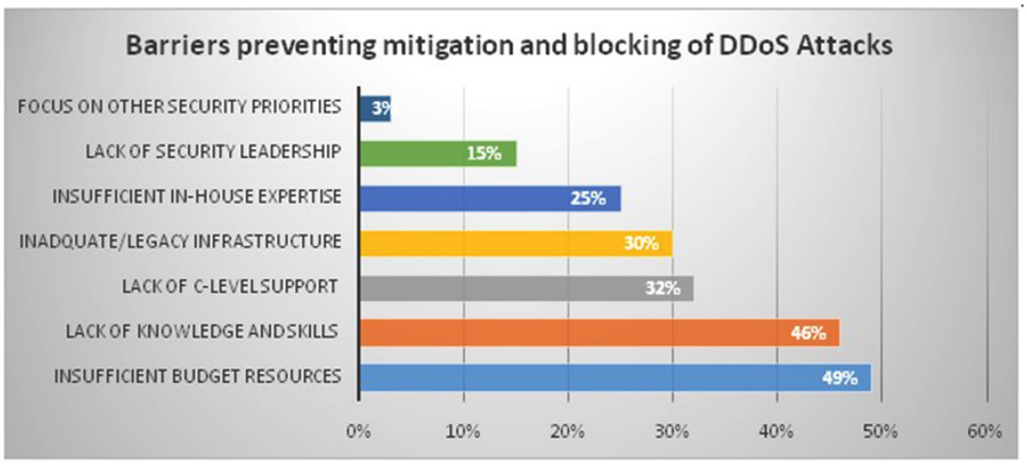

Fig. (5.4). Barriers Preventing DDoS Mitigation.

The survey results provided insights into the existing state of DDoS levels for organizations, with most admitting that the impact of DDoS attacks was on the rise with new attack vectors and volumetric attacks beyond their existing infrastructure. Unfortunately, most organizations we reviewed do not have a plan despite acknowledging the impact and still rely on operational infrastructure.

3. TRADITIONAL SECURITY *V/S* NEW-AGE DDoS ATTACKS

Traditional network security solutions such as Firewalls [1], Intrusion Prevention Systems (IPS) [2], and Web Application Firewalls (WAF) [3] are insufficient to

CHAPTER 6

Review of Solutions for Securing End-User Data Over Cloud Applications

Abstract: With more and more organizations working on the cloud over unsecured internet, sharing files and emails and saving them on cloud storage is imperative. Securing the end-user sensitive data in transit has thus started to get maximum priority to protect it from Cloud company staff, hackers, and data thieves. In this study, an attempt is made to review the research on end-user data security. There is an urgent need for solutions for end-users data protection privacy during the times when migrating from one cloud service provider to another. This chapter reviews the challenges in Cloud computing services regarding end-user data, analyzes the issues face, and presents solutions to overcome them. The chapter identifies end-users data security issues when using cloud computing services. The focus is directed to critical issues related to unauthorized access to integrity during data in transit. This can be addressed using Public Key Cryptography or PKI. For Confidentiality and Data Integrity for end-user data over Cloud. Then for migrating from one cloud service provider to another, data security and privacy are addressed by Cloud-aware applications. Lastly, using Multi-Factor Authentication combined with network and application detection systems, Intrusion Detection Systems, and Network traffic routing in case of cyber-attacks can help achieve denial of service attack mitigation or prevent man-in-the-middle and network snooping in Cloud Computing.

Keywords: Cloud Computing, Cloud Security, CSP, PKI, Public Key Cryptography, IDS, Firewall.

1. INTRODUCTION

The end-user data required to be protected by four types ranging from usage data which is the information collected from computer systems than is sensitive information on health and bank accounts, then is Personally identifiable information, information to identify an individual, and finally, Unique device identity information that is uniquely traceable like IP addresses, unique hardware identities (MAC address). A survey conducted by International Data Corporation (IDC) declares that 47% of IT Heads are highly concerned about security threats in cloud computing. In a recent survey conducted by Cisco, two-thirds of the respondents acknowledged that security and privacy are the top two security

Akashdeep Bhardwaj

issues for cloud consumers. As per a recent survey conducted by International Data Group (IDG), the top three challenges in implementing a cloud-based security strategy differs between IT and the line of business (LOB). They use solution paths such as digital keys, multi-factor authentication, and cloud-aware applications. Cloud-based services provide a flexible, scalable, pay-per-use, short-term contract model for IT Services, making Cloud-based services an efficient, affordable, and easy-to-implement option reducing capital expenditure involving IT hardware, licenses, office space, computing power, and bandwidth. Security of user data needs to be in place, especially in today's context with Cloud-based applications being hosted on the service provider premise and the end-user residing in a remote data center, well outside the user's control. When there is a need to provide End users with the right IT resources to enable them to perform their tasks, we usually do not emphasize the importance of securing the end-user data. End-user data for end-user functionalities [1] such as support, buying hardware, software, and licenses, then plan endlessly for installation, support, and maintenance, as well as worry about capacity planning, creating IDs, configuring profiles, or sitting on a budgeted pile of money waiting for hiring to be completed.

