Chapter

Cloud Computing Security Services to Mitigate DDoS Attacks

Akashdeep Bhardwaj and Sam Goundar

Abstract

This chapter focuses on the challenges and risks faced in cloud security services in the areas which include identity access management, web security, email security, network security, encryption, information security, intrusion management, and disaster management while implementing a cloud service infrastructure. This chapter endorses the best practices in successfully deploying a secure private cloud infrastructure with security measures and mitigation and proposed a unique three-tier infrastructure design to mitigate distributed denial of service attacks on cloud infrastructures.

Keywords: threats/vulnerabilities, security policies, data protection/security, firewall, security model, monitor traffic, authorization

1. Introduction

Cloud computing is vastly increasing in demand for its popularity. Cloud services deliver up to its expectations if properly maintained. Users choose cloud because the cost is affordable, is easy to access, and has a positive uptime. Unfortunately, a high number of cloud users face difficulties when issues arise such as the frightening news about data confidentiality and integrity which gets posted online all the time, and they are in darkness when such situations occur [1]. In this modern age, cloud computing has been progressively popular within the IT organizations, and we notice many institutes are moving most of their IT services towards the cloud services here in Fiji to improve their information communication technology (ICT) service delivery to the clients or stakeholders. It is important for any organization to do an appropriate background research before making decisions of upgrading for which type of cloud services they are acquiring, depending on the organization's requirements. Many organizations prefer a private cloud infrastructure which has many advantages compared to the public cloud and hybrid cloud services; however, administrators tend to overlook that private cloud infrastructure comes with an exceptional set of challenges and risks. Cloud computing security service categories are identified and illustrated as follows:

- Identity access management
- Data loss prevention
- Web security

- Email security
- Network security
- Encryption
- Information security

2. Literature review

Cloud computing security keeps on changing as new technologies emerge. Services provided by the three basic cloud service models, which are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), give more outbreak to exploit such state-of-the-art models. As the cloud expands, so does its vulnerabilities [2]. It is the hosting providers or administrators duty to ensure that these vulnerabilities are kept on patching up as new threats arise. One must always be on the look for any threats coming their way towards the cloud servers. If such threats enter the cloud, it could be devastating for the cloud hosting providers and even the cloud servers itself. We as human beings need to keep in mind that a person who wants to get the data for their benefit or even for fun purposes [3] creates those threats. There are certain software programmed and integrated to the cloud server to automatically mitigate a certain level of threat, and an example is a web application firewall (Barracuda).

Stated in the research paper regarding a study on security model in cloud computing, we vastly agree to the statements stated such as the security being a real-time obstacle of the everlasting picture and foundation of cloud computing [4]. Furthermore, this research will now move towards focusing on the security aspect and its services shown by cloud computing itself as keeping in mind the increasing need for security in the cloud as we see a new day moving forward in our daily lives.

This paper starts with cloud identity access management as the first level of cloud computing security service that we identified based on various researches conducted. Whenever a user has established the connection to the cloud, the user will need to login and access the cloud resources in order to drive forward the idea of hosting applications, websites or even doing online sales securely through a secure login tunnel. This has to be fully done by successful authentication and authorization to avoid loss of data and identity being manipulated which could lead to unwanted access to the cloud system [5].

The need to have identified information in this case, which related to identity access management itself, first needs to be synchronized so that there are no conflicts when identifying the cloud user [6]. One needs to keep in mind there are many users who have the same name although their username can differentiate the users and their level of access. For user information to be synced properly, the old user data will need to be checked if there are any, which were used previously, and it should not match with the new data. Such scenarios occur when a user cancels their online subscription to a cloud host provider and comes back after a few years wanting to again host their applications on the cloud [7]. This reflects on mostly public clouds. This can also be hinted at a private cloud when the administrator permanently deletes the user's data, which in this case is the user's login and registration details to focus on. A hacker can pose as a new user and easily gain access to the cloud system if he/she is able to manipulate the registration and other details.

This can happen when the administrator is adding a new identity to the system, and if the administrator is not careful, the system does not identify old data. This will lead to an identity within the cloud system that will gain access to certain module level-based information because the identity has not been synced and verified with real time updates [8]. Another issue could be confidentiality, which focuses only on authorized access to cloud data; an authentication that is related to checking of the received data to be from a legit source and integrity, which relates to only authorized party, should be allowed to modify data in the cloud [9].

Building trust in cloud computing services may help prevent data loss to some extent, but it does not guarantee it. The cloud server needs to be equipped with state-of-the-art hardware and software in order to prevent such issue. This service protects data from being lost based on the rules deployed on cloud servers. Data can be lost in various ways such as the hacker sends a malicious file, which infects the cloud server and deleting the files and folders [10].

Data storage repository must be secured enough to handle such attacks although the level of attacks varies from high to low and each attack is to be considered no matter which level that threat is. Suppose a low level of threat occurs in the cloud server where that data is stored and the administrator does not take any action to fix the issue or just ignores it thinking that it is a small issue, it could multiply and do its job on the storage server leading to data loss [11].

Securing the storage in the cloud is very important where the storage or based in geographical location or not, but at the end of the day, the storage repository is linked to a network and that is enough information for an advanced hacker to easily delete the data by entering into the system from just a small script which will eventually grow to a virus or Trojan to inflict the damage.

If the administrators are not monitoring such scenarios, that virus can do the damage to the storage server. In such cases, it may send a lot of traffic request to the storage server, and this can result in overload. Such case is mostly described as denial of service attacks. With DoS attacks, the server will notice a change in traffic load coming in, and if there are no intelligent applications installed in the server to mitigate, there could be serious implications. These attacks can corrupt data, delete data, and data loss. This is a common issue faced by a lot of users, which ultimately will become the administrator's responsibility.

We noticed a virus spread across the globe called WannaCry, which is a ransomware virus where it locks down your computer system and asks for money in order to unlock the affected system. This type of attacks can lead to data loss as well. Supposedly, this threat can affect the data stored in the cloud server, which is definitely huge on a threat level. Microsoft had to realize patches for their operating systems in order to prevent such attacks. This results in a lot of distress around the globe and was one of most talked about attacks. It not only inflicts damage to the affected system, but it also has the ability to destroy the data itself, which is stored in any system [9]. One must be very careful of such attacks if not then data loss is inevitable. Such attacks are a wake-up call for cloud system, which does not have any type of data loss prevention techniques implemented, and if such techniques are implemented, then the administration must map out ways to block or to prevent data being lost. Therefore, security rules need to be in place to avoid customers from being frustrated with one of the major issues, which are data loss [4].

Web security plays a vital role as well in clouds. While the servers are hosted in clouds, websites and applications are also hosted in it which combines the functionality to work with cloud resources and deliver as expected to customers. Protection against virus and malware nowadays is very common as new types of such threats emerge almost every day. In cloud, all folders are synchronized at all times as the

user updates their data. What could happen is that if a malware enters the cloud and data sync is taking place, the malware gets synched together, spreading around with the configured account, which is the source in which the malware entered into the system [11].

Hosting service providers for cloud-based will need to get a good web application firewall (WAF), which can prevent attacks to web servers and applications. Traffic going in and out of the web server needs to pass through WAF in order to check for malicious responses [12].

As proposed in the paper by Fernandez et al [13], web application scanner and a cloud-based web application firewall can be used to identify vulnerabilities and scan for sensitive data [13]. This type of scanner is very useful in a cloud computing environment. The cloud-based web application firewall will also be integrated with the scanner. The first step will be the scanning process followed by filtering unwanted request, keeping in mind that these unwanted requests are the virus and attacks coming into the system. In their paper, they have also stated that the firewall can control the web application communication via HTTP based on the rules for authorizing and with the main purpose for it to stop SQL injection, XSS, and other types of similar attacks on the cloud servers [12]. What our research has looked into is one of the WAF available for purchase called Barracuda. This application is very useful as it generates a whole lot of data that is not required for processing based on the traffic flow in which the attackers can come in and out of the system. This application has the ability to scan, put cloud applications and websites behind a state-of-the-art firewall system, and monitor traffic to name some of its core functionalities. When we look at a WAF system for cloud, we must have reports generated in order to do research that is more thorough from where the particular attack is coming from and how these attacks can be mitigated. The WAF provides a solution to every attack or vulnerability that is present in the generated report as well. This firewall will be able to stop unwanted traffic into the system, keep the cloud servers safe, and transfer those IP addresses that are suspicious to the suspicious list from the whitelist causing it to be classified as a threat [14]. The users can do online banking securely and other tasks that they would prefer to be done under a secure application layer.

Email security is being implemented in clouds as well. It has major advantages. Any inbound and outbound emails will need to go through email security protocols to ensure that the user sending and receiving the email does not contain any type of malicious data, which can affect the customers' online activity in any way. This could also lead to having a bad impact on web servers as well if proper security protocols are not in place to filter malicious emails. Cases of security policies need to be implemented in order to run the workflow of emails and filtering unwanted emails [15].

As outlined in the paper published as from Barracuda itself, using such application will not limit the functionalities of email security being deployed in the cloud servers. Some things to notice about the paper is that they have outlined the suit for the cloud services with the following combinations for the advanced package, multilayer security which extends the protection for the email also being integrated with Office 365 which is currently being well-known for its cooperative feature for an organization provided by Microsoft. Multilayer security is one of the core features that the email security giant company looks in depth, for the application itself is being a guard against threats arising from emails, data loss protection through spam emails, data being leaked with encryption, and all the email contents being inspected. Another advanced feature that they explained in their paper was cloud-based archiving. This feature is very important, and emails need to be

archived frequently for an organization. Such feature in the cloud will enable users to retrieve any previous email at any time from any device, and this can be from any cloud environment whether it being the hybrid cloud-based environment, Microsoft 365, Microsoft Exchange, and even any other types of email service being used on-premise. They also mentioned retrieving emails such as cloud-based backup and recovery features. This feature will allow the administrators to retrieve any email from the frequent backup storage and send it to the live server so that the user requesting for the email can view and retrieve their contents for that particular email [16].

According to Rawezh Tara and Nashwans' paper based on private cloud and implementation of software, routing in it identifies the use of virtual private network (VPN), which enables the ability to ensure that the user who is logged into the cloud service can do their online transactions without any issues. The attackers will not be able to judge where or how the data is being transferred to. This creates a secure environment for customers doing online shopping or banking. It is a good practice to provide VPN to users who are already logged into cloud service. Each user will have a VPN client profile. Using this they can establish the VPN connection, and a secure tunnel is enabled, and authentication is being done on the data center firewall end [17].

Only two types of users use VPN tunnel, which will be the employees and the cloud administrator. The VPN tunnel works as the employee will establish a secure connection through a VPN tunnel; the employee will then login to the VPN client profile using username and password. The authentication is verified with the security policies and the data center. Once the connection is successful, the remote client is connected to the cloud and is ready to utilize the resources and services offered by the application itself. The login of the user will fail if the user is not a valid user, which is checked in the system mainly through the active directory [18]. This type of secure login is highly desirable and is present in the Barracuda application, which was also tested while carrying out this research. It not only protects the user's data, but the users who login into the system through VPN tunnel can be rest assured that they can perform their task without anyone capturing their information.

Encryptions ensure that the data, which are available in the cloud, is secure. Although there are many types of encryption techniques available, attribute-based encryption will provide favorable results. This provides access control with a private key, master key, and ciphers text [19].

