Cloud based "Online Art Gallery" using PaaS with its Security, Privacy, and Compliance Challenges

Shreya Sharma
Assistant Professor
Department of CSE
RCEW Jaipur, India

Manoj Kumar Sah
Assistant Professor
Department of CSE
NIT Jalandhar, India

Alok Kumar Pani
Assistant Professor
Department of CSE
Christ University, Bangalore

ABSTRACT
The paper comprises of deploying whole web application and its related services in cloud platform using PaaS, here major concern is to secure the data and maintain the data flow in a streamlined manner. Methodology adopted here is using virtualization technique and utilizing resource developing platform as a service platform and it is used as a service.

Online art gallery is the search engine friendly content management system in which user and admin interact with each other. Here the application is being deployed in Amazon AWS and PaaS used is Appfog which is build of cloud foundry, the open platform as a service and the database used is MySQL.

Keywords
Cloud Computing, Appfog, Wordpress, Amazon Web Services, Cloudnary, Cloudflare;

1. INTRODUCTION
Applications that share photos or support critical operations of business require rapid access to flexible low cost IT resources. Cloud computing is a scenario of on demand delivery of IT resources with pay as you go pricing. Cloud Computing offers following benefits they are as follows [1].

a. No Upfront management
Building an on premise infrastructure is slow and expensive we need expensive hardware's which are to be ordered, paid for, installed and configured which is required to be done long before we actually need them , with cloud computing we pay as we need resources in accordance to our requirement.

b. Low Ongoing cost
Massive economy of scaling and efficiency improvement allow a continually lowering of prices It derives down upfront and ongoing IT labor cost and gives an access to the fully distributed and featured services to the customer.

c. Flexible Capacity
It eliminates the guessing of the infrastructure needs .Decisions of capacity prior to deploying an application seems to be unpredictable as sometime we may require more or sometimes we may lack resources so it offers capacity as we require in accordance to the application.

d. Speed and Agility
With traditional architecture it require a weeks to get server procured, delivered and running. With cloud computing, resources can be used on demand hence increasing speed of deploying and developing applications.

e. Apps not Ops
Cloud computing allows to focus over the application by providing complete infrastructure requirements.

f. Global reach
For large potential users across the globe it provide an adequate and efficient services which is impossible with traditional infrastructure which employ many organizations to focus over a specific infrastructure for there accessibility.

1.1 Definition of Cloud computing
Cloud computing is a mechanism which describes many variety of computing concepts that include:

a. Software as a service (SaaS)
These are on demand software which is priced on demand based; here cloud providers provide complete application software to the customers according to their requirements. Eg Google Apps, Microsoft office 365

b. Platform as a service(PaaS)
Cloud providers delivers complete computing platform including operating systems, programming language execution environment and web server. Eg: Cloud foundry, Google App engine.

c. Infrastructure as a service (IaaS)
Cloud providers provide physical or the virtual machines to the customer on pay as peruse bases. Eg: Amazon EC2, Windows azure, Google compute engine.

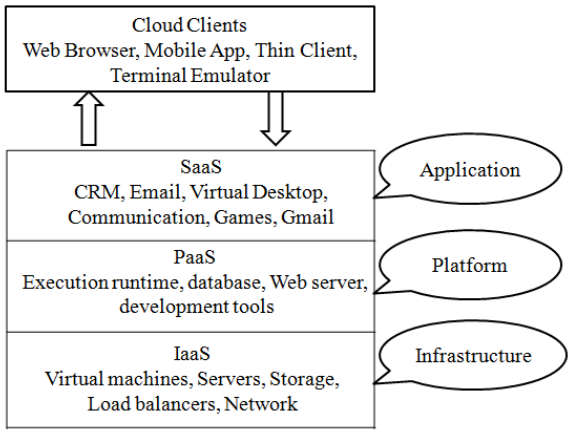

Fig 1 : Cloud computing service model

2. APPFOG (PaaS)
Appfog is a simple cloud platform for deploying web applications it is based on cloud foundry the open source platform as a service project for php, Ruby, Node.js and java. Working with Appfog involves following Steps [2].

