Chapter

Cloud Security in Middleware Architecture

Jagdish Chandra Patni

Abstract

The new Internet of Things (IoT) has increased the need for computing, connectivity, and storage capacities as the amount of sensitive data grows. Since it provides on-demand access to a common pool of resources such as processors, storage, software, and services, cloud computing can seem to be a convenient solution. However, there is a cost, as excessive communications burden not only the core network, but also the cloud data centre. As a result, it's critical to consider appropriate approaches and security middleware solutions. In this chapter, we define a middleware architecture to address security concerns and explore the general concept of cloud to achieve a higher level of security. Since it is designed to pre-process data at the network's edge, this security middleware functions as a smart gateway. Data can be processed and stored locally on fog or sent to the cloud for further processing, depending on the information obtained. Furthermore, the devices communicate via middleware, which gives them access to more computing power and improved security capabilities, allowing them to conduct safe communications. We discuss these concepts in detail, and explain how this is effective to cope with some of the most relevant security challenges.

Keywords: Internet of things, Cloud middleware, Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-service, Amazon web service, Microsoft Azure, Virtual machine, Virtualization

1. Introduction

Cloud security ensures the secure cloud computing environment from both the internal and external cybersecurity attacks. Cloud computing, deliver the services to the end users by using information technology tools and methods that is now most demanding area of research for the public as well as private sectors those want to accelerate in the field on research and innovation. Widespread use of cloud computing technology also emerge the security challenges to the cloud developers. It becomes more interesting to create the cloud security solutions to prevent from unauthorised users or cybersecurity attacks/threats [1].

1.1 Cloud computing categories

Basically four main categories of cloud computing in practice and they are as follows:

1.1.1 Public cloud services, by public cloud provider

Public cloud services are the services provided by the public cloud providers, are SaaS, IaaS, and PaaS.

In public cloud type all the computing resources are available for the public use via internet [2]. All the resources may be varied depending upon the services providers but all include storage, applications or virtual machines. It provides the resource sharing and processing power distribution that is difficult to achieve by an organisation on its individual capacity.

Some public cloud services are free to use for all the users and some services are restricted to selected individuals or organisations. The use of resources are available to rest of users by paying the charges or subscriptions that vary one to another. That will save the huge amount of money of an organisation that want higher processing speed without setting its own setup (**Figure 1**).

While cloud services are used by public, security becomes the major concern and that need to be addressed properly. To address the security concern we needed the experienced staff and set of methods and protocols those can deal with security. Strict policies and procedures have to deployed to protect data from other different intended users.

1.1.2 Benefits and challenges of public cloud

The cloud services provides the faster and complete solution that is really not possible with the individual capacity of an organisation. It also ensures that no need to go for additional hardware and software solutions once the business is growing.

Cloud based services and applications can be used with the help of less hardware and software with great performance. We can also explain that end users not need to worry about installing and updating the hardware as well as software. It always ensures that all the applications will be up to the mark all the time without investing too much infrastructure and budget.

Public cloud helps to the organisations to grow without accumulating substantial costs. Examples of public cloud include like Amazon AWS, MS Azure are charging as per the usage by customers or organisations that reduce the operational cost of the organisations.

Figure 1.
Cloud computing architecture [3].

DOI: http://dx.doi.org/10.5772/intechopen.98541

1.1.3 Private cloud services, managed by a public cloud provider

The for the individual customers that can be operated by third party.

- Operated by internal staff — The cloud services are managed and maintained by data centre internal staff as per the individual customer requirement in a virtual environment they control.

- The computing will be dedicated to the individual business of individual entity. This can be setup by cloud providers on the customer premises.

- By deploying cloud services it enhanced the control given to the individual business organisation.

- It is a type of virtual private cloud that can be set as at the customer unit or by virtual environment (**Figure 2**).

1.1.4 Benefits of private cloud

The following are the benefits to use the private cloud [4]:

Security and compliance: Compliance is critical for companies operating in highly regulated industries. Since confidential data is stored on hardware that no one else can access, private cloud storage allows businesses to comply with strict regulations. This benefit is available both in on-premises hardware installations and in hosted services.

Customization: An on-site cloud architect builds a completely private cloud, allowing stakeholders to decide exact environment required to run specific applications. The benefits of private clouds are similar to those of on-premise private