Furthermore, as proposed a clear explanation of encryption by Rohit, Rituparna, Nabendu, and Sugata research paper based on security issues in cloud computing, they outline the very important aspect of how the encryption can occur in a cloud-based environment. The argument raised is that that data that is stored in the cloud is secure enough towards any type of security breach. They come up with utilizing homomorphed token, which can help secure data through encrypting by private and public keys, respectively. The trust-based methods for the cloud environment are very valuable towards secure private and public key exchange over a secure seamless synchronized connection. Moving on to further discuss encryption supposedly if data is not encrypted, spoofing attacks can take place. Such attacks can be checked by performing user authentication based on key exchange and even encryption techniques [20]. By enabling encryption sessions with filtering at the entrance of traffic management, such attacks can be avoided. Encryption plays a very important part in securing the cloud services with its unique ability to transform the data into cipher which makes the attackers difficult or almost impossible to alter the data.

Information security relates to gathering the alerts which come about the cloud service monitoring tools. Logs get created for the events. Being a central point, cloud computing is able to handle the information stored and how it gets altered by malicious activity which leads to a crisis situation. If an alert gets ignored, it becomes a golden opportunity for attackers to exploit the cloud services and can access the data of customers. If such a case does happen, the admin must take immediate actions and retrieve data backups. Cloud computing can aid in the seamless transfer of the information to a backup server which will store the information of all the customers. Cloud IaaS is a possible direction of data backup in which data needs to be firmly protected as it should be a specialized cloud-based backup server [21].

Intrusion management looks after the packets coming in and going out of the network. It has got a set of predefined rules which can handle a particular event. A cloud service provider needs to have an intrusion management tool such as anomaly detection. This type of detection system trains itself by observing network behaviors. It identifies the class level for the intrusion whether normal or intrusion, based on the network packets. If an intrusion is found, it should send a warning to the alert or information security system for further action [22]. Hadoop is an open source software, which is becoming popular with cloud administrators. Hadoop is used to distribute processing of big data using MapReduce. MapReduce is a model which can perform analysis very quickly to locate the malicious activity and the area in which the attack occurs [23].

Disaster management in collaboration with disaster recovery relates to cloud data storage in its servers. One must be prepared for it; thus, disaster rescue management can be put in place by the hosting providers in the cloud servers. Attackers can disrupt services by sending malicious requests to the server if there are no strong security policies placed, and they can create downtime of the server as the servers can get overloaded through it. For natural disasters, cloud hosting providers can place their data centers at geographical locations so that if one center gets affected, another will pick up and prevent downtime of services [24].

Looking at an infrastructure point of view, we picked Veeam, a software product developed by Veeam organization itself to replicate, backup, and restore data on virtual machines. It has a lot of capabilities as it pools together one of the leading backup services for a cloud infrastructure. Having the ability to replicate with advanced monitoring, reporting tools, and capacity planning functionality, Veeam is highly desirable to be used for a disaster management tool.

3. Methodology

Based on the research ideas provided, we have used qualitative research method, and the theory we have decided to use is as follows. A local user agent is created by the user to establish a temporary security certificate for safe authentication over a given period of time. This certificate will contain the username, user id, security features, hostname, session times, and other relevant features. Once this is done, the authorization for the user is finalized. As the user will start to use the resources on the cloud, mutual authentication will initiate between the cloud application and user. The application will check if the certificate is valid for the user, a security policy is applied to it. As per the requirements stated by the user, the application will create a list of service resources which will send it to the user. Finally, through an application programming interface (API) security used by the application, the user's session will be fully initiated and connect to cloud services [4, 13].

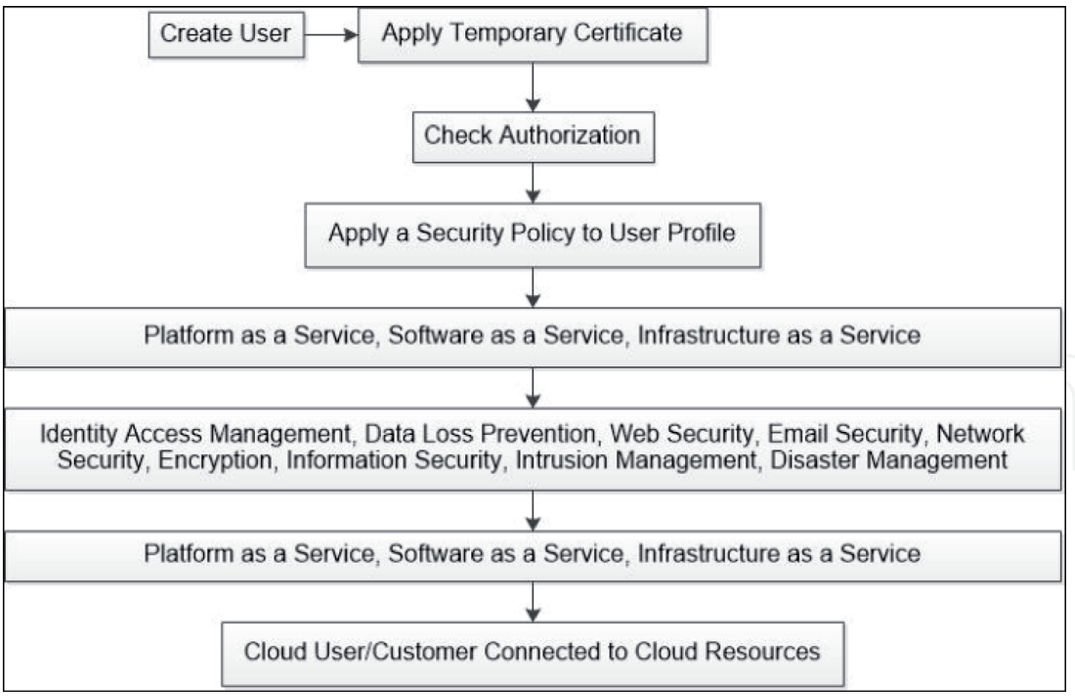


Figure 1.
Model for secure connection with a trusted certificate in a cloud environment.

Figure 1 describes the method for secure connection with a trusted certificate in a cloud environment and describes its successful implementation as well as usage of cloud resources.

Some of the research questions we have identified are as follows:

- Which security protocols you have placed in your cloud architecture to ensure a seamless connection between users does not result in online data theft?

- In case an attack on the cloud service occurs, how will the server mitigate those attacks?

- Is there a disaster recovery management tool in place for the cloud servers? If so then what procedures will be followed to ensure that there is little or no downtime?

- Are the cloud services running behind a trusted firewall? If yes, then how does the firewall report incidents as logs to the administrators and is the firewall artificially intelligent enough to challenge such difficulties?

Our research came up with some cost analysis based on cloud infrastructure. The below details were developed for a cloud-based premise comparing both private and public cloud. Shown below is the cost for Azure sizing based on the requirements; the cost is higher than the private cloud infrastructure with much higher requirements (**Figure 2**).

Shown below is virtual storage area network for a hyper-converged solution which is the most popular infrastructure technology in the current market according to Gartner report. This is very helpful for cloud-based organization to grow as it exceedingly with a lot of resources available for use in the cloud deployment models itself (**Figure 3**).

Based On	Azure Sizing (Public cloud)	Private infrastructure Requirement
Total vCPU	320	775
Total Memory (GB)	1280	2400
Total Storage (TB)	162.56	200
cost	$ 3,974,990.00	1.8 M Production and DR

Figure 2.
Cost analysis with Azure vs. private cloud infrastructure based on resource requirement.

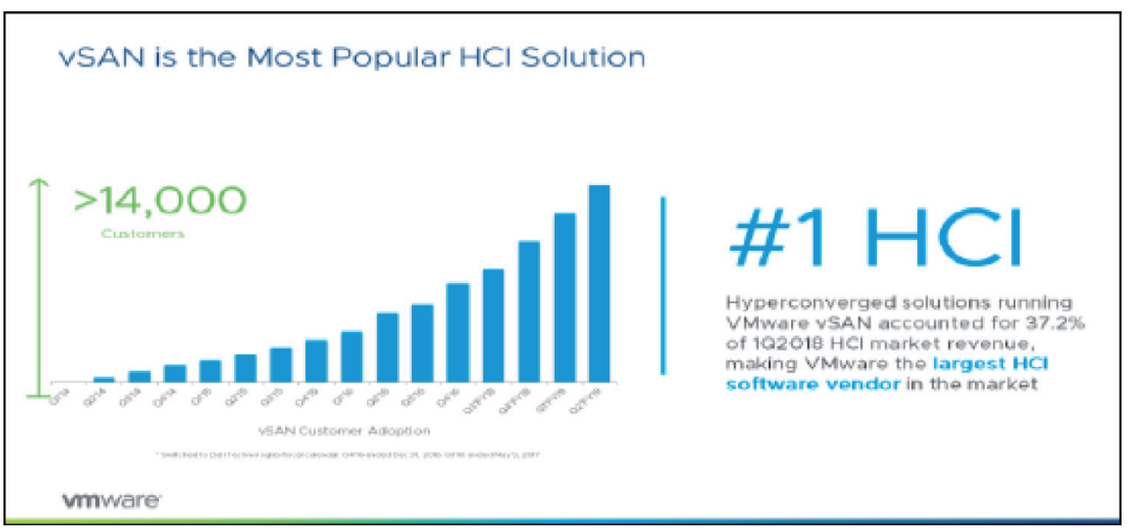


Figure 3.
Virtual storage area network for a hyper-converged solution.

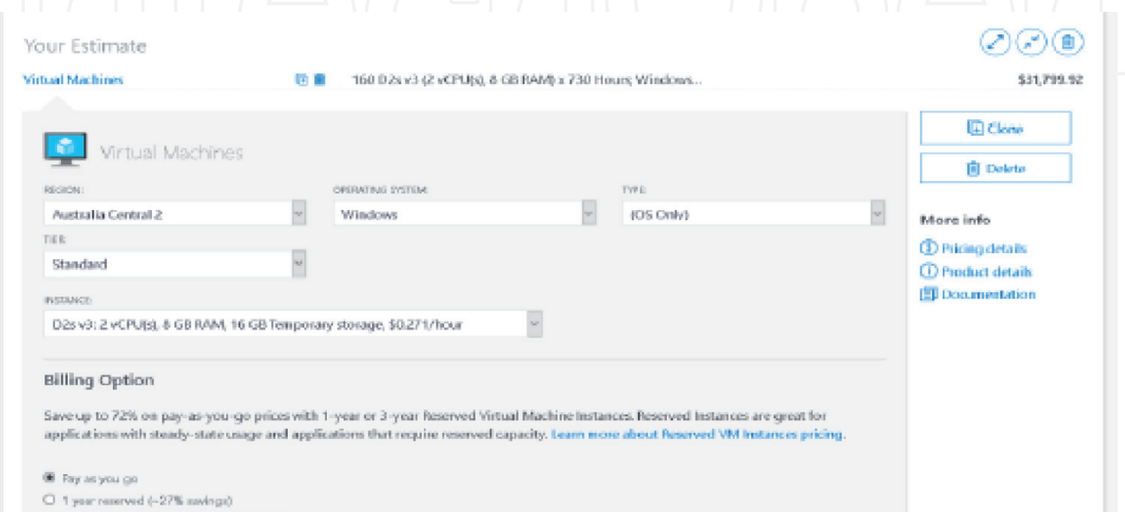


Figure 4.
Billing and purchase interface when requesting a virtual machine in a cloud-based environment.