Step 1: Sign up at www.appfog.com

Step 2: Select the application or framework

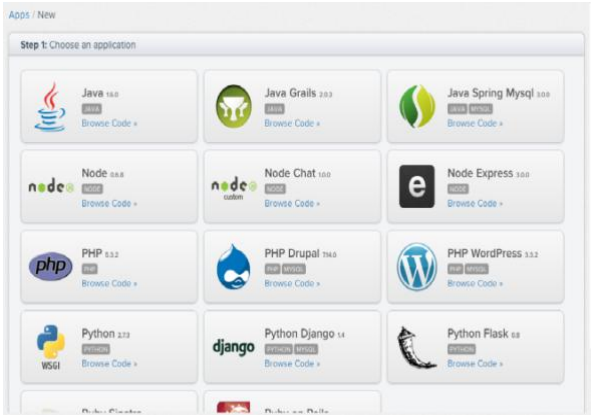

Fig 2 : Appfog jumpstart to select an application

Step 3: Choose an infrastructure: It allows us to host application in the infrastructure as required.

Fig 3 : Appfog Infrastructure panel

Step 4: Choose a sub domain: We can select a sub domain in accordance to our need.

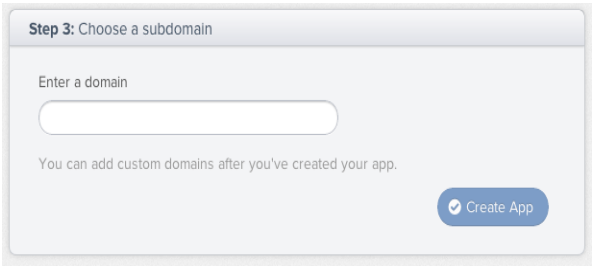

Fig 4 : Appfog sub domain selection

Step 5: It will take a few minutes and web application will we deployed over the Appfog we can access the application by clicking visit live site.

2.1 Appfog provides following functionalities

a. Services

It provides support to various services like Mongo DB (The scalable, open source document based database), My SQL (The open source relational database), Redis (The open key value data structure server), Rabbit MQ (Reliable and portable messaging for applications), vFabric Postgres (Relational database based on Postgre SQL).etc

b. Languages

Appfog supports many different languages like Php, Java, Ruby, and Node. Js.

c. Tunneling

Interacting services using AF tunnel command .This uses an app called Caldecott is a proxy of TCP over Https, it creates a tunnel that connects a port on your local computer to the service Appfog. The command uploads the app, sets up tunneling and offers to start a standard client on the computer.

d. Add-ons

Appfog provides additional functionality to the web application by partnering with various third party services, which are committed to provide a time relevant and efficient services to the clients

2.2 Appfog has following add-ons:

a. Searchify

It provides hosted full text search, allows developers to easily add search to their applications without need of configuring the whole search infrastructure. Searchify offers true real time search, so documents added are so easily and immediately searched.

b. Iron worker

It's a product that enables separation of the elements into specialized and resilient chunks. Each worker is intended to be individual project, operating independently. By using workers an easily manageable application can be easily created that operates under worst case scenario.

c. Cloud mailing

It provides a functionality of receiving email and forwarding them to the application by performing a POST to a specific page.

d. Blitz

As it is unpredictable to guess the number of resources required for any applications, The best way to determine what services are needed is by simulating load. Blitz provides user to test load on apps quickly and rapidly.

e. Cloud nary

It streamlines the applications image manipulation needs. It automates image uploading, resizing, cropping, optimizing, sprite generation and much more. It is build using modern web development framework and leverages Amazon web service cloud solutions.

f. Memcachier

It's an implementation of Memcache which is a free and open source, distributed memory object caching system which intends to speed up dynamic web applications by alleviating database loads.

g. Nexmo

It's a cloud based API which lets user send and receives a high volume of messages at whole sale rates.