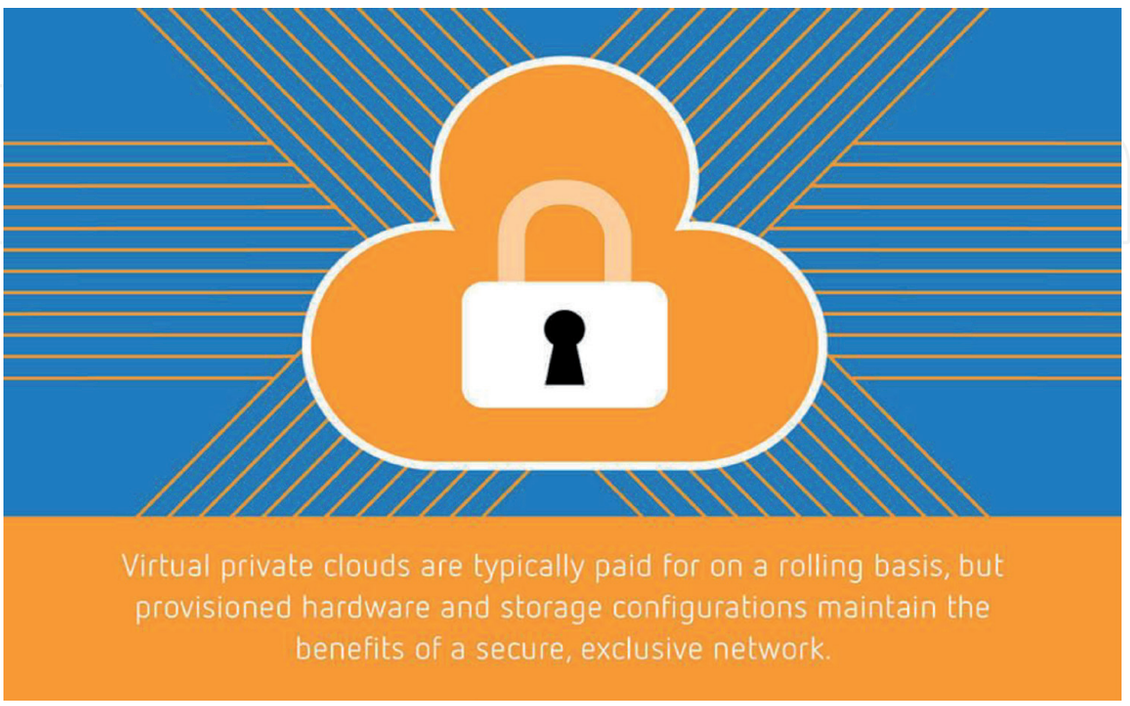

Figure 2.
Virtual private cloud [3].

clouds, but they do not need any on-site configuration. The company collaborates with a provider to set up and maintain a cloud that is solely for its use.

Hybridization: Hybridization expands the capabilities of a both private cloud and public cloud to ensure uptime without the need to mount new physical servers when an application requires more computing resources. This will be a cost-effective option for businesses that need protection of a private cloud also require the powerful services of public cloud for other functions.

1.1.5 Challenges of private cloud

If a company's computing needs aren't predictable, a private cloud can be problematic. When resource demand fluctuates, a private cloud can be unable to scale efficiently, thereby costing the company high investment. Some key considerations for IT peoples to think about.

Direct cost on Investment: It require significant investment to deploy the fully functional private clouds that hosted on-site and it may be value for the organisation after long time. Hardware cost is very high to establish a private cloud, and the environment would need to be set up, maintained, and managed by an expert cloud architect. Hosted private clouds, on the other hand, will significantly reduce these costs.

Capacity utilisation: The company is solely responsible for optimising resources usage in private cloud model. A cloud deployment that is underutilised can cost a company a lot of money.

Scalability: Where more computing power needed from private clouds, scaling the resources of private cloud that can take more time and money. This procedure would typically take more time to scale a virtual machine or requiring more services from a public cloud service provider.

1.1.6 Private cloud providers

Organisations who want to use the private cloud but do not have the funds to invest in an on-site solution will partner by using private cloud service provider. Some of the most well-known names in this field are:

Hewlett Packard Enterprise

HPE is a big name in the field of cloud computing era. Offering robust services as per the organisational needs. Customers can select hardware as well as software as per their needs.

Cisco

On-demand storage, advanced application performance management and automated container management are all available from Cisco. Data protection that have sufficient workloads to improve compliance is provided by Cisco solutions. Cisco have teamed up to provide stable application, desktop, networking and cloud delivery solutions to help businesses grow into digital enterprises.

Microsoft

Any corporate data centre will benefit from Microsoft's Azure Stack solution, which brings the power of an integrated cloud to any data centre. Azure is ready for hybridization, so businesses can take advantage of compliance features while still taking advantage of the full Azure cloud solution as required. Learn how Citrix and Microsoft are working together in the cloud to help you keep up with the pace of business.

Dell, IBM, VMware, Oracle and Red Hat are other big names in the field of private cloud providers [3].

1.1.7 Hybrid cloud services

Price, protection, operations, and access can all be optimised by combining private and public cloud computing configurations to host workloads and data. Internal personnel and, if desired, the public cloud provider would be involved in the operation.

A hybrid cloud services are combining the on premises computing infrastructure with private cloud services and public cloud services to get the higher computing, storage and services.

1.1.8 Hybrid cloud benefits

While cloud providers can help you save money, their real value comes from their ability to support a fast-paced digital business transformation. There are two priorities in any technology management organisation: various key points like IT and business transformation. Traditionally, The IT key points more focused on cost-cutting. ON the other hand digital transformation focused on making money from investments.

The main advantage of a hybrid cloud is its flexibility. A central concept of a digital company is the need to adapt and change direction quickly. To achieve the high performance and robustness the organisations combines all three public clouds, private clouds with on-premises resources [5].

1.1.9 What about hybrid Cloud good of bad?

Everything cannot belongs in the public cloud, the progressing businesses are opting for a hybrid cloud solution. Hybrid clouds combine the advantages of both by using existing data centre architecture.

This approach enables its components and other applications to communicate across boundaries, instances of cloud, and architectures. Data needs the same degree of delivery and access flexibility. In the complex digital world, whether you are dealing with workloads or databases, you can prepare for things to change around in response to changing needs.

1.1.10 Hybrid cloud scenarios

- **Dynamic workload Conditions-** For our dynamic workloads, use scalable public cloud and computing sensitive workloads on private clouds or in our private data centres.