Name	All Flash FTT1 / RF2
Hardware	Lenovo SR650
Number of Nodes	6
Per Node	Thinksystem SR650
Processor	2 x Intel Gold 6126 12C 2.6GHz
Memory	512GB
Storage Drive	15 x 3.84 TB
Cache Drive	3x400GB + 2x128GB M2
Networking	4 x 10GbE SFP+
Dual Hot Plug Power Supply	Yes
Warranty Hardware	3 Year
VMWare	Included
Cost Per Node	
Cost for Production	$ 900,000.00
Cost for DR	$ 900,000.00

Figure 5.
Costing for a cloud infrastructure with a disaster recovery package.

The screenshot shown below shows the virtual machine on a cloud premise. When a user wants to purchase a virtual machine, the cost related to the resources requested will be shown on the cloud interface and can be upgraded as well when one wants to deploy a virtual machine in their cloud (**Figures 4** and **5**).

4. Existing cloud security solutions

The focus of this research is on distributed denial of service (DDoS) attacks on the cloud. The authors researched on existing cloud security solutions and also present an implementable solution focusing on DDoS mitigation for IT infrastructure. The authors define the scope and recommend few focus areas:

- Defending volumetric attacks is a need for cloud components.
- Blocking application-level attacks without submitting SSL Key.
- Deploying acceptable network infrastructure as per IT security policy.

DDoS attack mitigation solutions are discussed here based on design perspective:

a. **On-premise based:** Having a devoted on-premise DDoS attack mitigation answer are first-rate desirable for government entities, financial establishments, and healthcare but not beneficial for all. When the highest stage of safety is mandatory and organizations opt to give as little visibility into their customer facts or approximately their encryption certificate to as few third birthday celebration providers, this could be regarded as a limited scope option. On-premise DDoS devices might store encryption certificates and inspect visitors regionally without any scrubbing, redirection, or inspection. The mitigation device would be required to guard against numerous DDoS vectors like flooding (UDP/ICMP, SYN), SSL based, application layer (HTTP GET/POST), or low and slow attacks. With mitigation structures in house, the proximity to facts center sources is useful, and the systems may be fine-tuned at once by the in-residence IT teams. They have a tendency to have a miles more cognizance to their setup for any adjustments in site visitor flows or from the

application servers. Thus, they might have a tendency to have a higher chance of detecting any suspicious traits or visitors requests.

b. **Cloud-based security services:** In providing anti-DDoS and superior mitigation protection in shape of managed security services, many cloud carrier companies offer protection from community floods with the aid of deploying mitigation system on the ISP network edge stage or with scrubbing centers. This involves traffic diversion from the corporation network to detection or scrubbing center. When a DDoS attack starts, human intervention is needed and takes as a minimum of 15–30 minutes all through which the online services are left unprotected and exposed. The cloud-based totally DDoS mitigation service guarantees quantity blocking off of community flood assaults from accomplishing the corporation edge devices or flooding the WAN circuit which is free of volumetric community flood attack. However, there exist glaring problems with a cloud primarily based on DDoS mitigation offerings.

   - Cannot discover and block application layer attacks and slow attack.
   - Unable to defend stateful infrastructure structures like firewalls or IPS.
   - Unable to deal with attacks like software layer attack, state exhaustion, and multi-vector attacks.

c. **Hybrid cloud-based security:** Using hybrid cloud functions gives the best-of-breed mitigation option, where the hybrid infrastructure combines the on-premise in-house setup with DDoS mitigation carriers to act as an included mitigation solution. In hybrid solutions, another option is to use a devoted DDoS mitigation provider's capability in order to detect and block a couple of DDoS vectors. Having public cloud issuer dynamically booms the community pipe bandwidth for the duration of a DDoS attack; takes off a while after being detected, till the time mitigation begins; and saves the on-premise infrastructure from the attack and affecting the provision of its online services. Typical answer is in the course of DDoS attack; the entire site visitors are diverted to a DDoS mitigation issuer's cloud, where it is scanned, scrubbed with the attack visitors getting diagnosed, and removed before being re-routed lower back to the in-residence information middle of the enterprise. Hybrid solutions permits organizations to gain from the following:

   - Widest security coverage that can simplest be finished by means of combining on-premise and cloud insurance.
   - Shortest reaction time by using an on-premise solution that begins right away and mechanically to mitigate the assault.
   - Single touch point during an attack both for on-premise and cloud mitigation.
   - Scalability—each tier is impartial of the other and can scale horizontally, in case there is a web application attack spike, adding extra WAF devices to ensure enough WAF capability may be done within the application defense tier without affecting the community tier.
   - Performance—on the grounds that requests come in tiers, network utilization is minimized, and load decreased overall.

- Availability—with hybrid solutions, if the first or second tier is down, at least there is one tier left to serve consumer requests. This satisfies the BCP of the organisation.

- Vendor independence—community and application protection infrastructure can setup the usage of hardware structures or even specific software program versions.

- Policy independence—while new policies are implemented at the application defense tier, the opposite tier directs simplest that specific visitors in the direction of the rules until they are established and ready for production use.

5. Proposed DDoS solution

Based on the developing threats and effect of attacks, company firms having their very own cloud services as well as cloud providers put into effect DDoS mitigation using hybrid cloud architecture. When there are multi-vector DDoS attacks targeted at layers 3, 4, and 7, mitigation strategies are essential. These mitigation strategies assist in detecting and preventing volumetric, software, and encrypted assault vectors. By making use of public cloud capabilities to cover for scalability taking on floods and appearing because the first point of defense with community and web application firewalls detecting assault visitors and mitigating the DDoS threats and the SaaS utility, web portals and backend database resides stable in the residence private statistics center. For this research, the experimental environment involved community infrastructure architectures being designed and setup to testing the proposed DDoS solution having the following hardware and software:

- Cisco 4000 ISR Series Routers and Cisco Nexus 5000 Series Switch for routing and switching

- Big IP LTM-4200 for high-performance application traffic load management

- Cisco Firepower FPR-2110, Imperva Web Application Firewall Gateway with Manager Console

- HP DL-360G8 1U-Rackmount with Intel E5, 128 GB DDR3, 32 TB SSD Servers

- VMware NSX-T 3.0 virtualization software on bare-metal HP Server

- SaaS Application running Windows Server 20012 64-bit OS

- Front End Web Portal with .NET supporting 2-Factor authentication

- Back End Database running Microsoft SLQ Datacenter license on Windows 2012 OS

- DDoS Tools for attack simulation: LOIC or Low Orbit Ion Canon, HOIC or High Orbit Ion Canon, Packet Storm (HTTP Unbearable Load King), Are You Dead Yet (R.U.D.Y), Motoma IO's PyLoris, Slowloris and TOR's Hammer

The networks were tested by community and alertness layer attacks with the use of ICMP flooding with a thousand echo requests with increasing buffer size from 3700 to 3805 bytes. The use of DDoS attacks such as LOIC, R.U.D.Y, and slowloris that simulated attacks denied valid users to get admission to the web software portal. When performing the simulated DDoS assaults, the real user monitoring records are taken as the standards, and parameters have been amassed for the logs to assist generated graphs for DDoS attacks. These parameters had been chosen due to the fact that they decide what performance problems the real users are experiencing on the site for the time being in actual time during an assault.

- Average ICMP latency (milliseconds) before and during the course of DDoS attacks on the apps
- Page load response that refers to time the app pages take to load and figuring out where exactly the time is spent from the time a user logs authenticates and logs in to until the page has loaded completely
- App response relates to the percentage time for a page load process to complete
- Status codes are gathered from the HTTP reputation codes the web server makes use of to communicate with the web browser or person agent

6. Performance analysis

6.1 Single-tier network architecture

The first framework was structured and implemented in the form of a single inbound and exit gateway. This mimicked the single-tiered level system including standard system design, directing the interfacing with an online interface containing the front end and back end. This simulated the standard cloud-based condition having a basic standard system configuration actualized in a server farm with hardware devices mentioned in the setup environment above (**Figure 6**).

Using the standard design, single-tiered architecture, multi-vector DDoS attacks were executed as network floods and volumetric and application layer 7 attacks. These critically overloaded and degraded the computing systems leading to access issues for legitimate users. Logs and data gathered for each attack are displayed below for reference (**Figures 7–9**).

6.2 Three-tier network architecture

The second infrastructure was designed as per the proposed design having three unique tiered designs. Each tier has different IP address schemes and communicates with others via site-to-site VPN. This design simulated public and private cloud integration. The first two tiers focused only on security protection against network and application layer attacks. The third tier only focused on access to the hosted SaaS application with database backend:

- The first Tier is built around layers 3 and 4 network defense system for IP and TCP defense using hardware firewalls and load balancer. This tier mitigates ICMP (Ping), UDP, or SYN flood attacks.

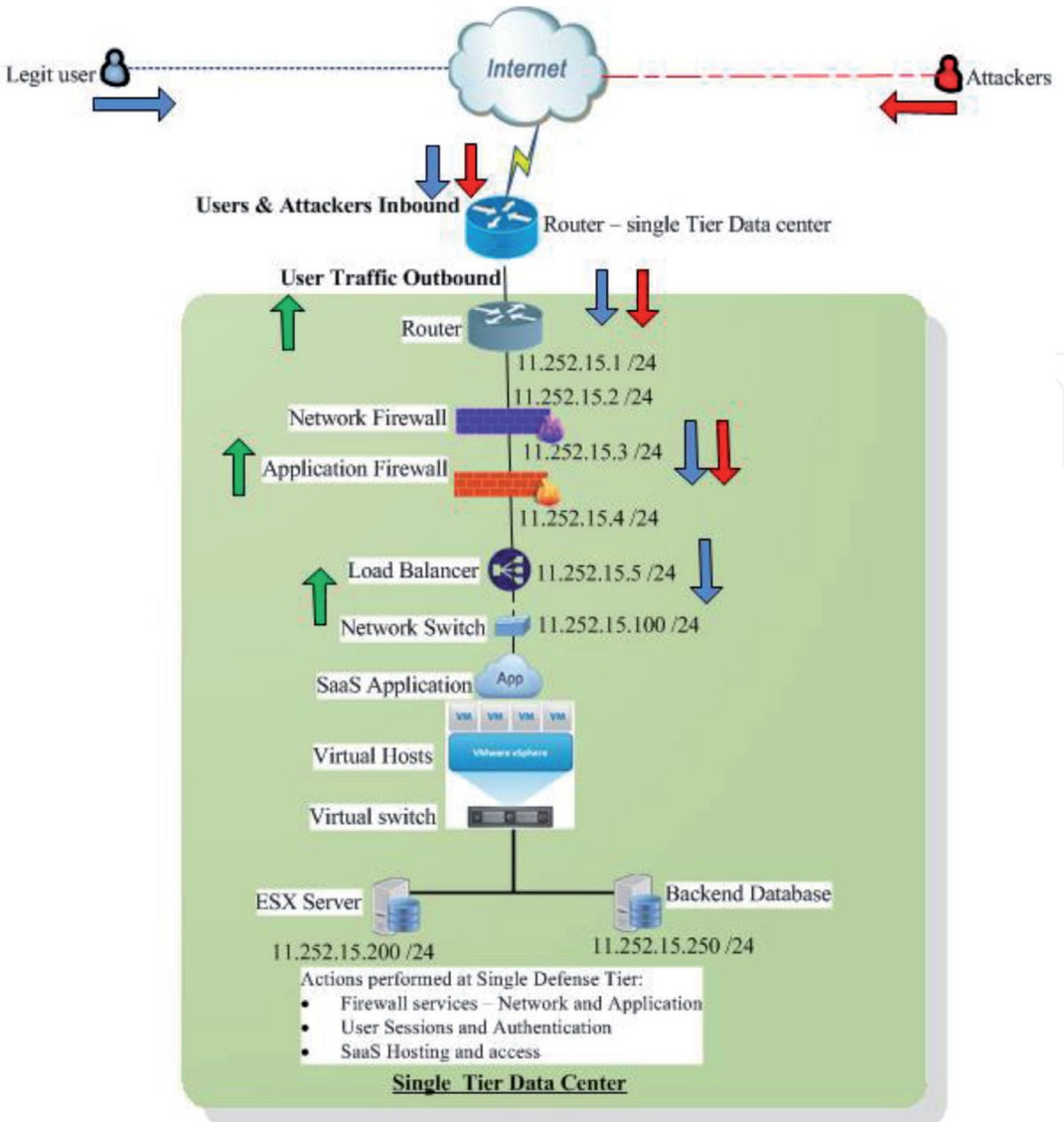


Figure 6.
Traditional architecture design (single-tier).