3. WORDPRESS (CMS)

A content management system is a computer program which allows editing, modifying and publishing of the content as well as maintenance from central interface [5]. Wordpress is a blogging tool free available over internet and a content management system based on php and MySQL, with thousands of plug-in, widgets, themes [3].

a. Themes

Word press users can install and customize theme according to their needs

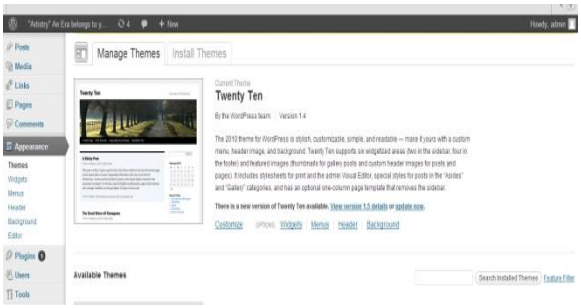

Fig 5 : Word press Themes

b. Widgets

These are small modules offering drag and drop sidebar and content placement is done through implementation of plug-in extended abilities [3].

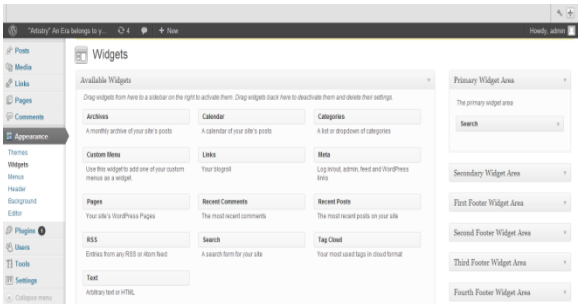

Fig 6 : Word press widgets

c. Plug-in

They allow users to extend the abilities of the web applications beyond its core architecture. Word press have thousands of plug-in which provide customization and added features in order to enhance the web application in better way this may also include Search engine optimization (SEO) ,enhancers to content displaying features such as widgets and

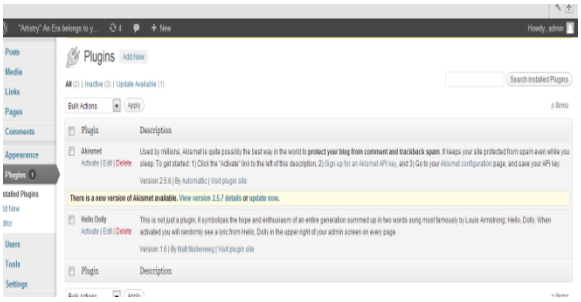

Fig 7 : Word press plug-in

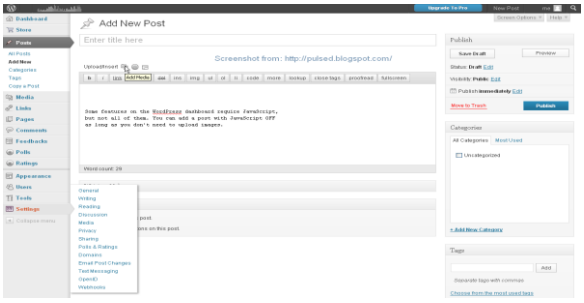

Fig 8 : Word press dashboard

4. AMAZON WEB SERVICES

Amazon web services provides an efficient, flexible, cost effective, easy accessible cloud computing platform which is suitable for user in accordance to their requirements [4]

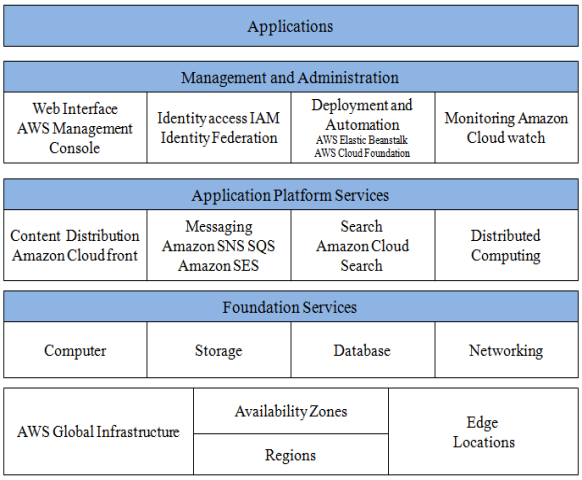

Fig 9 : Services offered by AWS

It's easy to use Amazon services via internet as it allows user to pay as peruse according to the requirement they can use maximal and minimal amount of resources. Amazon web services allow users to have IT resources on lease, thereby becoming infrastructure tenants rather than owners.

With Amazon web services the user pay only as they use .Here we have used Amazon web services in our application and in the context below complete description of the services running behind the applications is done.