- **Categories between critical and less-sensitive workloads-** We use a public cloud to compute our other business applications and other sensitive or critical applications on our private cloud.

- **Processing huge amount of Data-** It's unlikely that you'll be able to process large amounts of data at a near-constant rate. Instead, we could use highly scalable public cloud tools for our big data analytics and to keep our confidential data with complete protection we can use the private clouds with higher set of security systems.

- **Easy switching of data -** Use a public cloud or a private cloud for rest of the miscellaneous workloads. Also see the best suit for the organisation and switch accordingly between public and private.

- **Temporary arrangements of Resources**- Whenever our requirements are for a short time so instead to setting our cloud setup go with a public cloud that reduces the extra burden on us.

1.2 Comparison between public, private and hybrid cloud

A private cloud, also known as a corporate cloud, is either provided by a service provider or built on-site at a company's data centre. In either case, since the services are earmarked for particular users only, the private cloud appears to provide more protection.

As resource demand increases, a hybrid cloud environment extends a stable private cloud to a public cloud. This model enables businesses to remain compliant while still taking advantage of public resources. Organisations that use hybrid cloud will get the most out of their internal resources without causing a resource overload if demand spikes unexpectedly [6].

To access the applications and services from online computer is a key benefit of public cloud services. We can use the critical or complex applications virtually because the computer performs little to no computation.

To ensure smooth and fast disaster recovery, a service provider can store replicated files across multiple data centres. Public cloud platform also ensure the data safely from outside world that considered secure from the majority of threats. Public clouds can be configured differently:

1.2.1 Software as a service (SaaS)

In which a provider distributes its computing hosted in the cloud is known as software as a service (SaaS). The programme is accessed via the internet. Individual users are not required to install software on their personal computers under this model. This lowers the organisation's hardware requirements while also lowering service and repair costs.

1.2.2 Platform as a service (PaaS)

Platform as a service (PaaS) is a computing model that enables a company to build software without having to worry about the infrastructure. In essence, a provider creates and maintains an optimised environment that users can easily access by internet. Version control and compile facilities, as well as computing and storage tools, are often included in PaaS.

Figure 3.
Cloud services [2].

1.2.3 Infrastructure as a service (IaaS)

Infrastructure as a service (IaaS) is a business model under which a company outsources the entire data centre to a cloud provider. The provider manages the virtualization of the environment and hosts. Cloud adoption is made easier with IaaS. Purchasing and repairing hardware on-site is also more expensive than using the device (**Figure 3**).

2. Cloud security responsibilities

All the services like data, applications are hosted by a third party while using a public cloud computing service, which is a significant difference between cloud computing and traditional IT services, where data is stored within a network that managed by self. First and main step in developing a cloud security plan is to understand security responsibilities [7].

Major cloud providers strive to provide consumers with a stable cloud. Preventing breaches and retaining public and consumer confidence is central to their business model. Cloud providers may try to prevent cloud security problems with their services, but they have no control about how consumers use them, add data and those are going to access the data. The provider and the cloud client share various levels of security obligation in each public cloud service form. These are the different types of services:

- **Software-as-a-service-** Users are self-responsible to secure the data and its access.

- **Platform-as-a-service**-Users are self-responsible to secure the data and its access and applications used by them.

- **Infrastructure-as-a-service-**Users are self-responsible to secure the data and its access, applications used by them, operating systems and network traffic.

2.1 On-premise SaaS vs. PaaS vs. IaaS

Clouds were once all white fluffy stuff in the sky, and the IT services are restored at on-premise. Almost all of the applications and processes can now be run on the Cloud platform.

- **IaaS:** Cloud services as per use and pay option for various services like storage and virtualization.

- **PaaS:** Various tools in place of hardware and software that are available with cloud providers.

- **SaaS:** software's that we can use with the help of third party using cloud platform.

- **On-premise**: The software and services are going to be installed within the organisation (**Figure 4**).

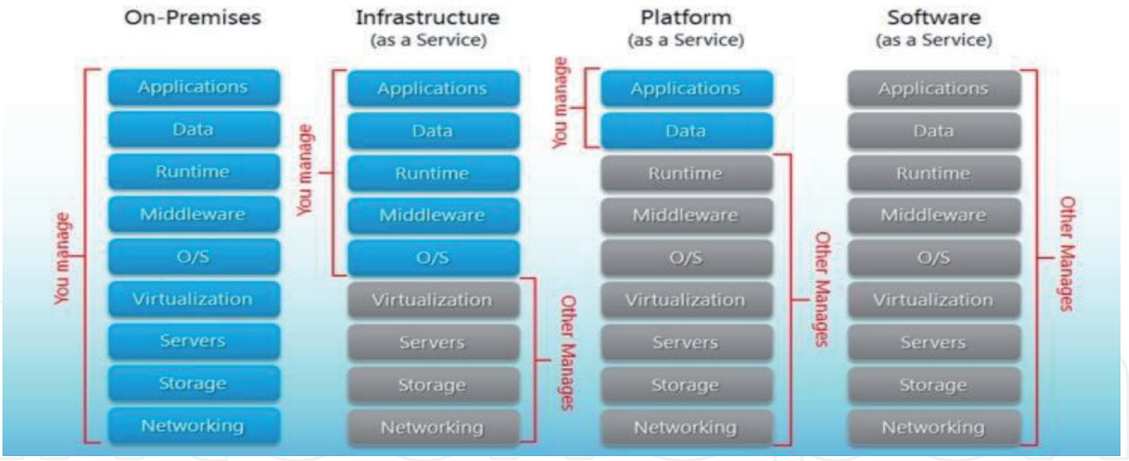

Figure 4.
SaaS, PaaS, and IaaS examples [2].