Before and After Attack Statistics:

Website Response for Network Defense				Real User Monitoring					
Attack#	Time (pm)	Buffer Size (bytes)	Echo Requests	Average ICMP (ms)	Page Load Response (ms)	Browser Throughput (rpm)	App server response (ms)	Status code	Attack Vector Deta
Attack#1	13:00	3700	1000	6545	45	1800	1636	200	No standard network layer place - single tier archi Ping AppServer -n 1000 Size: 3xxx, Echo request co
	13:30	3750	1000	6670	54	1856	1496	429	
	14:00	3760	1000	6575	55	1727	1624	200	
	14:30	3780	1000	6791	46	1627	1784	200	
	15:00	3790	1000	6583	41	1606	1713	429	
	15:30	3795	1000	6745	55	1806	1686	204	
	16:00	3800	1000	6790	50	1651	1488	429	
	16:30	3820	1000	6794	54	1761	1795	204	
	17:00	3810	1000	6690	47	1800	1833	503	
	17:30	3805	1000	6512	42	1849	1565	503	
	18:00	3820	1000	6692	48	1835	1726	503	
	18:30	3810	1000	6589	50	1635	1570	503	
	19:00	3805	1000	6995	50	1839	1663	503	
Attack#2	13:00	3750	1000	2795	30	1325	1297	200	Network Firewall Defense in Attack vector categories o ICMP/UDP/SYN floods pe
	13:30	3745	1000	2911	32	1327	1243	200	
	14:00	3760	1000	2805	29	1208	1298	200	
	14:30	3780	1000	2963	30	1306	1043	200	
	15:00	3770	1000	2746	29	1235	1097	200	
	15:30	3783	1000	2933	32	1245	1213	200	
	16:00	3780	1000	2988	28	1219	1228	200	
	16:30	3794	1000	2994	29	1270	1064	200	
	17:00	3790	1000	2666	31	1256	1066	200	
	17:30	3789	1000	2934	28	1293	1282	200	

Figure 7.
Single-tier DDoS attack logs.

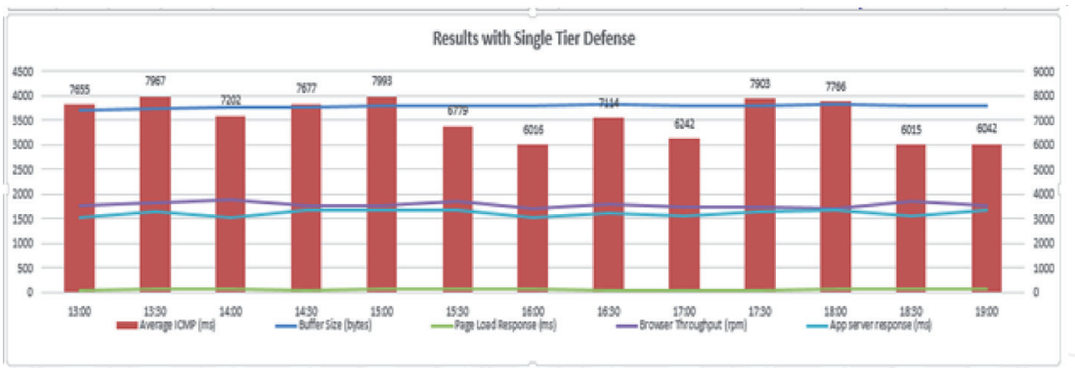


Figure 8.
Single-tier attack results.

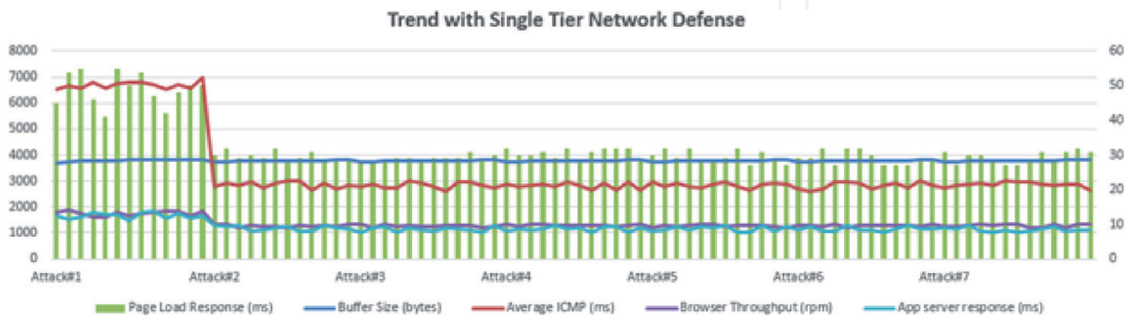


Figure 9.
Single-tier results (with and without network security).

- The second Tier provides layer 7 application defense using web application firewalls and customized load balancing rules along with SSL termination. This tier mitigated ARP spoofing, POST Flood, and DNS poisoning and detected malwares from inbound user traffic.

- Once both network and application attacks are cleaned from the traffic, only legitimate user traffic remained. This traffic is directed to access the private tier cloud (or the third tier), hosting only the SaaS Web portal. After processing and completing the work, user traffic is again reverted to tier 2 for exit instead of tier 1 and following the same traffic route back to the user. This form of asynchronous routing ensures the attackers are not able to execute denial of service attacks that always have the condition of user traffic having the same inbound and outbound gateway and traffic routes (**Figure 10**).

DDoS assaults were performed at first on the single-level system plan and our proposed three-level system structure and assembled result that demonstrate our proposed half-breed cloud configuration having the main level for accepting inbound traffic from clients and aggressors with layers 3 and 4 gadgets and performing system assault alleviation, utilizing a system firewall blocking ICMP floods. The inbound traffic was then permitted to stream to the second level which alleviated application-level assaults utilizing a WAF. Here utilizing F5 and Cisco gadgets intelligently, we had the option to square 80% of the assaults. This was assembled subsequent to contrasting the assault information and single-level system arrangement. The three-level system configuration is executed in a test server farm with Cisco and F5 arrange gadgets for steering, VPN, and exchanging. We utilized VMware and Microsoft operating system servers with a SQL server as backend database to mimic cloud-based SaaS applications. DDoS assault reproductions were performed on the three-level engineering to check the patterns for system and application-level

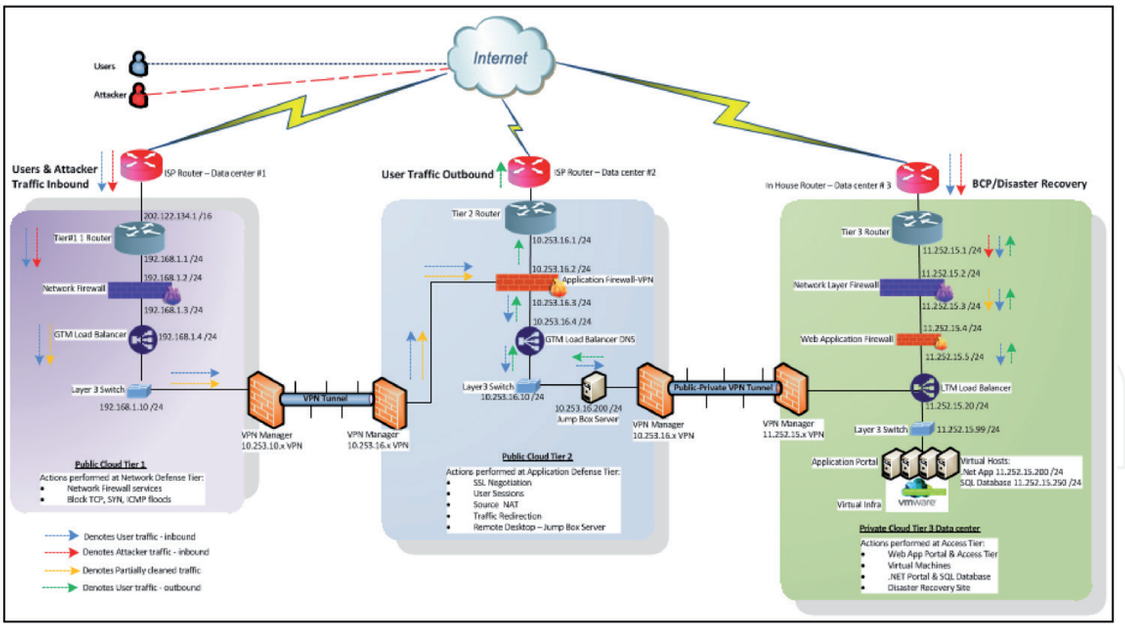


Figure 10.
Proposed three-tier architecture.

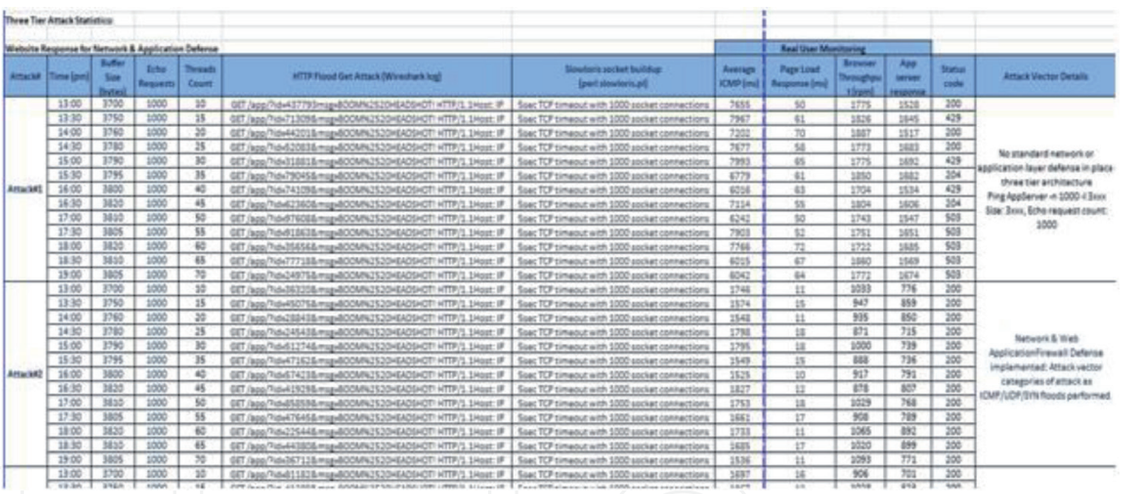


Figure 11.
Three-tier logs (network attack).

outcomes after the assaults. ICMP flooding was performed with 1000 reverberation demands each with expanding support size (3600–3800 bytes) with each assault. They made the objective server to react and process the ICMP demands, taking cost of CPU assets and at last square substantial solicitations. Application-level assaults were finished utilizing HTTP Flood GET assault with expanding string check and 1200 reverberation demands utilizing "GET/application/?id=479673msg=BOOM %2520HEADSHOT! HTTP/1.1Host: IP" and moderate attachment development mimicking moderate HTTP assault utilizing perl with logs taken from Wireshark.