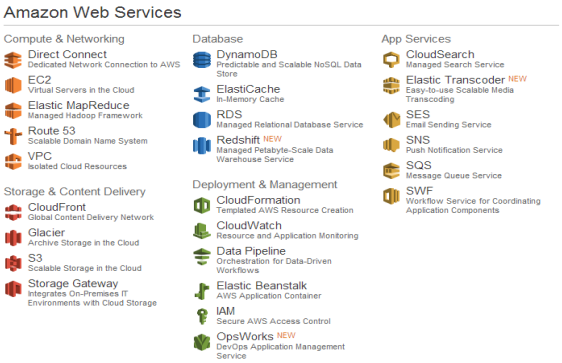

Fig 10 : Amazon Web Services

As given in above figure (Fig-8) we can see block representation of the services offered to the applications by Amazon which include

4.1 Management and Administration

a. Web Interface

AWS management console provide an user interface for the services

b. Identity and Access

IAM i.e. AWS Identity and Access management is a web service that enables managing users and user's access permissions .The service provide an aid to the organizations which have multiple user scenario. Without IAM the organizations must either create multiple AWS accounts each with different billing and subscription, or employees were required to share the security credential with one another,

without IAM there is no control over the task of any particular user and what a system can do and how many resources to be used.

Thus IAM provides mechanisms where multiple users can access AWS account with different security credentials all are controlled by and billed to a common account. In this a user is allowed to do what is actually required as a part of their job.

c. Deployment and Automation

i. AWS Cloud formation

It provides the developers and system administrators an easy way to create, manage, update, and provisioning of the AWS resources in an orderly and predictable manner.
It provides sample templates or user can create their own customized one to describe AWS resources and any associated dependencies or run time parameters.

Once an application is deployed it can be modified and updated very easily using cloud formation. A template is deployed using AWS management console [5].

ii. AWS Elastic Beanstalk

Using AWS Elastic Beanstalk user can quickly deploy the applications and mange them efficiently without concerning the infrastructure running beyond the applications. Here we simply need to upload the application and the Beanstalk handles capacity provisioning, load balancing, scaling, application health monitoring. It uses highly scalable and reliable services that are present in the AWS free usage tier [6].

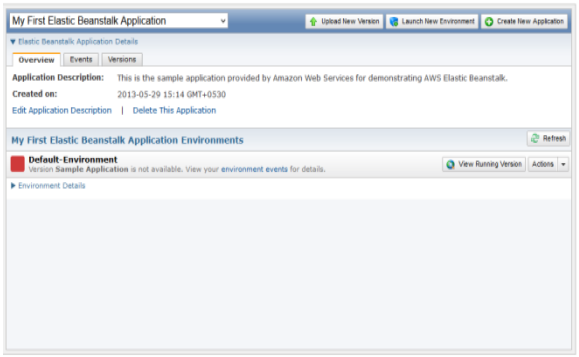

Fig 11 : AWS Elastic Beanstalk

d. Monitoring

Amazon Cloud Watch allows user to select, analyze, and view metrics. It allows to monitor our application and results are concluded as graphical form to the user.

4.2 Applications platform services

a. Amazon Cloud Front

Amazon Cloud Front allows user to develop an easy of distributing content among end users with low latency and high data transfer speed. It is used to deliver static, dynamic and streaming content using global network of the edge locations, Request of the users object is easily automatically routed to the nearest edge locations hence content is delivered to the users with best performance. It is also optimized to work with other AWS services like Amazon S3, Amazon EC2, Amazon Elastic load balancing and Amazon Route 53 It can also work seamlessly with the non AWS origin server with the original, definitive versions of your file [7].

b. Messaging

i. Amazon Simple Queue Services

Amazon SQS provides a highly reliable, Scalable message queue services that enables asynchronous message based communication between distributed components of an application. The components can be two computers or Amazon EC2 instances or combination of both. Using Amazon SQS one can send any number of messages to an Amazon SQS queue at any time from any component and messages can be retrieved from same component or a different one at the same time or later [8].