Most of the companies are using the combination of all three computing models, and few of the organisations are hiring the developers for PaaS-based applications.

Google Apps, Salesforce, Dropbox, MailChamp, ZenDesk, DocuSign, Slack, Hubspot are the examples of IaaS.

AWS Elastic, Windows Azure, Force.com, OpenShift, Apache Stratos, are the examples of PaaS Cloud Services.

AWS EC2, Google Compute Engine, Digital Ocean, are the examples of SaaS cloud services.

Customers are responsible for protecting their data and monitoring who has access to it in all forms of public cloud services. Cloud storage data protection is critical to effectively implementing and reaping the advantages of cloud computing. Organisations considering common SaaS services such as Microsoft Office 365 or Salesforce should think about how they'll handle their shared responsibility for cloud data security. IaaS providers such as Amazon Web Services (AWS) and Microsoft Azure need a more systematic strategy that begins with data [8].

2.2 Cloud security architecture- Consumer's perspective

Cloud services come in a variety of flavours, including SaaS, PaaS, and IaaS (SPI), using the public, private, and hybrid operating models. The issue and solutions pertaining to Cloud security depends on the patterns. The defined architecture should be aligned with all the issues, and security controls built into the cloud architecture.

So, when designing applications for computing models, what architectural requirement and resources needed for cloud application development and their disposal. In this post, I'll go over how to build "adequate" protection into your IaaS and PaaS applications [9].

2.3 Cloud security model

Let us start with the operational model for cloud protection. In public cloud protection obligations are shared between the cloud service providers and cloud users, while the customer manages all the activities in a private cloud. The shared infrastructure, like routers, is the responsibility of cloud service providers.

Within a cloud service, the figure below depicts the layers that are protected by the provider versus the client (**Figure 5**).

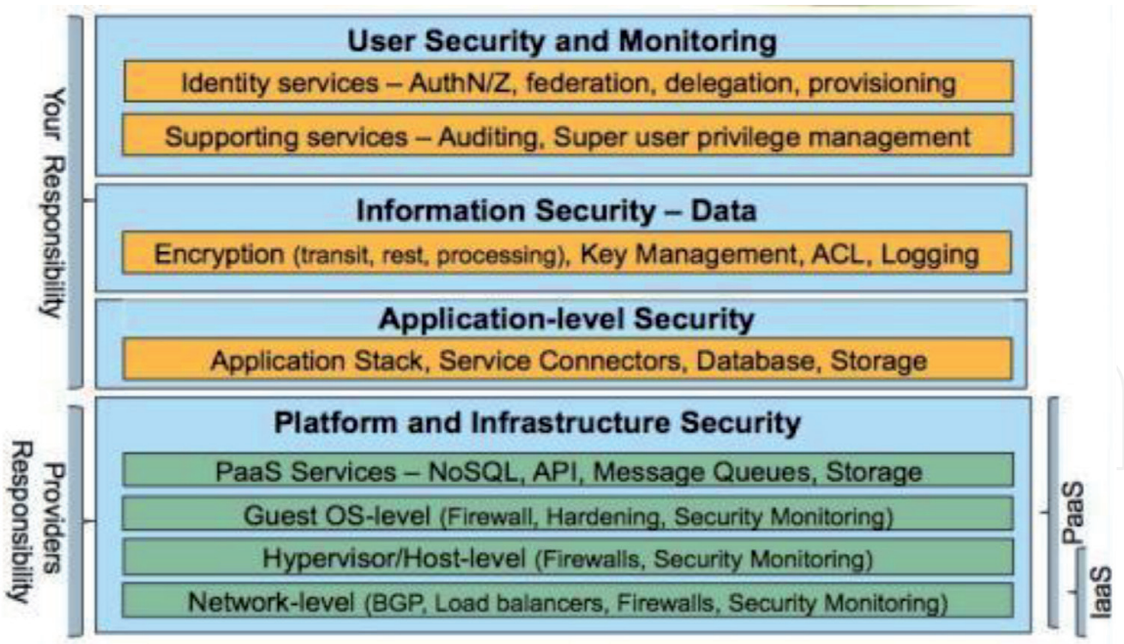

Figure 5.
Layered architecture of Cloud services [5].

It's important to do a difference review on cloud service capabilities before signing up with a provider. This exercise should assess the cloud platform's maturity, accountability, and compliance with enterprise security requirements (such as ISO 27001) as well as regulatory standards like PCI DSS, HIPAA, and SOX. Application migration can be sped up with the use of cloud security maturity models.

The following the security measures are used to ensure the proper safety of the cloud services.

- **Security policies, compliance and practices**: Industry standard frameworks such as ISO 27001, SS 16, and the CSA Cloud controls matrix should be demonstrated by the cloud service provider. Controls approved by the vendor should meet the enterprise data protection standard's control requirements. The scope of controls should be reported when cloud services are approved for ISO 27001 or SSAE 16 [10].

- **Cloud Security architecture:** As per the enterprise norm, the cloud service provider should report security architectural information that either support or impede security management. For example, the virtualization architecture that ensures tenant isolation should be made public.