- Web-based services: Internet email services (Gmail, Yahoo, and Hotmail), Online stores (Amazon, Fab furnish, Jabong), and Web hosting (NetMagic, Tulip). These have been around for many years.
- Distributed computing: Splitting the processing workload among multiple systems usually connected at the same sites is done in Parallel and Grid computing technologies.
- Datacenters: Single application being hosted in one location (over a single or even multiple servers) does not qualify as a Cloud. Cloud computing leverages pooled hardware resources and automation services involving a great deal of virtualization hosted across data centers.

In these avenues, there are different types of security challenges [2] and versatile solutions for each cloud deployment model and overcoming them.

• Software as a Service (SaaS) is paid on demand where users access over the cloud, examples as On-Demand CRM Salesforce, Google Apps, Microsoft Office 365, and Microsoft Sky Drive.

• Platform as a Service (PaaS) provides end-users with a complete environment so that developers can deploy their apps, perform testing and hosting of web applications and databases, and provide virtual servers, OS, development framework, and coding apps. Examples are Google apps, Azure from Microsoft, and Rack Space.

• Infrastructure as a Service (IaaS) provides hardware and computing power to end-user to provision and harness resources from computing, network devices, storage, or servers where the customers pay only for the amount of infrastructure used and do not worry about buying hardware, maintaining or upgrading issues [3]. Infrastructure can be scaled dynamically based on application resources and market demands. Some examples are Amazon EC2, Rack Space, Attenda RTI, and Eucalyptus (Open source).

2. CHALLENGES IN CLOUD COMPUTING

2.1. End User Challenges in Cloud

End users typically face the following challenges in Cloud Computing:

- Limited support for customization: there are limits to the customization that can be done for Cloud applications and services to suit end-user-specific requirements.
- Constraints on features: cloud apps tend to be less feature-rich than their on-site or in-house counterparts because of in-built capabilities.
- Application latency: latency becomes a major factor for Cloud apps dependent on the transfer of large volumes [4] or time-sensitive data.
- Statelessness: performance issues arise for Cloud apps as the communication is unidirectional; single requests and responses from end users traveling to and from a service provider experience drop or disconnects travel over different paths/routes tend to arrive out of sequence.
- Legal restrictions sometimes force organizations to secure and control their data in a specific geographical location for the Cloud provider's data center.
- Security of end-user data is the most critical issue; depending on the Cloud provider's architecture and model, cloud vendors are primarily responsible for managing environmental and virtualization security, ensuring Security, Authentication, Integrity, and Privacy for data stored on their sites or in transit over unsecured internet links. Here data breaches, compromised credentials/broken authentication, hacked interfaces and APIs, system vulnerabilities due to Zero Day attacks, Account hijacking, Malicious insider threats, Advanced persistence threats, permanent data loss, inadequate compliance checks, DDoS attacks, and use of shared resources and storage are among the most critical security issues plaguing end users and their data.

Typical concerns raised by end-users to Cloud Service Providers or CSPs when adopting Cloud services are:

CHAPTER 7

DDoS Attacks, New DDoS Taxonomy, And Mitigation Solutions

Abstract: Cloud computing has started to gain acceptance for adoption and implementation among organizations, however, this new technology area has already started to deal with security, performance, and availability challenges. Within Cloud Security issues being paramount for corporates, and private enterprises, the denial of service attacks are rated as the highest priority threat to the cloud environments. This chapter presents a review of the academic literature research work on the DDoS attack on the Cloud, introduces a new DDoS Classification taxonomy, and proposes parameters for determining an effective DDoS solution.

Keywords: Cloud Computing, Cloud Security, DoS, DDoS, Distributed Denial of Service, ICMP Flood.

1. INTRODUCTION

To determine the DDoS attack, existing academic literature research work is surveyed by IEEE, ACM Science Direct, Elsevier, and ACM, searching for keywords, such as Cloud Security, DDoS Mitigation, Detecting DDoS, Hybrid Cloud, Network Architecture, Packet Flooding, SYN Flood, TCP Flood, and UDP Flood. The chapter is classified in terms of Infrastructure level Direct Network layer attacks, as illustrated in Fig. (**7.1**) for Infrastructure-layer and Application-layer attacks. A new Taxonomy for classifying DDoS Attacks is also proposed in the chapter by Degree of Attack Automation, Exploitation of Vulnerabilities, Attack Rate Dynamics, and Impact of DDoS Attacks. This section reviews related research work that has already been carried out in the same domain area.

The author surveyed several research publications from IEEE, ACM, Science Direct, and other digital libraries using keywords as mentioned below and in Fig. (**1**) for DDoS attacks like Cloud Security, DDoS Mitigation, Detecting DDoS, Hybrid Cloud, Network Architecture, Packet Flooding, SYN Flood, TCP Flood, and UDP Flood. With the advances in technology, and new powerful attack tools available for launching DDoS attacks, the attack trends and threats security offered are not static. This trend forces cloud service providers to maintain state-

Akashdeep Bhardwaj

of-art defenses to stay ahead of the most recent attack. The main focus of a network security attack is to be able to infiltrate, crash data center devices or alter configuration information, adversely impacting the uptime, availability, reputation, productivity, quality of service, and revenue of the service providers.