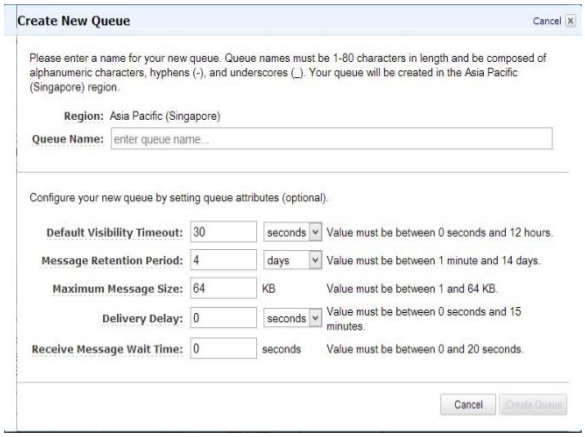

Fig 12 : Amazon Simple Queue Services

ii. Amazon Simple Notification services

Amazon SNS is a web service that makes it easy to setup, operate and send notifications from cloud. It provides developers an aid with highly, scalable flexible and cost effective capability to publish the

Messages from an application and immediately deliver them to applications or the subscribers.
Amazon SNS provide web service interface that can be used to create topics that user needs to notify application about, subscribe clients to these , publish messages and deliver the messages over the client protocol (HTTP/HTTPS).It delivers notification using push mechanism which eliminates the need for periodically checking or poll for new information's or updates. The use of SNS include monitoring certain applications, many workflow systems, time sensitive information updates, mobile applications and much more.[9]

iii. Amazon Simple Email Service

Amazon Simple Email Service allows bulk highly scalable bulk and transactional email sending service. It reduces costs of developing an in house email solutions licensing, installing, and operating a third party email service instead we have an application inbuilt in itself [10].

Fig 13 : Amazon Simple Email Service

c. Amazon Cloud Search

Amazon Cloud Search is a service which allows easy to setup and scale a search solution for users web applications. It allows user to search a large collection of data such as web pages, document files, forum post, or product information's. It enables users to quickly add search capabilities to the websites.

Fig 14 : Amazon Cloud Search

5. SECURITY PRIVACY AND COMPLIANCE CHALLENEGES

5.1 Traditional client server security issues

In Traditional centralized systems the operating system of the host performs the necessary processing for the operation on that system all screen handling, performing logical checks, validations etc.

In these paradigms where the data is distributed across multiple servers and sites , each having its own administrator it is impractical to have centralized security services , and thus avails more opportunities for the intruders to access the system in an unauthorized manner.

Thus it becomes essential to have security individually sustained over each component of the architecture which may include Client, Server, and Network. This increases many overheads and also becomes unreliable in terms of cost and efficiency, Also has many more overheads to secure data.

5.2 Amazon Cloud Security

Amazon web services offers highly scalable cloud computing platform with high availability, flexibility, reliability, which enables users to build a wide range of applications. In order to provide end to end security and end to end privacy AWS provides best security practices in the services enabling the users to ensure confidentiality, integrity and availability of data .At a high level following security approaches are made to secure AWS infrastructure :

Physical Security: AWS infrastructure are placed in Amazon controlled datacenters throughout the world ,whose location information's are known to only those users who have an essential business need and the datacenters themselves are having variety of physical controls within themselves in order to prevent unauthorized access [5].

Secure Services: Every service within the architecture is secured among them and contains number of capabilities that restricts the intruders attack.

Data privacy: AWS allows its users to encrypt their personal or business data within AWS cloud and thus publishes the backup and redundancy procedures for the services.
Moving IT infrastructure to AWS builds a shared responsibility model between the customer and AWS. This shared model reduces operational burden as AWS manages, operates, and controls the components of the host operating system and the virtualization layer beneath the physical security facilities where the services are employed.

5.3 AWS Infrastructure Security [12]

AWS infrastructure provision a number of basic computing resources like processing and storage. Its infrastructure includes facilities, network, hardware along with some operational software's (host OS, Virtualization software etc) that support access of these resources in a secured manner.

a. AWS Compliance program

It enables the user to understand the robust security and have many standards in order to provide security, like SOC 1, SOC 2, ISO 27001, PCI DSS Level-1, ITAR, FIPS 140-2, and HIPPA.

b. Physical and environmental security

Location of the datacenter is generally not available to every individual user and some legitimate business centric user can only acknowledge locations under number of security considerations. It also provide Fire detection and suppression, Uninterruptable power supply, Climate and temperature control, monitoring of electrical, mechanical and life support systems and preventative maintenance of equipments for continued operability.