- **Automation –** Providers can adopt the security automation by publishing API's that used to allow the users to access the logs, privileges and other security threats.

- **Governance and Security Management:** The customer's governance and security management obligations should be specifically defined in comparison to those of the cloud provider.

2.4 Cloud mitigation and security threats

Is cloud computing making the application more vulnerable to security threats? What are the most pressing emerging threats? What are the traditional risks that

have been exacerbated or muted? Answers are contingent on the implementation and operating models used by cloud services. The threats will be like data leakage, misconfiguration of services, weakness of VM, attacks via API and failure of VM. The problems can be resolved by making Hardening of VM, incorporating encryption, authentication with security automation, etc. [11].

Threats to service availability, information confidentiality and honesty, must be factored into the design.

2.5 Threat to cloud service availability

DDoS attacks or misconfiguration errors by cloud service providers or customers can interrupt cloud services (SaaS, PaaS, IaaS). These errors have the ability to spread across the cloud, disrupting the network, processes, and storage that are used to host cloud applications. Cloud systems should be designed to survive disturbances to shared resources in order to achieve continuous availability. Applications that were designed to withstand faults within an area, on the other hand, were largely unaffected by the outage and remained accessible to users. As a design philosophy, assume that something will go wrong in the cloud and plan accordingly. Physical hardware failure as well as service interruption within a geographic area should not be a problem for applications.

2.6 Cloud architecture- security services

As a first step, architects should learn about the security features that cloud platforms have (PaaS, IaaS). The framework for integrating protection into cloud services is depicted in the diagram (**Figure 6**).

Offerings and capabilities in terms of security continue to change and differ between cloud providers. As a result, you'll sometimes find that security features like key management and data encryption aren't available. For example, encrypting security objects and keys escrowed to a key management service requires an AES 128 bit encryption service. For such applications that rely on internal resources, a "hybrid cloud" deployment architecture pattern may be the only viable choice. Single Sign-On is another common use case (SSO). If it is a federation architecture

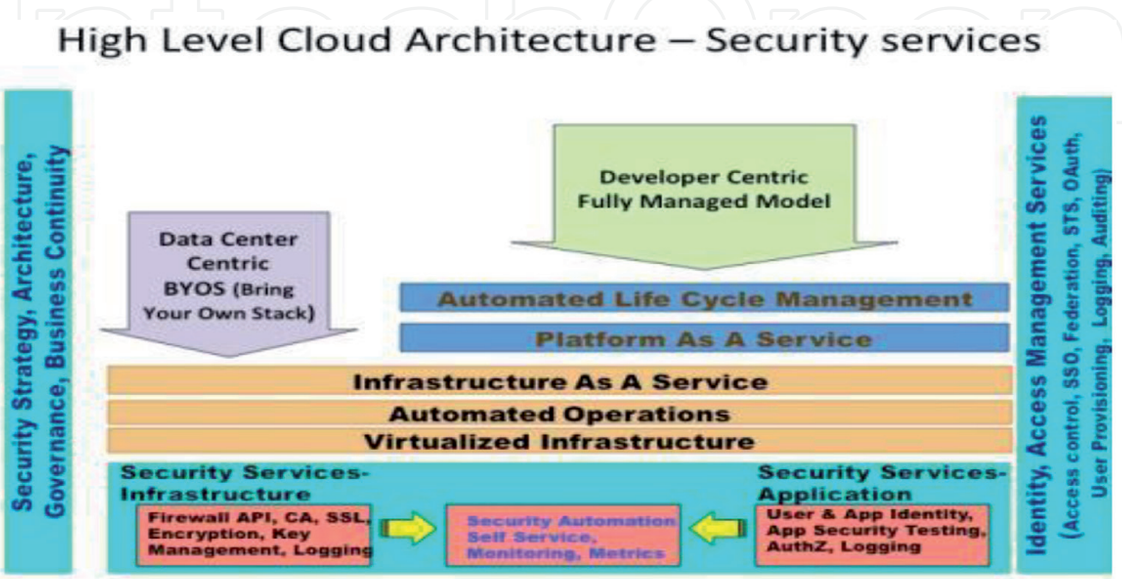

Figure 6.
Cloud security architecture [5].

using SAML 1.1 or 2.0 provided by the cloud service provider, SSO deployed within an organisation may not be extensible to cloud applications.

The following are best practices used in cloud security to mitigate risks to cloud services:

2.6.1 Security service architecture

In the cloud, application implementations necessitate the orchestration of various resources, such as DNS, load balancing, network QoS, and so on. Security automation encompasses the automation of firewall policies between cloud security zones, certificate provisioning (for SSL), virtual machine device configuration, privileged accounts, and log configuration, among other things. Security-related application deployment processes, such as firewall policy development, certificate provisioning, key delivery, and application pen testing, should be moved to a self-service model. This method eliminates human interaction and allows for a security-as-a-service scenario.

2.6.2 Implement identity, access management architecture and practice

Strong user access management infrastructure will be needed as a result of scalable cloud bursting and elastic architecture, which will rely less on network-based access controls. User provisioning and deprovisioning, authentication, federation, authorization, and auditing are all aspects of user and access management lifecycles for both end users and privileged users that should be addressed by cloud access control architecture. In public, private, and hybrid cloud models, a sound architecture would allow reusability of identity and access services for all use cases. Stable token facilities, as well as correct consumer and entitlement provisioning with audit trails, are best practises. The first step in expanding enterprise SSO to cloud services is to construct a federation architecture. Cloud protection partnership is a good place to start.