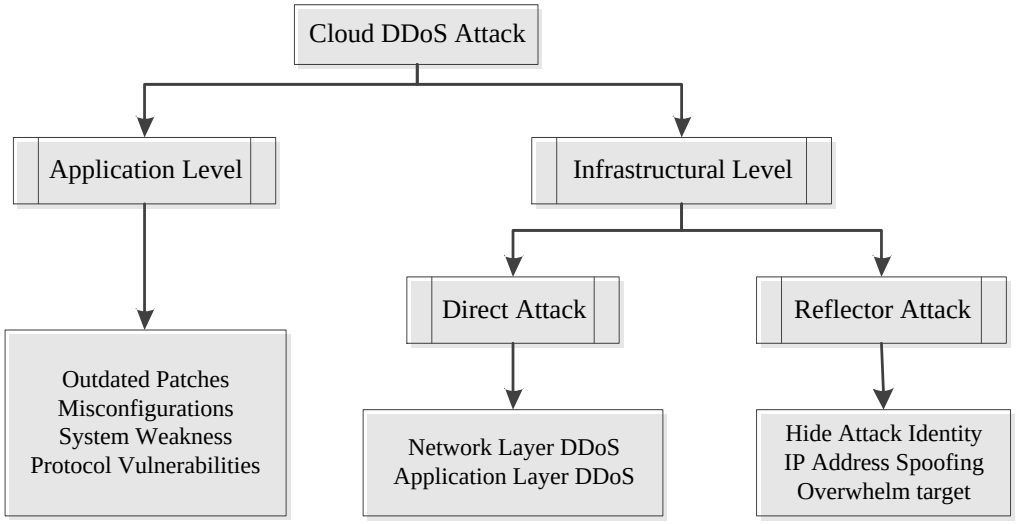

Fig. (7.1). DDoS Attacks in the cloud.

2. RELATED WORK

While several research surveys have been published on the DDoS topic, this survey is different from them in the following manner:

- Wong and Tan (2014) [1] focused on DDoS attacks on Cloud infrastructure and application systems, while DDoS attacks and DDoS Mitigation are the focus of this survey. Several other surveys and conference papers are of limited scope in Darwish *et al.* (2013) [2].
- Consequences of DDoS attacks against a cloud environment were highlighted in some review papers as well by Anwar, and Malik 2014 [3] for DDoS attacks on the cellular network were explained by Merlo *et al.* (2014) [5], while Hybrid cloud environment architecture design is focused here.

This section presents the classification, as illustrated in Fig. (**7.2**), for the DDoS attacks as per degrees of automation, vulnerabilities exploited, attack rate dynamics, and impact of the attack.

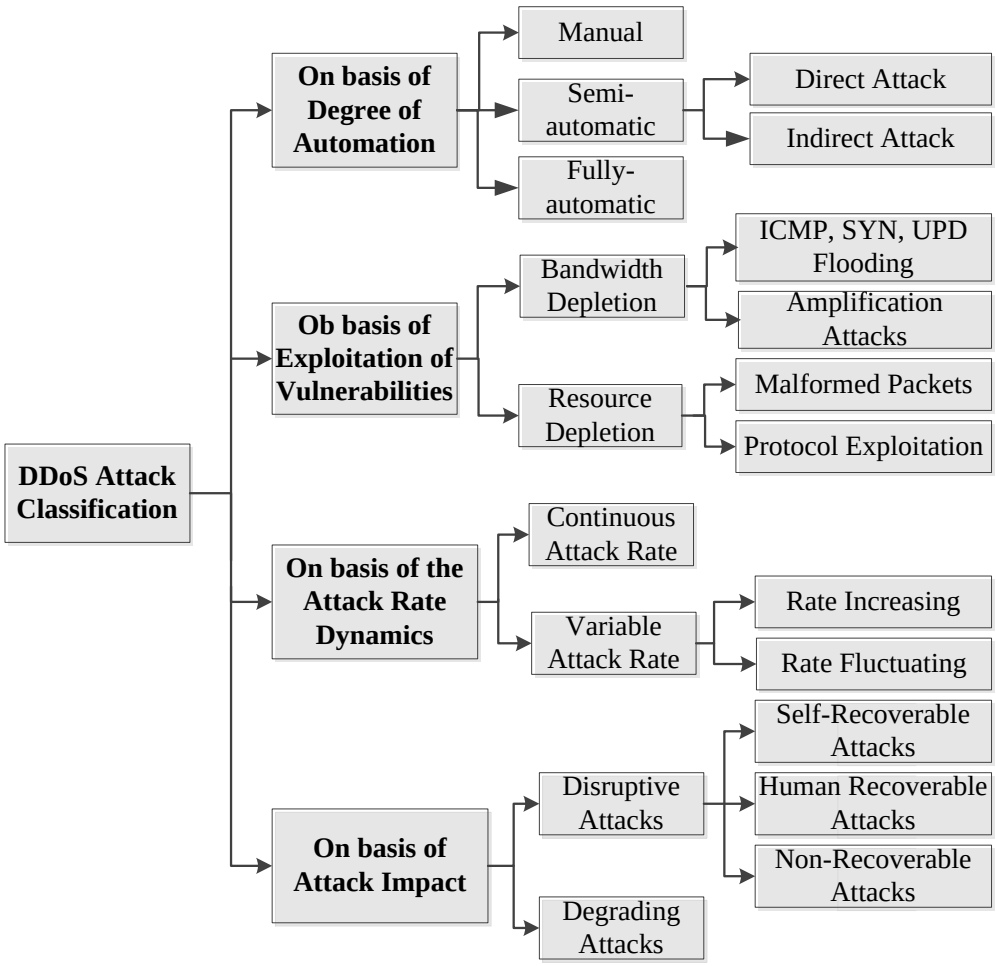

Fig. (7.2). DDoS Attack Classification.