5.4 Network security

AWS provide security in relevance to the workload

a. Secure network architecture

Many network devices like firewall and other boundary devices are placed in order to perform control and monitoring over external boundaries and key internal boundaries within network, and these boundary devices employs set of rules called as ACL (Access Control lists) whose policies are managed by the Amazon Information Security.

b. Secure Access Points

AWS has limited number of access points to the cloud in order to provide comprehensive monitoring of the inbound and outbound communications and network traffic. The access points of the user are called API which allow secure HTTP access, which thereby enables users to establish a secure communication session.AWS provides a redundant connection to multiple communication service at internet facing edge of AWS network

c. Transmission Protection

User connects to an AWS access point via HTTPs using Secure Socket Layer (SSL) which is a cryptographic protocol designed in order to protect against eaves dropping, tampering and message forgery. AWS requires every message to be authenticated for this it has WS Security standard Binary Security Token profile, consisting of X 5.09 Certification with RSA public key.

AWS also supports SSH (Secure shell network) protocol to enable user to connect remotely with the Unix/Linux instances and gain access securely. Authentication used here is via public or private key. Remote desktop protocol is used to connect with the windows instances.

For users who require some additional layers of security AWS offers Amazon Virtual Private Cloud which provides a private subnet within AWS cloud and also aids an ability to use IPSec Virtual private network which is a device providing encrypted tunnel among Amazon VPC and user's datacenter.

d. Amazon Corporate segregation
AWS production network is logically segregated from AWS corporate network by means of complex set of network security or segregation devices If the developers and the administrator need to interact one another they are first required to have permission from the AWS ticket owner all the requests are reviewed and then approved by the applicable service provider. The approved personal can connect to the AWS network though bastion host that restricts access to the network devices. The bastion host requires SSH Public key authentication.

e. Fault Tolerant Design
AWS has designed the system in such a way that it is can easily tolerate system and hardware failure without imposing any impact over the customer.
There are cluster of datacenters which are placed in the global regions and all the datacenters are function none of them is in cold state and whenever any failure occurs at any datacenter then the deployed applications are shifted to n+1 configuration in order to handle the capacity so that traffic can be load balanced to the remaining sites.

f. Network Monitoring and Protection
AWS provide protection against traditional network security issues as following

i. Distributed Denial of service attack: Here Proprietary DDOS migration techniques and there is enough diversity of internet as they are multi hosted.
ii. Man in Middle attack: All the AWS API are available via SSL protection thus preventing Man in middle attack
iii. IP Spoofing: Host based firewall structure does not allow any instance to send traffic via IP address o MAC address.
iv. Port Scanning: Amazon EC2 does not perform unauthorized port scan by customers.
v. Packet sniffing of other tenants: Virtual instances running in the promiscuous mode cannot receive traffic which is intended for another virtual instance.

5.5 AWS Service Specific Security

Amazon Elastic Compute Cloud (EC2) [5] is a Amazon's Infrastructure as a Service (IaaS) which provide resizable computing capacity using datacenters server instances, it allows creation of instances which are collections of platform hardware and software.

Security within Amazon EC2 is provided on multiple levels i.e.; Operating system of the host platform , virtual instance OS or guest OS, a firewall and signed API calls which prevents the data from unauthorized access of intruders.

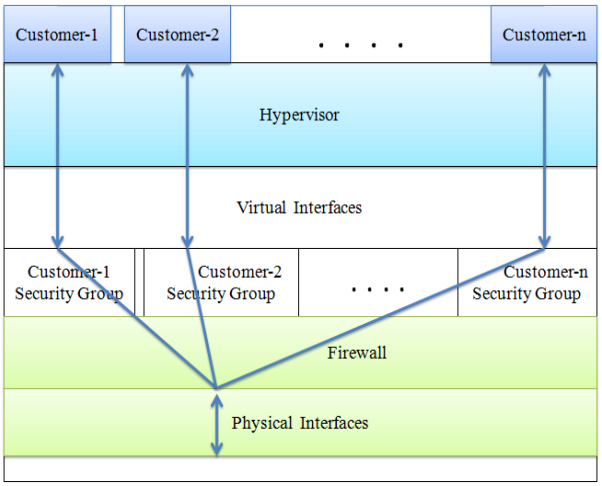

Fig 15 : Amazon EC2 Multiple Layer Security

a. The Hypervisor
Amazon EC2 utilizes Xen Hypervisor taking advantage of Para virtualization as the Para virtualized guests rely on the hypervisor which require privileged access and the guest OS has no elevated access to the CPU.