2.6.3 Automate safeguards

To allow automation, any new security services should be deployed with an API (REST/SOAP). At the time of application deployment, APIs can help simplify firewall rules, configuration hardening, and access control. This can be accomplished by combining open source resources like puppet with the API provided by the cloud service provider.

2.6.4 Encrypt sensitive data

Private cloud applications can be deployed in the public cloud tomorrow. As a result, regardless of the potential operating model, design applications to encrypt all confidential data.

2.6.5 Authenticate IP address and services

Since IP addresses in the cloud are ephemeral, you cannot rely on them to enforce network access control. To allow SSL between cloud providers, use certificates.

2.6.6 Log, log, log

All security activities should be logged centrally in order to build an end-to-end transaction view of non-repudiation characteristics. Logs and audit trails are the

only accurate evidence used by forensic engineers to analyse and understand how an application was compromised in the case of a security incident.

2.6.7 Continuously monitor cloud services

Given that preventive controls cannot meet all enterprise requirements, monitoring is an essential feature. To perform security event correlation, security monitoring should use logs produced by cloud services, APIs, and hosted cloud applications. The CSA's cloud audit (cloudaudit.org) will help with this mission.

2.7 Cloud security principles

The product development culture, emerging technology implementation, IT service delivery models, technology policy, and investments made in the field of security tools and capabilities all show that each company has a different level of risk tolerance. When a company's business unit chooses to use SaaS for business purposes, the technology architecture changes. The security architecture should also be consistent with the technology architecture and principles. An enterprise technology architect should understand and configure the following cloud security concepts [12]:

- Cloud-based services should adhere to the concept of least privilege.
- Using firewalls and container – isolation between different protection zones should be ensured. Cloud firewall policies should adhere to data sensitivity-based trust zone isolation requirements.
- End-to-end transport level encryption (SSL, TLS, IPSEC) can be used by applications to protect data in transit between cloud and business applications.
- Authentication and authorization should be delegated to trusted security providers by applications. SAML 2.0 can be used to support single sign-on.
- Enterprise standard VM images can be used to deploy applications in a trusted zone.
- When implementing a virtual private cloud, industry standard VPN protocols including SSL, SSH, etc.
- Using an API, cloud security monitoring can be combined with existing security tools and services.

2.8 Cloud security architecture patterns

Cloud security risks can be mitigated by designing effective security controls that secure the CIA of information in the cloud. The vendor, the enterprise, or a third-party provider can provide security controls as a service (Security-as-a-Service). The point of security controls (safeguards) – technologies and processes – is usually where security architectural trends are expressed [13].

Security architecture trends act as a compass, allowing developers to move applications to the cloud faster while minimising security risks. Furthermore, cloud security architecture trends should emphasise the trust boundary between different cloud services and components. Normal interfaces and protection protocols (SSL, TLS, IPSEC, LDAPS, and so on) should also be highlighted in these patterns.

Finally, the patterns can be used to build security checklists that can be automated using configuration management software such as puppet.

For each of the security resources consumed by the cloud application, trends should highlight the following attributes (but not limited to):

- Logical place – in-house, third-party cloud, native to cloud service The service's efficiency, availability, firewall policy, and governance can all be affected by its venue.
- Protocol(s) – Which protocol(s) is/are used to call the service? For e.g., for service requests, REST with X.509 certificates.
- Service feature – What is the service's purpose?
- Input/output – What are the security service's inputs, including monitoring methods and outputs? Input = XML doc and Output = XML doc with encrypted attributes, for example.
- Overview of the security control – What security controls does the security service provide? For instance, information confidentiality at rest, user authentication, and device authentication.

2.8.1 Security services based on infrastructure

A cloud service provider is required to provide security controls for DoS privacy, as well as confidentiality and integrity protection for sessions originating from mobile and PC, according to the pattern.

2.8.2 Application based security services

Identification, authentication, access enforcement, system identification, cryptographic services, and key management can all be handled by the cloud service provider, the corporate data centre, or a combination of the two (**Figure 7**).