2.1. As per the Degree of Attack Automation

The Manual attacks involve the attacker scanning the network, IP Addresses, and machines for vulnerabilities, breaking into the system and deploying a code, and executing a malicious payload for remote control access of that user system which is kept ready to launch an attack on the attackers' command. Semi-automatic attacks involve deploying attack scripts that scan and compromise the user machines and download a payload and install the attack codes. These victim systems are bots under the control of the handlers who choose when and how the attack type and targets victims. On the other hand, automatic attacks are carried

CHAPTER 8

Designing A Framework For Cloud Service Agreements For Cloud Environments

Abstract: Cloud Computing has emerged as the prime IT computing model for on-demand access using a pool of shared resources with the least IT support. Cloud computing is starting to replace the legacy office IT infrastructure and helpdesk support system. Corporate and home users alike are hugely turning into cloud service consumers and moving their data and work to the cloud. Therefore, the Cloud Service Agreement (CSA) between cloud service consumers and cloud service providers has a critical significance that can guarantee the highest level of service quality and delivery. The current CSA parameters and CSA terms tend to fall short of the service delivery commitments with no common terminology or standard followed industry-wide by the cloud service providers. Comparing similar service offerings and agreements from multiple cloud service providers continues to be a complex issue. This chapter provides a pragmatic approach to Cloud Service Agreements, comparing the current process with the proposed parameters and the new framework for CSA to determine the role of various elements and terms in the decision-making process for cloud service agreements for SaaS, PaaS, IaaS, and STaaS.

Keywords: Cloud Service Agreement, CSA, Cloud Service Agreement Framework, Cloud Computing, Service Level Agreement, SLA.

1. INTRODUCTION

Cloud computing is the new IT medium to provide virtualized computing resources in a dynamic, elastic, and scalable manner. This enables dynamic on-demand requests from cloud service consumers, corporate employees, or home users to access computing resources. These include user requests for CPU, Memory, Storage space, Network/Firewall devices, Operating systems, Databases, Software, apps, and development environments to be delivered and made available involving minimum IT Administration or IT helpdesk support. As the number of cloud-based services made available over the internet by the cloud service providers multiplies, this requires having a well-defined Cloud Service Agreement (CSA) as an essential component that should be referred to by end-users and cloud service providers (National Institute of Standards and Technology, (2011) [1]. This guarantees service delivery superiority and agree-

Akashdeep Bhardwaj

ment compliance is preserved and delivered at defined levels irrespective of the dynamic nature of future requests. Service Level Agreements for Cloud Computing Services are termed Cloud Service Agreement CSA) and include the cloud service consumer, cloud service provider, and the service agreements between them (SoftLayer, 2016) [2]. The Cloud Service Consumer is the end-user needing to access cloud computing services. These individuals (like corporate employees) consume services from the cloud service provider demanding appropriate cloud service delivery and the service level agreements that are in place with that cloud service provider. As cloud computing provides scalability and flexibility, cloud consumers pay for the type and amount of cloud services used and pay accordingly. Cloud users thus require CSAs to ascertain the service delivery and technical performance demands that are delivered by the cloud service provider.

Cloud service providers are organizations responsible for providing the cloud services to end users/cloud users and are mandated to deliver and administer the computing infrastructure required to ensure the cloud services are accessible to the cloud consumers. Cloud Service Agreements, therefore, help accomplish specific environments requested by the cloud service consumers regarding service, security, privacy, and solutions for issues when faced with delivery failures. A cloud service provider could also state in the service agreement about guarantees that are not available to users, *i.e.*, restrictions and duties that cloud users have to approve. A cloud user can select a cloud supplier with preferable pricing and more complimentary requirements. Normally, a cloud supplier's pricing strategy and service agreements are non-negotiable, unless the user is looking for comprehensive or customized services from the cloud service provider. The Cloud Service Agreement concerning the cloud service provider as well as the cloud service consumer is examined in this chapter to draw attention to its importance. This chapter discusses the general overview of Service Level Agreements and the advantages the proposed Cloud Service Agreement delivers, such as: improving customer acceptance levels, enhancing relationships, and enhancing the cloud service quality. Cloud Service Agreements contain responsibilities and activities that need to be completed after service starts to get delivered. The service contract governs quantifiable terms and conditions for the service provider in case there are delivery issues and the minimum objectives are not being met. Cloud Service Agreement is being implemented in a variety of Cloud domains related to IT delivery services such as Web Hosting Services, Network Delivery, and Data Centre Management.