Device logs gathered for each attack are illustrated in **Figure 11**.

6.3 Comparing single- and three-tier architectures

DDoS attacks were performed on single-tier and the proposed three-tier infrastructure architecture and results gathered for real user monitoring parameters during the network attacks (**Figure 12**).

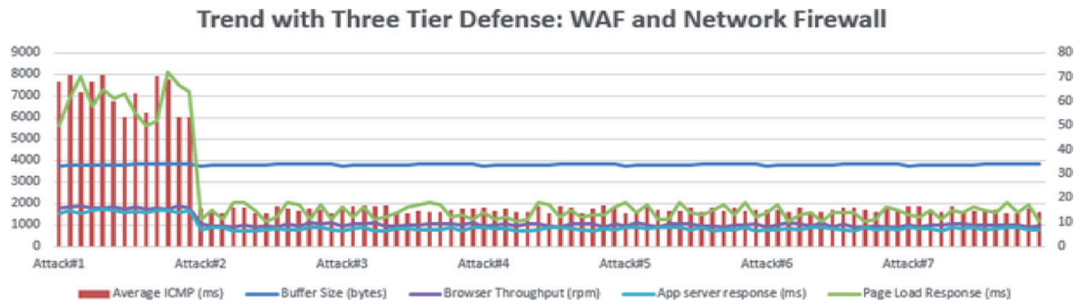


Figure 12.
Network and web defense trends.

					Real User Monitoring					
Attack#	Time (pm)	Buffer Size (bytes)	Echo Requests	Target Server IP	Average ICMP (ms)	Page Load Response (ms)	Browser Throughput (rpm)	App server response (ms)	Status code	Attack Vector Details
Attack#1	13:00	3700	1000	11.252.15.100	6545	45	1800	1636	200	No standard network layer defense in place - single tier architecture Ping AppServer -n 1000 -l 3xxx Size: 3xxx, Echo request count: 1000
	13:30	3750	1000	11.252.15.100	6670	54	1856	1496	429	
	14:00	3760	1000	11.252.15.100	6575	55	1727	1624	200	
	14:30	3780	1000	11.252.15.100	6791	46	1627	1784	200	
	15:00	3790	1000	11.252.15.100	6583	41	1606	1713	429	
	15:30	3795	1000	11.252.15.100	6745	55	1806	1686	204	
	16:00	3800	1000	11.252.15.100	6790	50	1651	1488	429	
	16:30	3820	1000	11.252.15.100	6794	54	1761	1795	204	
	17:00	3810	1000	11.252.15.100	6690	47	1800	1833	503	
	17:30	3805	1000	11.252.15.100	6512	42	1849	1565	503	
	18:00	3820	1000	11.252.15.100	6692	48	1835	1726	503	
	18:30	3810	1000	11.252.15.100	6589	50	1635	1570	503	
	19:00	3805	1000	11.252.15.100	6995	50	1839	1663	503	
Attack#2	13:00	3750	1000	11.252.15.100	2795	30	1325	1297	200	Network Firewall Defense implemented: Attack vector categories of attack as ICMP/UDP/SYN floods
	13:30	3745	1000	11.252.15.100	2911	32	1327	1243	200	
	14:00	3760	1000	11.252.15.100	2805	29	1208	1298	200	
	14:30	3780	1000	11.252.15.100	2963	30	1306	1043	200	
	15:00	3770	1000	11.252.15.100	2746	29	1235	1097	200	
	15:30	3783	1000	11.252.15.100	2933	32	1245	1213	200	
	16:00	3780	1000	11.252.15.100	2988	28	1219	1228	200	

Figure 13.
Single-tier attack parameters.

			Real User Monitoring					
Date	Time (pm)	Threads Count	Average ICMP (ms)	Page Load Response (ms)	Browser Throughput (rpm)	App server response (ms)	Attack detected	ICMP Food Attack
Attack#1	16:00	40	6544	40	1651	1728	GET /HTTP/1.1 404 204	layer defense in place - single tier architecture
	16:30	45	6511	51	1501	1566	GET /HTTP/1.1 404 204	
	17:00	50	6576	37	1555	1728	GET /HTTP/1.1 404 204	
	17:30	55	6525	45	1604	1598	GET /HTTP/1.1 404 204	
	18:00	60	6577	35	1669	1696	GET /HTTP/1.1 404 204	
	18:30	65	6567	38	1594	1575	GET /HTTP/1.1 404 204	
	19:00	70	6402	36	1674	1529	GET /HTTP/1.1 404 204	
Attack#2	13:00	10	4239	24	1132	1053	GET /HTTP/1.1 404 204	WAF Defense implemented: Application layer attack vectors as HTTP attack, Slowloris attack performed
	13:30	15	4113	29	1182	1066	GET /HTTP/1.1 404 204	
	14:00	20	4184	30	1140	1200	GET /HTTP/1.1 404 204	
	14:30	25	4112	20	1219	1000	GET /HTTP/1.1 404 204	
	15:00	30	4233	22	1221	1184	GET /HTTP/1.1 404 204	
	15:30	35	3938	27	1106	1127	GET /HTTP/1.1 404 204	
	16:00	40	4274	25	1258	1012	GET /HTTP/1.1 404 204	
	16:30	45	4269	25	1208	1000	GET /HTTP/1.1 404 204	
	17:00	50	4198	20	1256	1170	GET /HTTP/1.1 404 204	
	17:30	55	4167	26	1204	1176	GET /HTTP/1.1 404 204	
	18:00	60	4318	29	1244	1096	GET /HTTP/1.1 404 204	
	18:30	65	3951	29	1131	1002	GET /HTTP/1.1 404 204	
	19:00	70	3947	27	1203	1022	GET /HTTP/1.1 404 204	
	13:00	10	4059	28	1260	1038	GET /HTTP/1.1 404 204	
	13:30	15	4169	30	1187	1047	GET /HTTP/1.1 404 204	

Figure 14.
Single-tier application attack logs.

6.4 Single-tier logs and data analysis

The below data and graphs illustrate the network firewall and application layer logs and graphs for the DDoS attack performed on single-tier data center architecture in order to determine the resilience for handling DDoS attacks. In **Figure 13** network

firewall defense is implemented after attack#2 with ICMP, page load, browser throughput, and application response as the key values.

Figure 14 illustrates real user monitoring values obtained during an application layer attack on single-tier network infrastructure in which application firewall defense is implemented after attack#2 with ICMP, page load, browser throughput, and application response key values.

Results of single-tier architecture attacks obtained before and during the DDoS attack are presented in **Figure 15**. This has the average ICMP, browser throughput, page load response, and application server response.

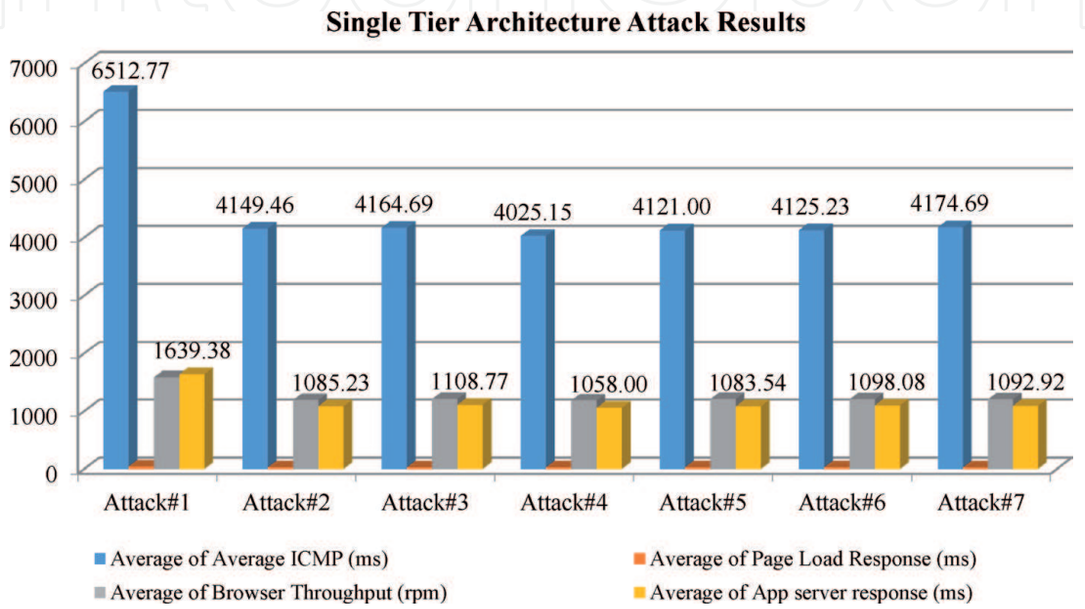


Figure 15.
Single-tier network attack parameters.

					Real User Monitoring					
Attack#	Time (pm)	Buffer Size (bytes)	Echo Requests	Threads Count	Average ICMP (ms)	Page Load Response (ms)	Browser Throughput (rpm)	App server response	Status code	Attack Vector Details
Attack#1	13:00	3700	1000	10	7655	50	1775	1528	200	No standard network or application layer defense in plac three tier architecture Ping AppServer -n 1000 -l 3xxx Size: 3xxx, Echo request count: 1000
	13:30	3750	1000	15	7967	61	1826	1645	429	
	14:00	3760	1000	20	7202	70	1887	1517	200	
	14:30	3780	1000	25	7677	58	1773	1683	200	
	15:00	3790	1000	30	7993	65	1775	1692	429	
	15:30	3795	1000	35	6779	61	1850	1682	204	
	16:00	3800	1000	40	6016	63	1704	1534	429	
	16:30	3820	1000	45	7114	55	1804	1606	204	
	17:00	3810	1000	50	6242	50	1743	1547	503	
	17:30	3805	1000	55	7903	52	1751	1651	503	
	18:00	3820	1000	60	7766	72	1722	1685	503	
	18:30	3810	1000	65	6015	67	1860	1569	503	
	19:00	3805	1000	70	6042	64	1772	1674	503	
Attack#2	13:00	3700	1000	10	1746	11	1033	776	200	Network & Web ApplicationFirewall Defense implemented: Attack vector categories of attack as ICMP/UDP/SYN floods performed
	13:30	3750	1000	15	1574	15	947	859	200	
	14:00	3760	1000	20	1548	11	935	850	200	
	14:30	3780	1000	25	1798	18	871	715	200	
	15:00	3790	1000	30	1795	18	1000	739	200	
	15:30	3795	1000	35	1549	15	888	736	200	
	16:00	3800	1000	40	1525	10	917	791	200	
	16:30	3820	1000	45	1827	12	878	807	200	
	17:00	3810	1000	50	1753	18	1029	768	200	
	17:30	3805	1000	55	1661	17	908	789	200	
	18:00	3820	1000	60	1733	11	1065	892	200	
	18:30	3810	1000	65	1685	17	1020	899	200	
	19:00	3805	1000	70	1536	11	1093	771	200	
	13:00	3700	1000	10	1697	16	906	701	200	
	13:30	3750	1000	15	1867	12	1028	823	200	
	14:00	3760	1000	20	1894	16	1016	857	200	
	14:30	3780	1000	25	1825	11	1093	710	200	

Figure 16.
Three-tier attack logs.