b. Instance Isolation
Different Instances running on the same machine are isolated from each other via Xen Hypervisor. AWS firewall resides in hypervisor layer which is in between physical network interface and instance virtual interface. Here physical RAM is also separated by the same mechanism.

c. Host Operating System
Administrator with business need is required to have multi factor authentication for the purpose build administrative host.

d. Guest Operating System
Virtual Instances are completely under control of the user and the amazon has no control over it. User can employ privilege escalation mechanism with logging per user bases. User can control updating and patching of the guest OS including the security updates.

e. Firewall
Amazon EC2 have complete firewall solution which is mandatory inbound firewall configured in the deny all mode and Amazon EC2 customer must open the ports explicitly in order to allow inbound traffic. The firewall requires X.509 certificate

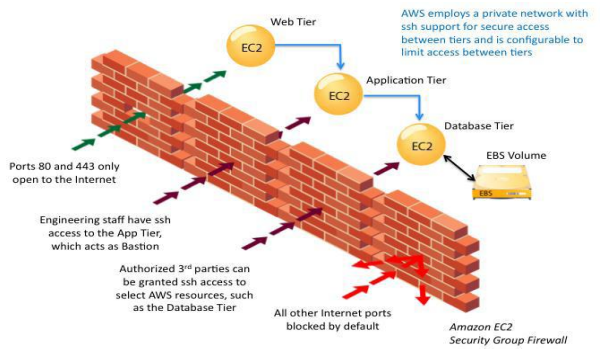

Fig 16 : Amazon EC2

5.6 Auto Scaling Security

Scaling the capacity of Amazon EC2 automatically in accordance to the conditions defined by the user comes under auto scaling. In auto scaling every request made to its control API is required to be authenticated by HMAC SHA-1 signature calculated among request and users private key

5.7 Amazon Virtual Private cloud

Every Amazon EC2 a user launched has randomly assigned public IP address in the Amazon EC2 address space, Amazon EC2 allows user to create their own choice address space in cloud with their own ranges of IPs, and it basically provides an isolated space on Amazon Cloud. An individual can create their own subnets within the VPC, can perform grouping of similar kind of instances based on their IP range and then rout them, impose security in order to control flow of traffic.[13]

5.8 Amazon Simple Database Security

Amazon simple database allows user to simply store and query data items via web service requests. Data is stored in domains similar to database tables except we cannot perform functions across multiple domains. It provides domain level control over APIs. And each request must contain HMAC Signature to enter in domain else rejected. It is accessible via SSL encrypted endpoints.

5.9 Amazon Dynamo DB Security

Amazon Dynamo DB is a No SQL database service which allows creation of any database tables and spreads the data automatically to number of servers to handle the request capacity specified by user and amount of data stored. All the data items are stored in the Solid State Drives. Access to each individual table is controlled by an ACL that maps authenticated users to their table. The user must gain security credentials from AWS Security Token service.
Amazon Dynamo DB is accessible via SSL encrypted endpoints. And each request contains a valid the HMAC-SHA256 signature.[13]

Dynamo DB does not offer any resource based permission system .However service integrates with AWS IAM security token service in order to give other users in the AWS account access to the dynamo DB.

5.10 Amazon relational database security

Amazon RDS creates a relational database instance and flexibly scale the compute, storage and resource capacity in order to achieve the application demand. It includes SSL Connections, automated backups, DB Security groups, multi A-Z deployment etc for network isolation one can run their DB instance in the VPC.

5.11 Amazon Elastic cache Security

Elastic Cache allows a user to retrieve information through a rapidly, managed, in memory caching system instead of using slower disk based database. The Amazon allows user to access cache cluster using Cache security groups which acts as a firewall, which controls network aces to the cache cluster and it is by default turned off and in order to access the cache cluster we need to explicitly enable its access from the host in specific EC2 security group. In order to allow network access to the cache cluster, one must create a cache security group and use the authorize cache security group ingress API to authorize the desired EC2 security group.