2. CLOUD SERVICE AGREEMENTS OVERVIEW

The clients of SaaS might be corporations that offer their users/customers access to software applications, end-users who immediately exploit software applications, or software application providers who constitute applications for the clients. SaaS expenses can be paid according to the number of end-users, the usage time, the network bandwidth spent, the quantity of information kept, or the period of keeping information. Cloud clients of PaaS can exploit the instruments and the resources supplied by cloud service providers to progress, examine, install and administer the applications presented in a cloud medium. PaaS clients can be application designers who develop and maintain application software. Also, they can be application examiners who execute and examine applications in cloud-based locations. They can be application publishers who distribute applications through the cloud or can be application managers who constitute and control applications. PaaS expenses can be paid based on, operation, database space, network resources used by the PaaS application, or the period of the platform convention.

With Security, Availability, and Quality as the prime features of cloud services, the cloud Service Agreements should be adhered to as described in the below-mentioned stages by user and cloud service consumers when evaluating Cloud Service Agreements and negotiating service delivery terms with cloud providers. The Cloud Service Agreement stages as mentioned by Clouds Standard Customer Council (2014) [3] are described above in Fig. (**8.1**). Clients of IaaS have an entrance to virtual computing machines, network storage space, network groundwork elements, and other essential resources on which they can install and operate random software. The clients of IaaS can be system designers or system managers who are concerned with running, organizing, and controlling services for IT groundwork processes. IaaS users are provided with abilities to enter these resources, and are paid depending on the quantity of period of the resources used like; CPU hours consumed by virtual computing machines, capacity, network bandwidth used, and quantity of IP addresses utilized for particular periods. Cloud users want a CSA before delivering their deployment of cloud information stations to have confidence about the resources supplied and to have the facility to get the preferred level of efficiency. The study on Cloud Service Agreement and Quality of Service (QoS) metrics has been done by lots of investigators in business and service-oriented construction like e-commerce and web services. Nevertheless, the normal IT Service Level Agreement (SLA) metrics in these fields are not appropriate for cloud computing because the kind and form of resources supplied and deployed are various. So, new SLA samples are needed to provide an elastic technique for making conventions between users and suppliers.

CHAPTER 9

Comparing Single-Tier And Three-Tier Infrastructure Designs Against DDoS Attacks

Abstract: With the rise in cyber-attacks on cloud environments like Brute Force, Malware, or Distributed Denial of Service attacks, information security officers and data center administrators have a monumental task. Starting from the need to safeguard the client data, data center security, and ensuring cloud service availability, the team needs to ensure the highest priority to service delivery performance and functionality being offered to the service consumers. Organizations design data center and service delivery to cater to maximize device provisioning & availability, improve application performance, ensure better server virtualization and end up securing data centers using security solutions at the internet edge protection level. These security solutions prove to be largely inadequate in times of a DDoS cyber-attack. In this chapter, traditional data center design is compared to the proposed three-tier data center architecture design. The author performed DDoS attacks on both architectures to determine the resilience to withstand DDoS attacks by measuring the Real User Monitoring parameters and then validated the data using the Parametric T-Test.

Keywords: DDoS, Data Center, ICMP, LOIC, RUDY, Single Tier, Slowloris, Three Tier.

1. INTRODUCTION

Modern-day cybercrime attacks are specific, targeted, and designed to compromise high-value customer data, including personal, financial, and corporate intellectual property. Distributed denial of service attacks is not just aimed at bringing down network infrastructure, hog bandwidths, or compromising applications. Bigger dangers are lurking behind these attacks targeting data security. Modern-day Data center designs have evolved in recent times, migrating from in-house private hosting centers with physical servers to hybrid clouds, spread across multiple locations with Software Designed Networks (or SDNs), virtualized hosts, Application Centric Infrastructure (or ACIs) running automation for IT recovery, detection tasks, dynamically accelerating application deployments with DevOps policy model for network, storage, servers, and services. Designing secure data centers has now become mandatory as well as challenging.

Akashdeep Bhardwaj

The motivation to perform this research firstly aims at designing a secure data center architecture; secondly, with security implementations being highly complex, one-off customized implementations as per client requirements, network architects and cloud providers tend to lean towards accelerating application and service delivery, dynamic scalability, resource availability, reduced operating costs and increasing business agility. Cloud providers tend to keep security on low priority, which results in security gaps that impact security and performance, real-time protection, Internet peering, or the use of dedicated protection technology right at the Data Center edge routers checking the inbound traffic seems to be the best way to mitigate DDoS attacks targeting the proposed businesses proactively.

2. LITERATURE SURVEY

Lone *et al.* (2013) [1] deployed a virtual machine-based intrusion detection with a graphical interface to monitor cloud fusion alerts by using Eucalyptus cloud architecture for the front end and MySQL database for the back end. Attacks are captured by the Barnyard tool while using SNORT for signature-based DDoS rules. The Stacheldraht tool is utilized for generating resource depletion data packets. These packets consist of UDP, TCP SYN, and ICMP floods. These attack packets are captured during the attack and stored in the central MySQL database. However, a limitation of this signature-based approach is that unknown or zero-day attacks could not be detected.

Bakshi *et al.* (2010) [2] proposed an Intrusion Detection based on Signature detection for DDoS by using virtual machines running SNORT to analyze real-time inbound traffic. The defense framework identifies the attacker's IP Address and auto scripts an Access Control List configuration for dropping the entire packets from that IP Address and black listing it immediately.