6.5 Three-tier logs and data analysis

DDoS attacks are performed on the designed network architectures and network and application attack results obtained before and after attack scenarios. Network attacks like ICMP flood are done with 1000 ICMP echo requests with each increasing the attack buffer size from 3700 to 3805 bytes. Application attack like HTTP Flood attack is done by increasing the thread count by "*GET / app/?id = 437793 msg = BOOM%2520HEADSHOT! HTTP/1.1 Host: IP*" and slow socket buildup simulating slow web attacks by the use of perl. The logs and Data gathered are gathered from the network firewall; for each attack is displayed in **Figure 16**.

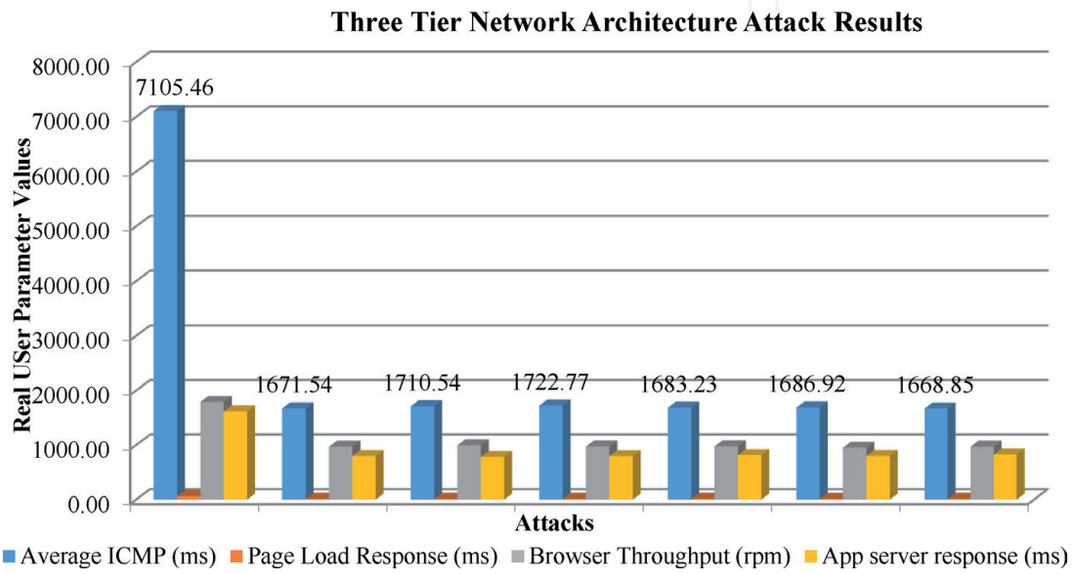


Figure 17.
Three-tier architecture attack parameter results.

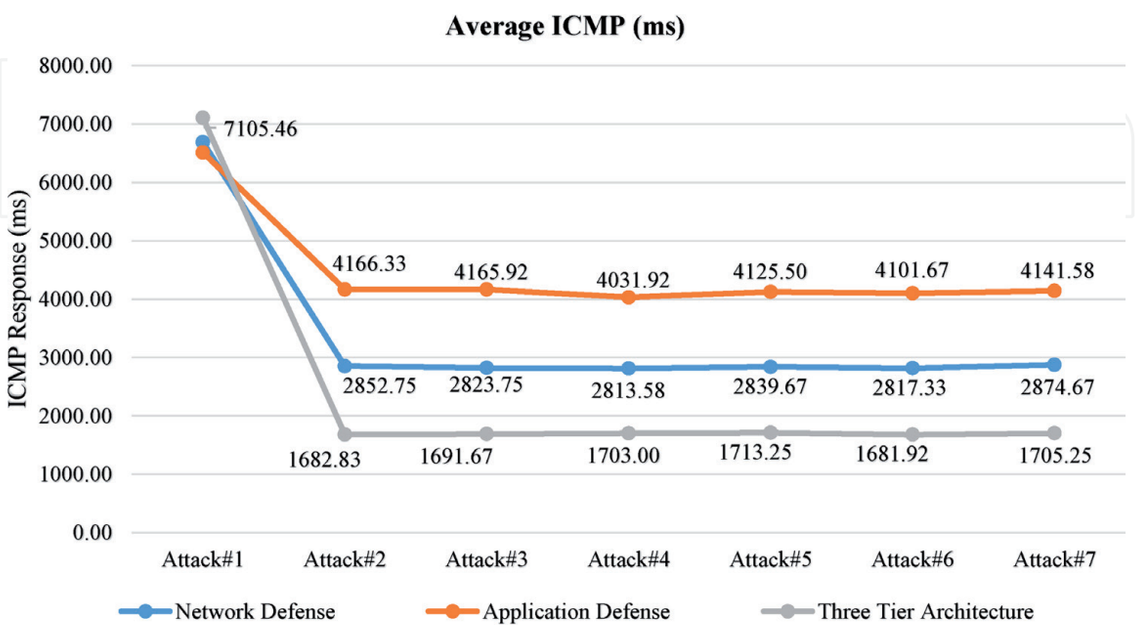


Figure 18.
Real user monitoring for ICMP (single- and three-tier).

Results of three-tier architecture attacks obtained before and during the DDoS attack are presented in **Figure 17**. This has the average ICMP, browser throughput, page load response, and application server response.

The graph in **Figure 18** presents the results of three-tier architecture attacks obtained before and during DDoS attack for ICMP response.

Results of three-tier architecture attacks obtained before and during DDoS attack for page load response is presented in **Figure 19**.

Results of three-tier architecture attacks obtained before and during DDoS attack for browser throughput are presented in **Figure 20**.

Results of three-tier architecture attacks obtained before and during DDoS attack for application server response is presented in **Figure 21**.

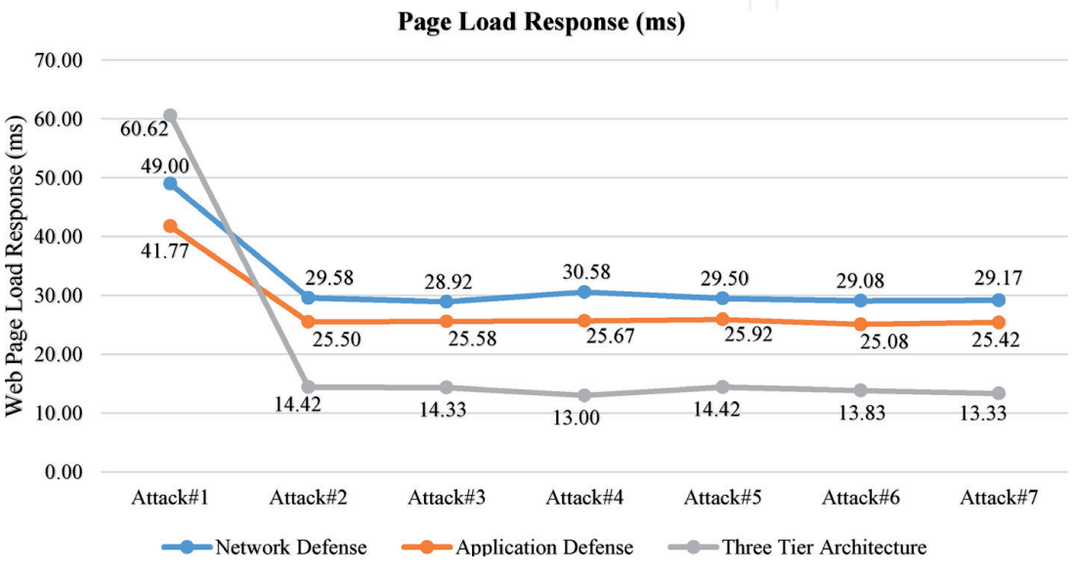


Figure 19.
Real user monitoring for page load response (single- and three-tier).

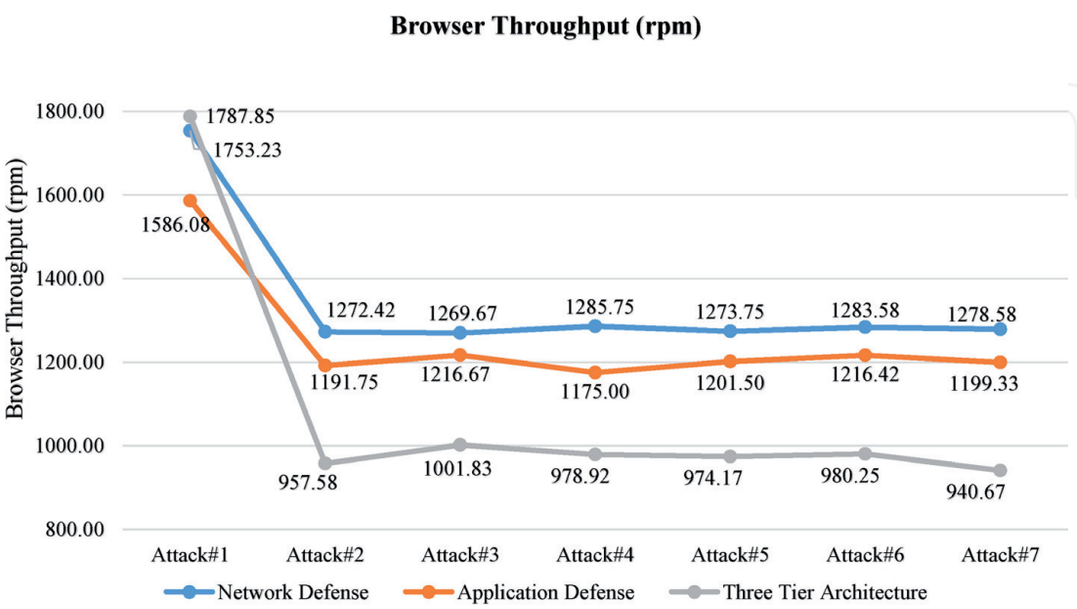


Figure 20.
Real user monitoring for browser throughput (single- and three-tier).

The below graph displays the availability trend metrics obtained after performing the DoS attacks on the two architectures for network and application layer design (**Figure 22**).

6.6 Result analysis

After analyzing the infrastructure, we now focus on what the cloud infrastructure has to offer for implementation (**Figures 23–25**).