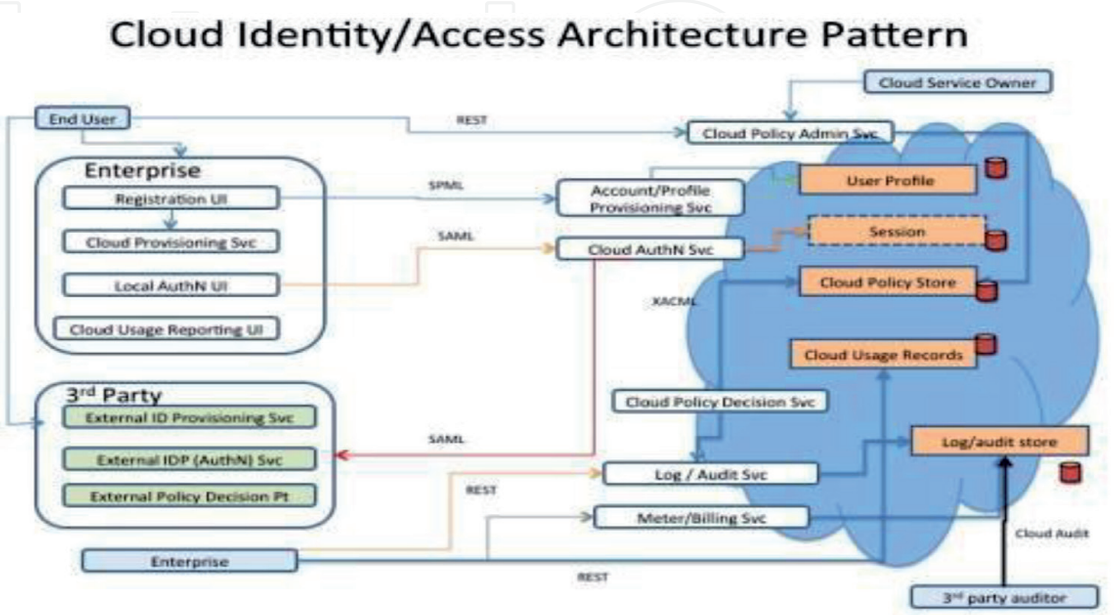

Figure 7.
Identity and access pattern [5].

User registration, authentication, account provisioning, policy compliance, logging, auditing, and metering are all examples of typical cloud access control use cases illustrated in this pattern. It focuses on the actors who communicate with cloud, in-house (enterprise), and third-party hosted services:

2.9 Identifications of security services

- An authentication service that allows users to log in via an enterprise portal (Local AuthN UI) and is usually provided via the SAML protocol. A cloud session store stores the authenticated session state.
- The account and profile provisioning service facilitates the development of new accounts and user profiles, usually through the use of SPML (Service Provisioning Markup Language).
- The cloud policy admin service is used to manage policies that control which cloud services end users have access to. Cloud service owners (enterprises) can use this service to perform administrative tasks, while end users can request access to cloud services. The cloud policy store is where cloud policies are held.
- The logging and auditing service can be used for two purposes. The first is cloud-based event reporting, which includes security events, and the second is auditing. This service can be accessed using Cloud Audit protocols and APIs.
- The metering programme keeps track of how much cloud resources are being used. This service can be used for chargebacks as well as billing reconciliation by finance departments.

2.10 Identity security services in the Enterprise

- Domain registration UI is a user interface for registering, managing, and provisioning new cloud services. The cloud providers implement authentication and authorization.
- End users produce usage reports using the cloud usage reporting UI.
- A cloud provisioning service is used to make cloud resources accessible (compute, storage, network, application services).

2.11 Third party identification of security services

Identity services provided by a third party and hosted at their location are used by cloud applications. Third-party users who need access to cloud infrastructure to conduct business functions on behalf of the company may get help from services. Backup and device control, for example. The third-party provider is in charge of user authentication, provisioning and access enforcement.

3. Cloud security challenges

According to Gartner, the global public cloud services market will increase 17 percent to $266.4 billion in 2020, up from $227.8 billion in 2019. In its study "high risk to Cloud Computing: Egregious Eleven," the CSA (cloud security alliance) outlined the following major cloud challenges.

3.1 Data breaches

The effects of data breaches will include the following:

- Impact on customer or partner credibility and confidence
- Loss of intellectual property (IP) to rivals, which could have an effect on the release of goods.
- Regulatory ramifications that could lead to financial loss.
- Brand effect, which may result in a decrease in market value due to the factors mentioned above.
- Legislative and contractual obligations.
- Expenses incurred as a result of incident response and forensics

3.2 Improper change management

This is one of the most popular cloud challenges. In 2017, a misconfigured AWS Simple Storage Service (S3) cloud storage bucket exposed 123 million American households' detailed and private data. Experian, a credit bureau, owned the data collection, which it sold to Alteryx, an online marketing and data analytics firm. Such occurrences have the potential to be catastrophic.

3.3 Poor architecture and mechanism

Organisations all over the world are moving parts of their IT infrastructure to public clouds. The introduction of sufficient security infrastructure to withstand cyberattacks is one of the most difficult challenges during this transition. Unfortunately, many businesses are still baffled by this operation. Another contributing factor is a lack of awareness of the shared security obligation model.

3.4 Improper identification and key management

Multiple improvements to standard internal system management procedures related to identity and access management are introduced by cloud computing (IAM). These aren't even brand-new problems. Rather, when dealing with the cloud, they are more serious concerns because cloud computing has a significant effect on identity, certificate, and access management.

3.5 Threats within the organisation

The employee within the organisation can be a threat by using the sensitive data in their personal use or sharing the confidential data with others.

3.6 Wrong interfaces and API

Customers can manage and communicate with cloud services through a series of software user interfaces (UIs) and APIs exposed by cloud computing providers. The security and availability of general cloud services are also reliant on these APIs' security. APIs that aren't well-designed can lead to misuse or, worse, a data breach.

APIs that have been broken, leaked, or compromised have resulted in significant data breaches.

4. Cloud security solutions

To address the primary cloud security challenges in terms of visibility and control the following requirement need to be accessed [14, 15].

4.1 Access to the cloud service

Direct access to the cloud service is needed for a full view of cloud data. An application programming interface (API) access to the cloud service is used by cloud security solutions to achieve this. It is possible to access data using an API link:

- Where does your data go in the cloud?
- Who is making use of cloud data?
- The positions of consumers of cloud service access.
- With whom do cloud users share data?
- The location of cloud data.
- The location from which cloud data is accessed and downloaded, as well as the user.