Gul *et al.* (2011) [3] have mentioned that an intrusion detection model that analyzes and reports on the attack packets is utilized to handle a large packet flow. These reports should be shared with the cloud actors involved. To improve the performance of the Intrusion Detection System, multi-threading techniques are used. The final evaluation concluded that the use of multi-thread deployment, as compared to a single-threaded deployment, is more efficient.

Shamsolmoali *et al.* (2014) [4] proposed using a statistical filtering system with two levels of filtering. The first level of filtering involves removing the header fields of incoming data packets, then comparing the time to live (TTL) value with a predetermined hop count value. If the values are not similar, the packet is termed to be spoofed and immediately dropped. The second level of filtering

involves comparing the incoming packet header with a stored normal profile header.

Zakarya (2013) [5] proposed an entropy-based detection technique that identifies attack flow based on distribution ratio using the attack packet dropping algorithm. The entropy rate identifies the attack flow, dropping the packets if the DDoS is confirmed. Cloudsim simulation shows an accuracy of almost 90%.

Vissers *et al.* (2014) [6] utilized Gaussian Model to perform defense against application-layer attacks on cloud services using the parametric technique. Malicious XML content in use requests inside SOAP resulted in DDoS attacks. Initially, the detection involves HTTP header inspection to detect any HTTP floods and SOAP action inspection. Then XML content processing action is checked for spoofing by comparing previous data. While this works very well for existing DDoS attacks, the disadvantage is the inability to detect the new-age threat vectors arising from new request schematics.

Girma *et al.* (2015) [7] proposed a Hybrid statistical model to classify the DDoS attack pattern using an entropy-based system and covariance matrix measuring the heightened data dependency. Similarly, Ismail *et al.* (2013) [8] proposed a dual-phase mathematical model with a covariance matrix for detecting DoS attacks on cloud application services. The first phase involves baselining the normal traffic pattern by mapping it into a covariance matrix. The next phase compares the current traffic with the baseline traffic pattern.

Using game theory, Bedi and Shiva (2012) [8] proposed securing cloud infrastructure from DDoS attacks. The legitimate and malicious virtual machine behaviors are modeled with a game-inspired firewall defense.

Huang *et al.* (2013) [9] proposed a Multi-stage detection and text-based system with a Turing test to mitigate HTTP request flooding attacks. The system works in a modular fashion, with Source checking and counting modules intercepting incoming packets, the DDoS attack detection module checks for the DDoS attack, with the Turing test challenging the packets by using text-based questions and answers to determine if the packet is suspicious. The attack detection module retrieves and records the traffic behavior of each virtual cluster for any suspicious traffic behavior by the inbound data packets. The text-based turning testing module receives the redirected blocked packets and presents a randomly selected question to the requester. Access is granted only if the question gets answered correctly. The question pool is updated regularly, and the system is a Linux kernel. The performance test suggested a low reflection ratio and high efficiency.

CHAPTER 10

Security Challenges For Cloud-Based Email Infrastructure

Abstract: To stay connected and interact with global peers, friends, co-workers, and corporate employees, use email communication technology to perform business with customers and communicate with each other globally. Emails are the best and simplest way of cyber communication. Email is often the first thing we do when entering the office as well as the last thing we do when going to bed. With Cloud-based services providing email servers and infrastructure hosted over the Internet, Security assumes a significantly high level of priority in today's cyber world. This chapter reviews the academic literature published on security challenges faced by Email Infrastructure over Cloud, discusses the limitations of Email protocols, and compares using cloud-based email infrastructures and on-premises email servers.

Keywords: Email Infrastructure, Email Cloud Service, Exchange Server, SMTP, POP3, IMAP.

1. INTRODUCTION

Over the last few years, the recognition and acceptance of Cloud-based applications have gained a lot of momentum. Commercial applications that were initially installed inside corporate on-premises server rooms are now hosted on cloud infrastructures. Software applications are provided in the form of commercial services, which are accessible anytime, anywhere. Cloud-based solutions also eliminate the need for regular maintenance-related activities, unnecessary downtimes or outages, attention to backups, or regular infrastructure upgrades. Moreover, new Unified Communications and other Office Productivity applications can also be integrated with existing Cloud-based solutions. This ensures efficient, lean, and effective business processes as compared to an on-premises solution. Cloud-based email infrastructure systems like Google's Gmail, Microsoft's Office 365, and Amazon's Simple Email Service are no exception to this Cloud advantage, and these solutions have also witnessed a huge increase in usage and user base globally. Cloud-based email infrastructure resolves operation cost issues, revenue loss, business disruption, scalability, employee productivity, and IT support complexities which are typically associated with an on-premises

Akashdeep Bhardwaj

email server. However, mitigating Cloud-based security risks involves the service providers and corporate users adopting a universal approach for ensuring the right-fit solution is in place, especially when the application services over insecure Internet bring forth new threat vectors and cyber-attacks. Given the high usage of cloud applications and more so for Email applications, it is no surprise that Cloud-based email solutions tend to be the primary target of cyber-attacker. The intent is to disrupt corporate email operations, which cause business disruptions, financial impact, and reputation loss, or even seek to acquire confidential information from email servers.