5.12 Amazon Simple Queue service security

Amazon SQS access is granted based on AWS account created with AWS IAM user who have access to the operations and queues for which they have been granted permission access via policy. Although by default access to individual queue is restricted to the account however one can allow other access to a queue using either a SQS generated policy or the policy of the user [12]. These services are accessible via SSL encryption endpoints.

5.13 Amazon Simple Notification service security

Amazon SNS provides access control mechanism so that topics and messages are secured against intruder attack. The topic owner can set policy for a topic that restricts who can publish or subscribe topic, and transmission can be encrypted by specifying that delivery mechanism is HTTPs [12]. Again same as SQS its access is also granted based on AWS IAM account , however the user have only access to the operations and topics

5.14 Amazon Simple Email Service Security

In certain conditions when some people intend to send spam messages when the receiver don't wish to receive and spoof other's identity and conceal their own. In order to prevent such problems Amazon services first makes the new users to verify their domain or email address in order to confirm it that they actually own it.AWS periodically reviews domain verification status.

5.15 Amazon Cloud Front Security

Amazon Cloud Front requires that every request must be authenticated by HMAC SHA-1 signature calculated from the request and user's private key.

And also this API is accessible by SSL encrypted endpoints
It also provides an ability to transfer the content over encrypted connection HTTPs.

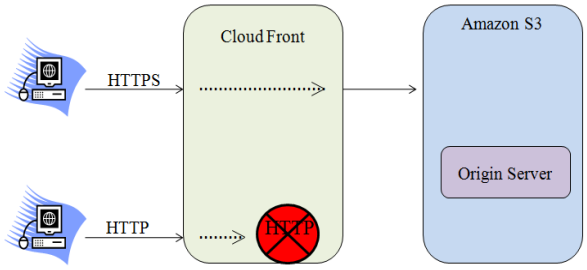

Fig 17 : Amazon Cloud Front Security

5.16 Amazon Cloud Search Security

Amazon Cloud Search encapsulates collection of the data user want to search, search instances that processes the search and configuration that controls how the data how data is indexed and searched. An individual creates separate search domain for each collection of data that is to be made searchable. Access to each of the search domain endpoint is restricted to the IP address so only authorized host can submit documents and submit search request [13].

Amazon Cloud Search provide separate endpoints for accessing the configuration, search and document service

6. SNAPSHOTS

Home Page of the Web Application

Fig 18 : Home Page of the web application

7. RESULTS

Successful deployment of cloud based "Online Art gallery" on cloud using Appfog as PaaS and Word press as Content Management System.

Efficiently security concerns related to the cloud computing scenario were solved using services of Amazon which provide complete and secure package with services and other functionalities suited for the web application deployment over cloud.

8. CONCLUSIONS

- **a.** Study of cloud computing scenario its benefits, PaaS, working with Appfog and Word press.
- **b.** Study of different Amazon services
- **c.** Complete discussion of the Security concerns in traditional and an improved secure system offered by Amazon web services including various security credentials over each and every services offered by Amazon cloud.
- **d.** Successful deployment of cloud based "Online Art gallery" on cloud using Appfog as PaaS and Word press as Content Management System.
- **e.** Amazon Web Services are successfully managed.
- **f.** Integrations of Add-ons like speechify, Cloudmalin, Iron maker, Cloud nary,
- **g.** Video integration over the web application in order to allow a better aid to the user.

9. REFERENCES

[1] aws.amazon.com/what- is-cloud-computing/

[2] www.appfog.com/docs/getstartes

[3] wordpress.org.com/docs

[4] docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/intro.html

[5] aws.amazon.com/documentation/cloudformation

[6] aws.amazon.com/documentation/cloud beanstalk

[7] aws.amazon.com/documentation/cloudfront

[8] aws.amazon.com/documentation/sqs

[9] aws.amazon.com/documentation/sns

[10] aws.amazon.com/documentation/ses

[11] aws.amazon.com/documentation/cloudsearch

[12] AWS_Security_whitepaper march 2013.

[13] aws.amazon.com/security