4.2 Cloud data control

Need to apply the controls that best suit the organisations demands. These safeguards include:

- Classification — As data is generated in the cloud, classify it on multiple levels, such as confidential, controlled, or public. Data may be prohibited from entering or exiting the cloud service after it has been classified.
- Implement a cloud data loss prevention (DLP) solution to protect data from unauthorised access and automatically disable access and data transport when suspicious behaviour is detected.
- Manage collaboration controls in the cloud service, such as reducing file and folder permissions for specific users to editor or viewer, deleting permissions, and revoking shared links. Ensure the cloud data should be encrypted from unauthorised users.

4.2.1 Data access and its applications

Security relies heavily on access control.

- User access control — Set up device and application access controls to ensure that only approved users have access to cloud data and applications. To implement access controls, a Cloud Access Security Broker (CASB) may be used.

- User access control — If a personal, unauthorised device attempts to access cloud data, access is denied.

- Malicious behaviour detection — Use user behaviour analytics (UBA) to detect compromised accounts and insider attacks, preventing malicious data exfiltration.

- Malware protection — Use techniques like file inspection, device whitelisting, machine learning-based malware identification, and network traffic analysis to keep malware out of cloud services.

4.3 Compliance standards and policies

The policies and standards should be updated and expanded as per the current and forthcoming threats.

- Risk assessment — Re-evaluate and upgrade risk assessments to incorporate cloud services. Identify and mitigate the risks posed by cloud environments and providers. To speed up the evaluation process, risk databases for cloud providers are available.

- Application regulatory requirements like PCI, HIPAA, Sarbanes-Oxley, etc. and its assessment.

4.4 Cloud security importance

According to news reports, one out of every four businesses that use public cloud services has had data stolen by a malicious actor. An additional one out of every five people has had an advanced assault on their public cloud infrastructure. According to the same survey, 83 percent of businesses said they store confidential data in the cloud. With 97 percent of businesses using cloud services today, it's critical that everyone assesses their cloud security and establishes a data-protection strategy.

McAfee's cloud protection helps businesses grow faster by allowing them complete visibility and control over their data in the cloud. Find out more about McAfee's cloud protection technologies.

Cloud MVISION

The enterprise's multi-cloud protection platform. Create a single protection policy that can be used through SaaS, PaaS, IaaS, Containers, and the Web. Accelerate cloud adoption by simplifying security for a distributed workforce.

Unified Cloud Edge (UCE) is a component of MVISION Cloud that integrates data security from devices, the network, and the cloud to make SASE architecture adoption easier.

Platform for Cloud-Native Application Security (CNAPP).

CNAPP, which is part of MVISION Cloud, audits and secures the entire IaaS/PaaS stack, including containers and private clouds.

5. Conclusion

We can integrate protection into your software without having to reinvent the wheel inside your app's boundaries, saving money on "bolt-on" safeguards. Creating security standards and architectural patterns that can be used in the design process is a good practise. During the design process, architectural trends will assist in

articulating where controls are applied (Cloud versus third party versus enterprise) so that sufficient security controls are baked into the application design. When designing cloud protection trends, keep in mind the applicable threats and the risk-appropriate principle. Discussed the various security challenges and its possible security solutions that mostly needed for the secure system. Finally, a cloud protection architecture should meet the needs of developers in terms of protecting the confidentiality, integrity, and availability of data processed and stored in the cloud.

Author details

Jagdish Chandra Patni
School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

*Address all correspondence to: patnijack@gmail.com

References

[1] Move confidently to hybrid multicloud and integrate security into every phase of your cloud journey, The premier hybrid cloud and AI event May 11-May 12, Americas

[2] The Different type of cloud computing and how they differ, https://www.vxchnge.com/ (April 2021)

[3] https://www.citrix.com/en-in/glossary/what-is-public-cloud.html (March 2021)

[4] Six Common Challenges of Cloud Implementations, white paper, September 2014.

[5] Managed Cloud Services for Hyper Performance and Uninterrupted Continuity, Cloud 4C, CtrlS (March 2021)

[6] Introduction to Cloud Security Architecture from a Cloud Consumer's Perspective by Subra Kumaraswamy, InfoQ, Dec 07, 2011

[7] The cloud-based energy and asset management platform from Siemens powered by MindSphere

[8] Roshana Gul, The Relationship between Reputation, Customer Satisfaction, Trust, and Loyalty, Journal of Public Administration and Governance ISSN 2161-7104 2014, Vol. 4, No. 3, September 22, 2014

[9] Jaydip Sen, Security and Security and Privacy Privacy Privacy Issues in Cloud Computing Computing, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[10] Security for Cloud Computing Ten Steps to Ensure Success, Cloud Standards Customer Council, 2017

[11] What is cloud Security, https://www.mcafee.com/ (May 2021).

[12] Cloud Security Challenges, https://cloudsecurityalliance.fr/ (April 2021)

[13] Hybrid Cloud, https://www.netapp.com/hybrid-cloud/what-is-hybrid-cloud/ (April 2021)

[14] Wissam Razouk, Daniele Sgandurra, and Kouichi Sakurai. 2017. A new security middleware architecture based on fog computing and cloud to support IoT constrained devices. In Proceedings of the 1st International Conference on Internet of Things and Machine Learning (IML '17). Association for Computing Machinery, New York, NY, USA, Article 35, 1-8.

[15] J. Yang, L. Zhang and X. A. Wang, "On Cloud Computing Middleware Architecture," *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, 2015, pp. 832-835, doi: 10.1109/3PGCIC.2015.46.