Email infrastructure systems have to deal with security threats as mentioned below, as referenced from the SANS white paper [1]:

- Credential Phishers and Sender Impersonations
- Spam, Ransomware, and Virus payload attachments
- Typosquatting or URL hijacking *via* DNS exploitation
- Internal employee data leakage and insider threats

  Cyber attackers gain access to user accounts and mailboxes in the below-mentioned ways, as referenced from the SANS white paper:
- Repeated brute-forcing combinations of user/passwords using automated tools and keywords
- Spoofed emails directing employees to a hacking link, enticing them to enter Email Id and passwords
- Embedded malicious attachments in emails to allow access to the network servers or systems
- Use of Social Engineering and human error by sending a direct request from a trusted source

2. LIMITATIONS OF EMAIL PROTOCOLS

Like any Cloud or Network-based service, email systems need to provide the following five services for security reasons:

- **Message Confidentiality:** It promotes privacy, that is, the message transfer between sender and receiver is secure, and no one can read or track the message while transferring.
- **Message Integrity:** It says that the same message/data should arrive at the receiver end as it can be sent by the sender. No alteration intentionally or accidentally takes place during transfer.

- **Message Authentication:** It ensures that message can be received from the sender only or the trusted source. In this receiver must be sure about the identity of the sender.
- **Message Non-repudiation:** It ensures that anytime sender should not be able to deny sending the message originally sent by him/her.
- **Entity Authentication:** It ensures the identification of the user; the user must be verified before accessing the resources and services. This is done by asking for a login-id and password.

Email security protocols and their limitations are discussed in this section:

- **SMTP or Simple Message Transfer Protocol** helps exchange servers send out new emails regardless of any protocol being used for retrieving the emails outside the organization over the Internet, this works on ports 25, 2525, or 587. Issues with SMTP range from not being able to encrypt messages. So the communication between SMTP servers is in plain text, so eavesdropping takes place. As also, this protocol can only send messages in NVT 8-bit ASCII format but not for languages like Chinese, Japanese, German or Russian, which don't support the 7bit ASCII characters. If you are login into the SMTP server using your username and password, that is also passed in plain text, so again anyone stole your information during the transfer. Messages sent through SMTP also contain information about sending computers and software used, which, when captured, can be used for malicious intent. So SMTP lacks privacy concerns. SMTP does not have any mechanism to authenticate the source. It also does not have the functionality to check message integrity and so it is easy to send phishing attacks. SMTP does not have any mechanism to control repudiation that would make the sender deny sending of emails. The messages are stored on SMTP servers as plain text and their backups are taken. Even if you delete the message they can be residing on the servers/backup servers for years. So anyone who can access the servers can also access or read messages easily.
- **POP3 or Post office Protocol Version 3** allows for the one-way move of new emails from the email server to the client machine running Outlook onto the PST file. This works in either 'keep' or 'delete' mode on email retrieval over port 110. Issues with POP3 range from deleting an individual item does not remove it from the server, if mail is left on the server, care should be taken that there is sufficient capacity allowed before senders encounter a bounce-back message being informed that the "mailbox is full – try again later". Each ESP sets its own rules regarding how many emails can be stored for each account. Sending an email that ultimately gets saved in the "Sent Items" folder is available locally only – not on the server. That means that any messages sent *via* Device #1 will not be accessible *via* Device #2. Contacts, calendars, and tasks

CHAPTER 11

Efficient Fault Tolerance in Cloud Environments

Abstract: With mission-critical web applications and resources being hosted on cloud environments, and cloud services growing fast, the need for having a greater level of service assurance regarding fault tolerance for availability and reliability has increased. The high priority now is ensuring a fault-tolerant environment that can keep the systems up and running. To minimize the impact of downtime or accessibility failure due to systems, network devices, or hardware, the expectations are that such failures must be anticipated and handled proactively, quickly and intelligently. This chapter discusses the fault tolerance system for cloud computing environments and analyzes whether this is effective for Cloud environments.

Keywords: Fault Tolerance, Replication, Redundancy, High Availability.

1. INTRODUCTION

The growth of the internet and cloud computing has transformed business opportunities globally. The availability of computing resources and IT services have risen from a low 90% to 99.999% for both corporate and non-business users. As more and more virtual business applications are being delivered over the internet to end-users and corporate enterprise employees, the cloud computing environment is evolving to deliver efficient services through innovative cloud models, multiple high-availability devices, and virtualized systems (Vishwanath *et al.,* 2010) [1]. These also include multiple layers of abstraction, which turn the applications and infrastructure more distributed and complex than ever before. On the other hand, end-users have come to expect a high level of fault tolerance and availability with swift and flawless execution of the hosted applications. Cloud providers and data center infrastructure management teams constantly strive to maintain this high level of availability and fault tolerance. Some of these methods are the use of Application Performance Monitoring (Armbrust *et al.,* 2010) [2], having multiple devices connected in high availability (HA) mode by over-provisioning devices, having a hot-swap Disaster Recovery (DR) site or Network Monitoring system to provide better fault tolerance in case of any downtime. Users expect their computing systems to have the ability to handle gracefully any

Akashdeep Bhardwaj

unexpected system or application programming malfunction and provide seamless availability, which in IT jargon is termed fault tolerance, as described below.