1. Firewall → Prevent threats entering the network from outside.

2. Active directory → Authentication, authorization, and group policies for access management.

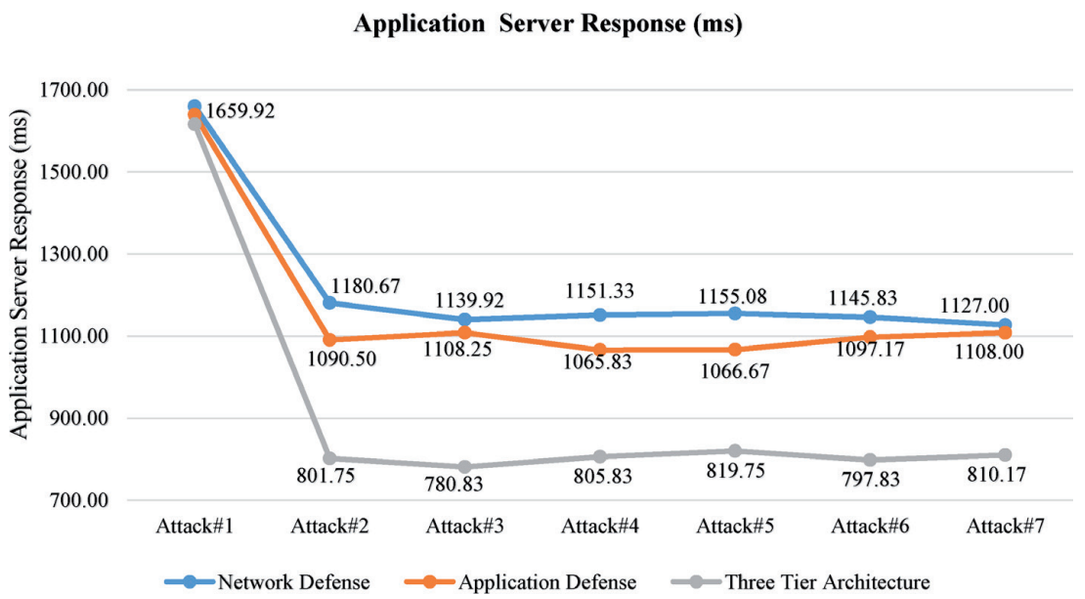


Figure 21.
Real user monitoring for application server responses.

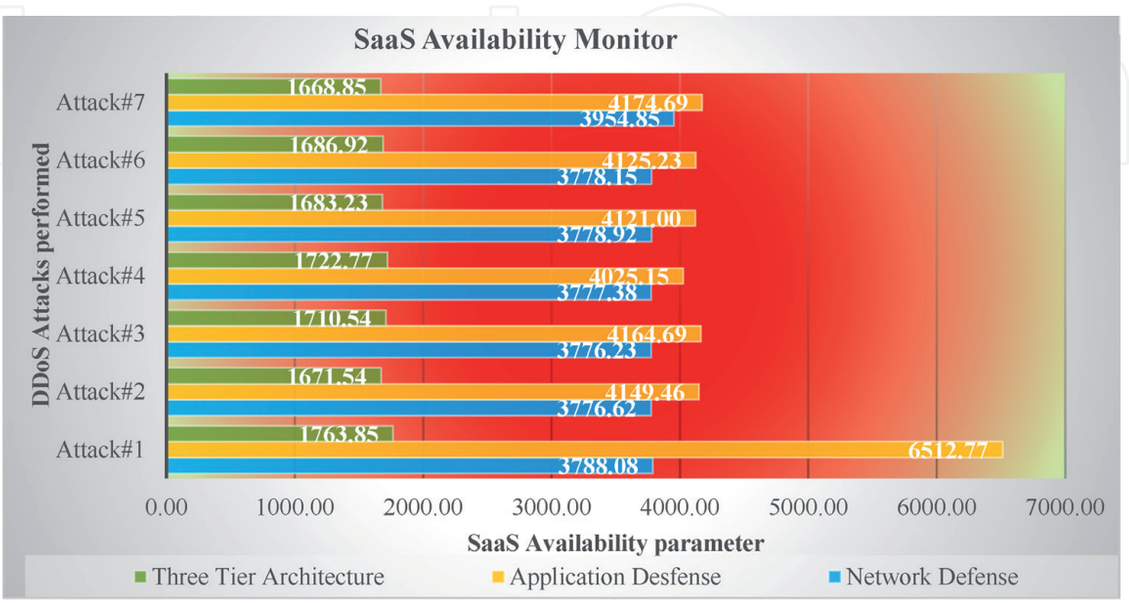


Figure 22.
SaaS availability monitor.

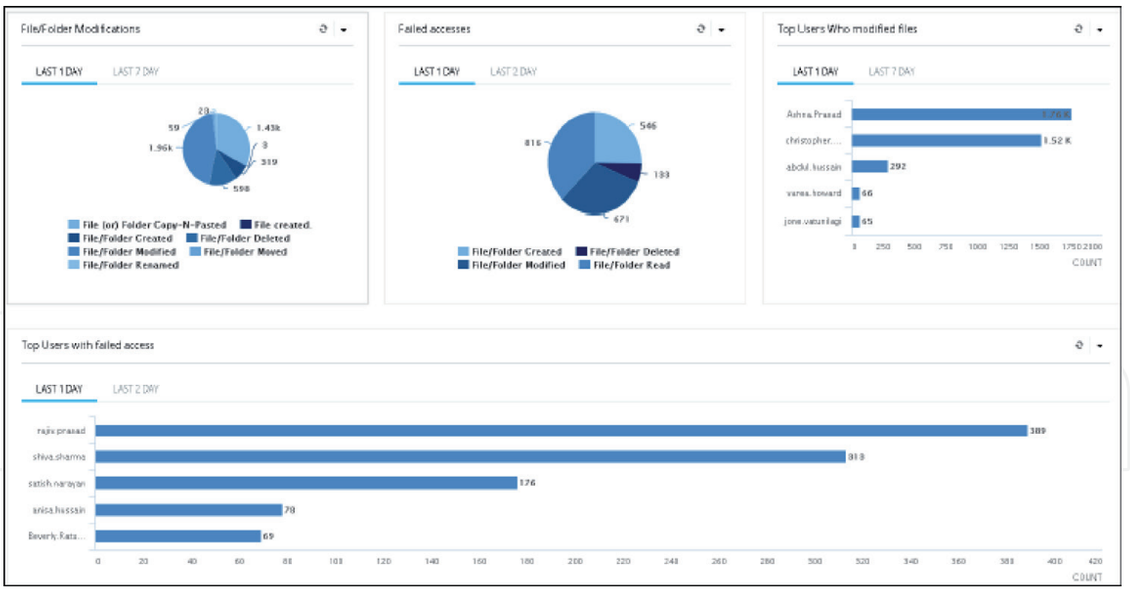


Figure 23.
Populated report for file server access activity on cloud-based premises.

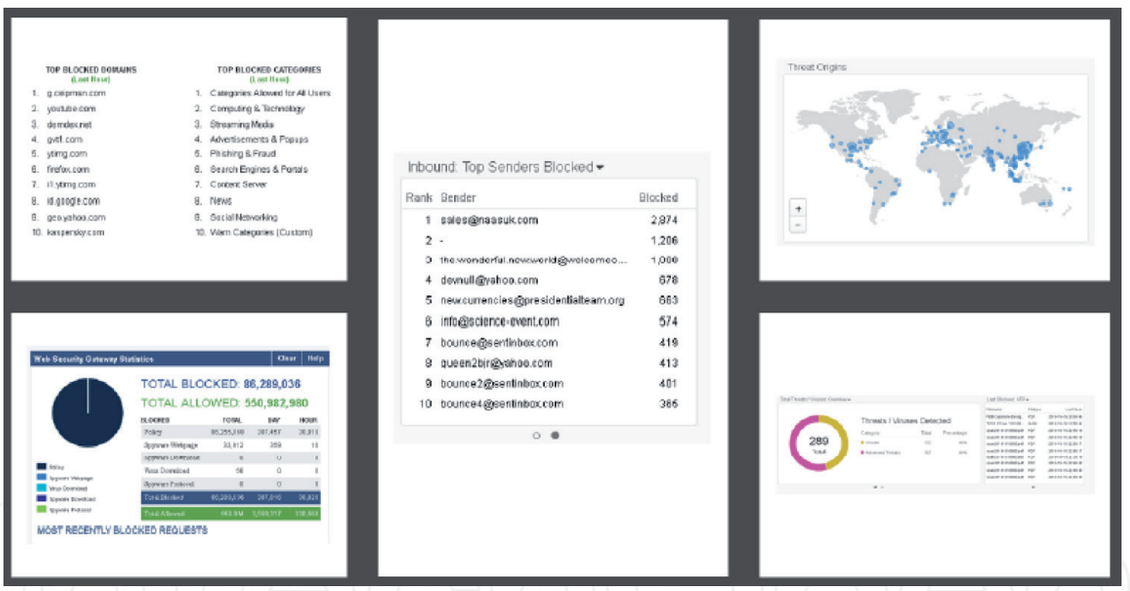


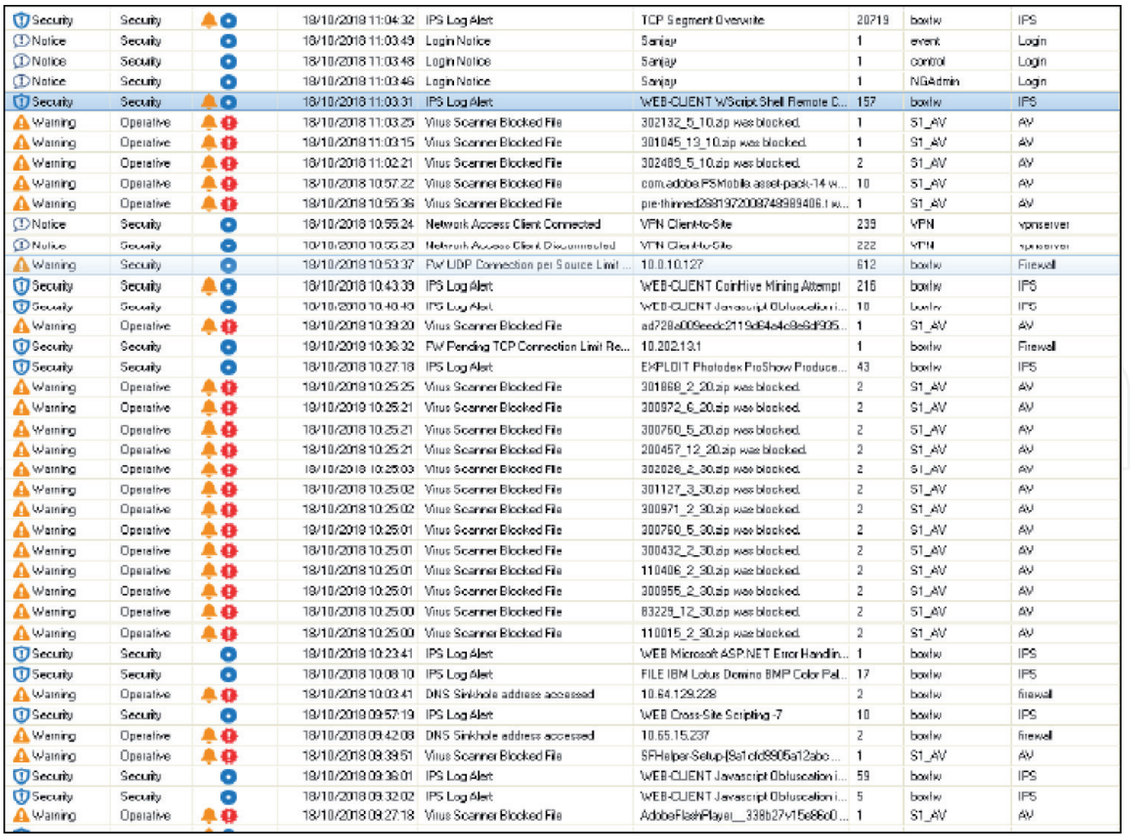
Figure 24.
Threats blocked based on the requests coming into the cloud system.