- **Fault Tolerance** means that the loss of service (the network itself, some host, or some critical software running on a host) is tolerated by the system (Yu *et al.,* 2016) [3]. Usually, it means that there are enough other instances of that service available that the system can use those other resources without a significant impact on the system's overall responsiveness.
- **Load Balancing** means that a large workload is shared among many instances, as presented by Zhao *et al.* (2010) [4] of a service (or many hosts, or even many instances of the service on many hosts) but doesn't guarantee fault tolerance, though it can help (Chen *et al.,* 2010) [5]. If one of the available participants in the load-balanced cluster fails, odds are that there are enough resources available to continue satisfying requests. However, if the load balancer itself fails, the cluster might become useless. The load balancer itself might need to be fault-tolerant - there might need to be two load balancers.
- **High Availability** ensures that a resource is available, even as the resource may suffer from some amount of minor downtime, Fault Tolerance (FT) can be defined as not losing (Kumar *et al.,* 2011) [6] that in-memory session state in an event of a failure like having a host server crash or a network device failure rather than the service failing.

2. FAULT TOLERANCE FOR CLOUD ENVIRONMENTS

Fault Tolerance aims to ensure systems can deliver in case of one or more failures of the unit’s components. Fault Tolerance [7] is system resource availability and reliability not being affected in case any of the preceding component or execution devices (Pandi *et al.,* 2016) [8] fail or there are multiple failures for the hosted application system or infrastructure devices (Mohammad *et al.,* 2016) [9]. Usually, systems, devices, or resources are often over-provisioned or purposely underutilized to ensure that even if the application performance might be affected during an outage, the systems continue to perform possibly at a reduced level, rather than falling within predictable and acceptable bounds. Fault tolerance is mostly implemented in high-availability life-critical system environments. Providing fault-tolerant design for every single component is, however, not an effective solution. The associated redundancy and over-provisioning [10] bring several parasitic penalties: increase in weight, cost, power, size, consumption, as well as time to design, verify and test before delivering the service. The following options are taken into account when determining how and why the computing components should be fault-tolerant:

- **How critical is that component?** In a data center, having a spare catalyst running idle is good to have but not critical, with a low failure rate Catalyst switch would be low on fault tolerance while an extra Supervisor management module would be great to have.
- **How likely is the component expected to fail?** Some components, like disk drives in SAN or Power supply in servers a car, are likely to fail, so fault tolerance is needed.
- **How expensive will it be to make fault-tolerant components?** Having redundant SAN would be too expensive both economically and in terms of commercials, weight, and space, to be considered.

Fault tolerance mechanisms can be subdivided into Hardware, Software, and systems.

- **Hardware Fault Tolerance** involves provisioning of secondary backup hardware components like CPU, Hard disks, Memory, and Power Supply. This type of fault tolerance delivers hardware support only by ensuring the availability of basic hardware backup components. This can, however, not mitigate error detection, accidental interferences among applications, or system program errors. In this stage, mechanisms that can perform hardware-related faults are used in which partitioning of a node into smaller units can in turn, perform as a fault control unit. Each such node is in turn, backed up with a secondary redundancy to inculcate the failure of one of the modules, then the other redundant modules can act or take up the function.
- **Software Fault Tolerance:** requires the use of a special application that is designed to take into account faults and errors originating from software and programming. This utilizes static and dynamic redundancy methods which are similar to the hardware fault mechanism. N-version programming approach, which provides static redundancy and Design Diversity and adds hardware and software fault tolerance, is used in this mechanism.
- **System Fault Tolerance:** This system stores not only the checkpoints but also errors detected in the applications. When a fault or an error occurs, the system provides a correcting mechanism.

3. LITERATURE SURVEY

A review of existing literature on Fault Tolerance for Cloud environments is presented in this section.

Heli Amarasinghe *et al.* (2017) [11] introduced a fault-tolerant IaaS resource management framework for networked cloud Infrastructure. Distributed multiple

SUBJECT INDEX

A

B

C

D

E

F

G

H

I

M

N

O

P

Q

R

S

T

V

W

AKASHDEEP BHARDWAJ

Dr. Akashdeep Bhardwaj is working as Professor (Cyber Security & Digital Forensics) at University of Petroleum & Energy Studies (UPES), Dehradun, India Dr. Akashdeep is an eminent IT Industry expert with over 27 years of experience in areas such as Cybersecurity, Digital Forensics and IT Management Operations, Dr. Akashdeep is the mentor of graduates, masters and doctoral students and leads several IT Security projects. Dr. Akashdeep obtained Post-Doctoral studies from Saudi Arabia, Ph.D. in Computer Science, Post Graduate Diploma in Management (equivalent to MBA), and an Engineering Degree in Computer Science. Dr. Akashdeep has published several copyright, patent, research papers, authored & edited books, and chapters in international journals. Dr. Akashdeep worked as Technology Leader for various multinational organizations during his time in the IT industry. Dr. Akashdeep is certified in Cybersecurity, Compliance Audits, Information Security, Microsoft, Cisco and VMware technologies.