3. Web application firewall → Protects web servers and manages the incoming and outgoing requests.

4. Web Security Gateway → Web proxy filters manage and monitor websites visited by users in network.

5. Email security → Scans, monitors, and protects emails incoming and outgoing.

Web application firewall (WAF) prevents DDoS attack including SQL injection and XSS attacks to name a few. This is integrated with the implementation as shown in **Figure 26**.



Security	Security	18/10/2018 11:04:32	IPS Log Alert	TCP Segment Overwrite	20719	boxlw	IPS
Notice	Security	18/10/2018 11:03:49	Login Notice	Sanjay	1	event	Login
Notice	Security	18/10/2018 11:03:48	Login Notice	Sanjay	1	control	Login
Notice	Security	18/10/2018 11:03:46	Login Notice	Sanjay	1	NGAdmin	Login
Security	Security	18/10/2018 11:03:31	IPS Log Alert	WEB-CLIENT VScript Shell Remote C...	157	boxlw	IPS
Warning	Operative	18/10/2018 11:03:25	Virus Scanner Blocked File	302132_5_10.zip was blocked.	1	S1_AV	AV
Warning	Operative	18/10/2018 11:03:15	Virus Scanner Blocked File	301045_13_10.zip was blocked.	1	S1_AV	AV
Warning	Operative	18/10/2018 11:02:21	Virus Scanner Blocked File	302489_5_10.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:57:22	Virus Scanner Blocked File	com.adobe.PSMobile.asset-pack-14.w...	10	S1_AV	AV
Warning	Operative	18/10/2018 10:55:36	Virus Scanner Blocked File	pre-thinned2881972008748989406.1.w...	1	S1_AV	AV
Notice	Security	18/10/2018 10:55:24	Network Access Client Connected	VPN Client-to-Site	239	VPN	vpnserver
Notice	Security	18/10/2018 10:55:23	Network Access Client Disconnected	VPN Client-to-Site	222	VPN	vpnserver
Warning	Security	18/10/2018 10:53:37	FW UDP Connection per Source Limit ...	10.0.10.127	612	boxlw	Firewall
Security	Security	18/10/2018 10:43:39	IPS Log Alert	WEB-CLIENT CoinHive Mining Attempt	216	boxlw	IPS
Security	Security	18/10/2018 10:40:49	IPS Log Alert	WEB-CLIENT Javascript Obfuscation i...	10	boxlw	IPS
Warning	Operative	18/10/2018 10:39:20	Virus Scanner Blocked File	ad728a009eedc2119d84e4c9e9df935...	1	S1_AV	AV
Security	Security	18/10/2018 10:38:32	FW Pending TCP Connection Limit Re...	10.202.13.1	1	boxlw	Firewall
Security	Security	18/10/2018 10:27:18	IPS Log Alert	EXPLOIT Photodex ProShow Produce...	43	boxlw	IPS
Warning	Operative	18/10/2018 10:25:25	Virus Scanner Blocked File	301869_2_20.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:21	Virus Scanner Blocked File	300972_6_20.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:21	Virus Scanner Blocked File	300760_5_20.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:21	Virus Scanner Blocked File	200457_12_20.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:03	Virus Scanner Blocked File	302026_2_30.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:02	Virus Scanner Blocked File	301127_3_30.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:02	Virus Scanner Blocked File	300971_2_30.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:01	Virus Scanner Blocked File	300760_5_30.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:01	Virus Scanner Blocked File	300432_2_30.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:01	Virus Scanner Blocked File	110406_2_30.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:01	Virus Scanner Blocked File	300955_2_30.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:00	Virus Scanner Blocked File	83229_12_30.zip was blocked.	2	S1_AV	AV
Warning	Operative	18/10/2018 10:25:00	Virus Scanner Blocked File	110015_2_30.zip was blocked.	2	S1_AV	AV
Security	Security	18/10/2018 10:23:41	IPS Log Alert	WEB Microsoft ASP.NET Error Handlin...	1	boxlw	IPS
Security	Security	18/10/2018 10:08:10	IPS Log Alert	FILE IBM Lotus Domino BMP Color Pal...	17	boxlw	IPS
Warning	Operative	18/10/2018 10:03:41	DNS Sinkhole address accessed	10.64.129.228	2	boxlw	firewall
Security	Security	18/10/2018 09:57:19	IPS Log Alert	WEB Cross-Site Scripting -7	10	boxlw	IPS
Warning	Operative	18/10/2018 09:42:08	DNS Sinkhole address accessed	10.65.15.237	2	boxlw	firewall
Warning	Operative	18/10/2018 09:39:51	Virus Scanner Blocked File	SFHelper-Setup-[8a1cfc9905a12abc...	1	S1_AV	AV
Security	Security	18/10/2018 09:39:01	IPS Log Alert	WEB-CLIENT Javascript Obfuscation i...	59	boxlw	IPS
Security	Security	18/10/2018 09:32:02	IPS Log Alert	WEB-CLIENT Javascript Obfuscation i...	5	boxlw	IPS
Warning	Operative	18/10/2018 09:27:18	Virus Scanner Blocked File	AdobeFlashPlayer__338b27e15e86c0...	1	S1_AV	AV

Figure 25.
Logs displaying the threat level with its warning on a cloud-based setup.

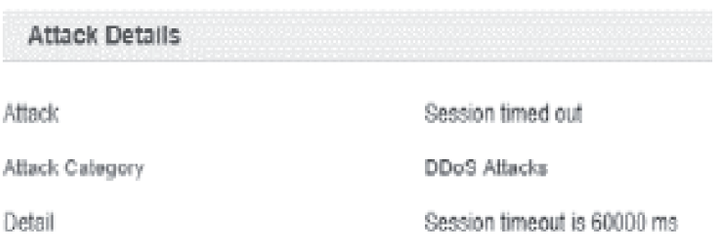


Figure 26.
Shows how an attack gets categorized in the WAF.

7. Conclusion

According to our findings and our recommendations having a private cloud, setup is best suited for the larger organizations due to the limitations of going on public cloud infrastructure in terms of bandwidth, data confidentiality, cost of Internet, and cost of its recommended with requirements for infrastructure itself on a public cloud. Setting up a private cloud helps organizations to mitigate risk with confidence and keep 100% control changes to the platform. However, not forgetting the security risks associated with a private cloud infrastructure in areas such as web application firewalls, web security gateways, main gateway firewall, end point security protection, etc., it is essential to have these security appliances implemented with the infrastructure to maintain and protect the cloud environment from outside threats.

Author details

Akashdeep Bhardwaj[1*] and Sam Goundar[2]

1 University of Petroleum and Energy Studies, Dehradun, India

2 The University of the South Pacific, Fiji

*Address all correspondence to: bhrdwh@yahoo.com

IntechOpen

References

[1] Rubóczki ES, Rajnai Z. Moving towards cloud security. Interdisciplinary Description of Complex Systems: INDECS. 31 Jan 2015;**13**(1):9-14

[2] Singh SK, Singh DK. Cloud computing: Security issues and challenges. International Journal of Advances in Engineering & Technology. Jun 2017;**10**(3):338

[3] Kajiyama T, Jennex M, Addo T. To cloud or not to cloud: How risks and threats are affecting cloud adoption decisions. Information & Computer Security. 13 Nov 2017

[4] Bunkar RK, Rai PK. Study on security model in cloud computing. International Journal of Advanced Research in Computer Science. 1 July 2017;**8**(7)

[5] Saeed MY, Khan MN. Data protection techniques for building trust in cloud computing. International Journal of Modern Education & Computer Science. August 2015;**7**(8)

[6] Khajehei K. Role of identity management systems in cloud computing privacy. International Journal of Education and Management Engineering. 2017;**7**(3):25-34

[7] Lazarova V. Managing user access to cloud services by company administrators. TEM Journal. 2016;**5**(3):289-293

[8] Habiba UM. Cloud identity management security issues & solutions: A taxonomy. Complex Adaptive Systems Modeling. 2014:1-37

[9] Shaik K, Narayana Rao TV. Implementation of encryption algorithm for data security in cloud computing. International Journal of Advanced Research in Computer Science. 15 March 2017;**8**(3)

[10] Das N, Sarkar T. Securing cloud from cloud drain. arXiv preprint arXiv:1407.6482. 24 July 2014

[11] Dahiya N, Rani S. Implementing multilevel data security in cloud computing. International Journal of Advanced Research in Computer Science. 1 September 2017;**8**(8)

[12] Xuan S, Yang W, Dong H, Zhang J. Performance evaluation model for application layer firewalls. PLoS One. November 2016;**11**(11):e0167280

[13] Fernandez EB, Monge R, Hashizume K. Building a security reference architecture for cloud systems. Requirements Engineering. 2016;**21**(2):225-249

[14] Alosaimi W, Zak M, Al-Begain K, Alroobaea R, Masud M. Economic denial of sustainability attacks mitigation in the cloud. International Journal of Communication Networks and Information Security. Dec 2017;**9**(3):420-431

[15] He J, Dong M, Ota K, Fan M, Wang G. NetSecCC: A scalable and fault-tolerant architecture for cloud computing security. Peer-to-Peer Networking and Applications. 2016;**9**(1):67-81

[16] Kimbrel JE. Barracuda Launches Suite of Cloud Services for Added Layers of Protection in Office 365 Environments. United States, New York: PR Newswire Association LLC; 2016

[17] Kamla RZ, Yahiya T, Mustafa NB. An implementation of software routing for building a private cloud. International Journal of Computer Network & Information Security. 2018;**10**(3)

[18] Raphiri TV, Dlamini MT, Venter H. Strong authentication: Closing the front door to prevent unauthorised access to

cloud resources. In: ICCWS 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security: ICCWS2015 Academic Conferences Limited; 24 February 2015. p. 252

[19] Potluri S. Primary methods to address the data security problems in cloud computing. IUP Journal of Computer Sciences. 2016;**10**(1/2):18

[20] Bhadauria R, Chaki R, Chaki N, Sanyal S. Security issues in cloud computing. Acta Technica Corvininesis-Bulletin of Engineering. 2014;**7**(4)

[21] Ramluckan T, van Niekerk B. Security requirements for cloud computing in crisis management. Journal of Information Warfare. 2014;**13**(1):33-46

[22] Al Haddad Z, Hanoune M, Mamouni A. A collaborative network intrusion detection system (C-NIDS) in cloud computing. International Journal of Communication Networks and Information Security. 2016;**8**(3):130

[23] Keegan Nathan S-YJ. A survey of cloud-based network. Human-centric Computing and Information Sciences. 2016

[24] Agarkhed J, Ashalatha R. Security and privacy for data storage service scheme in cloud computing. International Journal of Information Engineering and Electronic Business. 2017;**9**(4):7