IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-7, July 2019 E-ISSN: 2347-2693

Cloud Security Based on PaaS Model

Saroj Kumar[1*], Santosh Kumar[2]

[1,2]Dept. of Computer Science and Engineering, Maharishi University of Information Technology, Lucknow, India

Corresponding Author: saroj.kumar999@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i7.378385 | Available online at: www.ijcseonline.org

Accepted: 12/Jul/2019, Published: 31/Jul/2019

***Abstract*-**Paas provide consumers easier way to produce and deploy software and cloud infrastructure [4], thus Paas doubtless occurs the best impact over any other aspect of cloud computing because it brings custom software development to the cloud. National Institute of Standards and Technology describes Paas as: "The capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider."[2]. Thus Paas security which is based on framework, environment, interface and different elements with connected data security. In this paper a secure model is proposed with is based on tokenization and masking technique with key management system. This paper conjointly fulfils the SPI service delivery model and FISMA ACT for PAAS security problems in any cloud service.

***Keywords*—**Paas[1], SPI Model[5], Framework Security[7], FISMA[6], Component Security[8], Security[10], Tokenization of sensitive data[13], Interface Security[11], Sensitive Data, Trusted Compute Pools[12].

I. INTRODUCTION

PaaS provides developers with easier ways to make and deploy software onto cloud infrastructure. Those "easier ways" generally exist as GUIs, sandboxes, programming languages, shared services, APIs and different online tools for software developers. The National Institute of Standards and Technology (NIST) describe three ways to deliver cloud computing capabilities: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Of the three cloud service delivery models, PaaS typically generates the most confusion; although it doubtless offers the best impact over the other side of cloud computing as a result of it brings custom software development to the cloud. Using PaaS, it's attainable to save lots of various bucks on one, large-scale software development project. Developers will produce and deploy software quicker. Agencies will lower their risks, promote shared services and improve software security via a typical security model. Information centers will leverage PaaS to create their infrastructure a lot if valuable. PaaS will lower the ability necessities to engineer new systems and might lower risks by taking advantage of pretested technologies. It has been said that an order-of-magnitude in economics can amendment an industry.

PaaS comes in several shapes and sizes:

- **Google is** presently dominating the consumer application platform with its Apps Engine.
- **Salesforce.com** is rising as a significant player within the enterprise application platform space.
- **SaaS Maker** provides integrated development tools, shared services and open interfaces.
- **Amazon's Elastic Beanstalk** provides sandbox capabilities on Amazon's infrastructure.
- **Heroku** provides machine controlled scaling and application management services.
- **Azure** provides enterprise infrastructure and database services by approach of APIs.

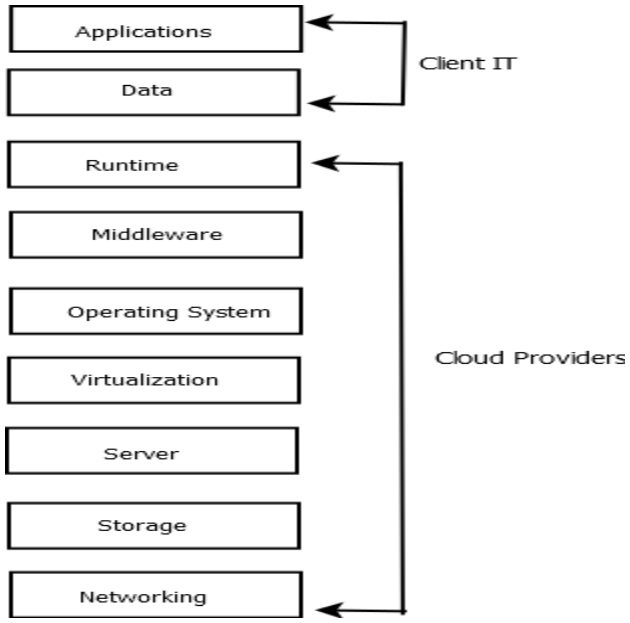

FIG 1. Paas Model with CSP responsibilities

II. SECURITY ISSUSES IN PAAS MODEL

Cloud computing could be a model for information and services by using existing technologies. It uses the web infrastructure to permit communication between client side and server side services/applications. Cloud service providers (CSP's) exist between clients that provide cloud platforms for their customers to use and build their own internet services. When making decisions to adopt cloud services, privacy or security has forever been a serious issue. To modify these problems, the cloud provider must build up ample controls to provide such level of security than the organization would have if the cloud were not used. The major security challenge is that the owner of the data has no management on their information processing. Owing to involvement of many technologies as well as networks, databases, operating systems, resource scheduling, transaction management, concurrency control and memory management, various security issues arises in cloud computing.

Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders.
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking.
- Unknown Risk Profile

Our research is to concentrate on Insecure Application Programming Interfaces, Data Loss/Leakage their risks and solutions for this. The basic security Issues involve securities at four level.

- Environment Security
- Component Security
- Framework Security
- Interface Security

III. PROBLEM STATEMENT

Our research focus is to provide a solution for the threats that are the major issue for anyone when they want to adopt cloud services for their work. For this purpose, a framework ought to be designed for execution of data and information securely in cloud environment. It will protect user's data, messages, information against various attacks.

IV. PURPOSED SYSTEM

API's are the interfaces that customers use to move with cloud services, for secure processing, interfaces must have secure verification, access control, encryption mechanisms particularly when third parties begin to build on them. For this purpose we need to analyze:

- Security model of cloud provider interfaces.
- Ensure sturdy authentication and access controls are enforced in performance with encrypted transmission.
- Perceive the dependency chain associated with the API.

Furthermore once data deleted none backup or encoding key loss/unauthorized access, data is usually at risk of being lost or stolen. To provide solution for this, we need to:

- Implement fault free API access control.
- Mechanism used for encryption and protection of data ought to be secure.
- Data protection analysis done at both design and run time.
- Provider backup and preservation methods must be outlined.

We concentrate on summarized details of what cloud computing is, its various models concerning to services and deployment ,main security risks and problems and to propose a possible solution that may offer a lot of security to data of customers from that are presently within the cloud computing services.

a) Component Security

Platform as a service contains basically three forms of components as follows:

1. Client Capabilities
2. Cloud Computing Services
3. General Purpose Support Services

b) Security of Paas Components:

1. Client Capabilities: Client capabilities can increase by browser based development tools such as Google Web Toolkit, Google Gadgets.

2. Cloud computing services: Cloud computing services can be increased by different tools such as Google App Engine etc.

3. General Purpose support services: These services provide a database, a web application runtime environment, and typically support internet services for integration. These services are secured by internet service tools such as GAE Data store, GDate.

c) Framework Security:

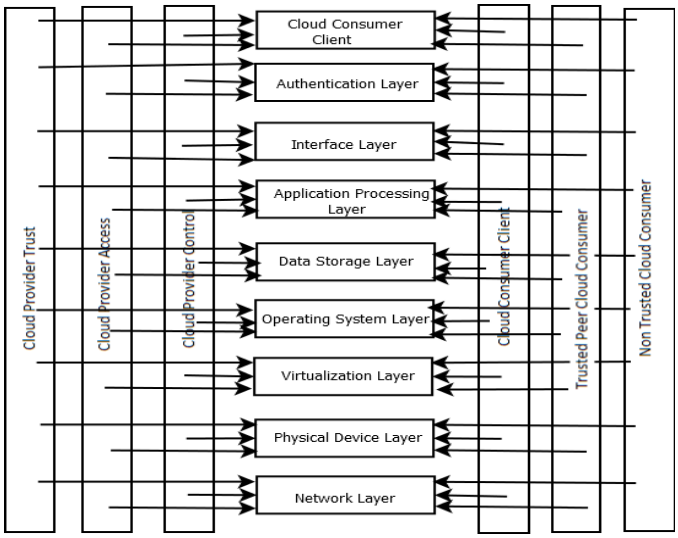

FIG 2. Secure Paas Framework

V. PAAS Framework

In this Proposed Cloud PaaS Model Framework which follows FISMA (Federal Information Security Management Act(2002)). In this cloud service provider is providing an application platform service with provider control of the infrastructure, operating system and database layer. The provider shares it access with peer cloud consumers on process layer and interface layer. It shares the control on layer 8 and 9.

a. Environment Security:

Environment Security not only solely focuses the data security but also the security management functions in context to delivery models.

Security, data security becomes a lot of vital when using cloud computing at all "levels": but significantly at Iaas And Paas platforms. The different aspects of data security include

1. Data in transit: In data in transmit it is secured using the security protocols over the network. such as SSL,TLS,HTTPS.
2. Data at Rest: In Paas model it is not useful to encrypt that data at rest because encryption would prevent indexing and searching of data.
3. Processing of data in multitenancy environment: Data will be unencrypted till the least part of its life cycle. By using homorphic encryption permit data to be processed without being decrypted.

Data Provenance: It means that not only the data integrity but also the computationally. In data

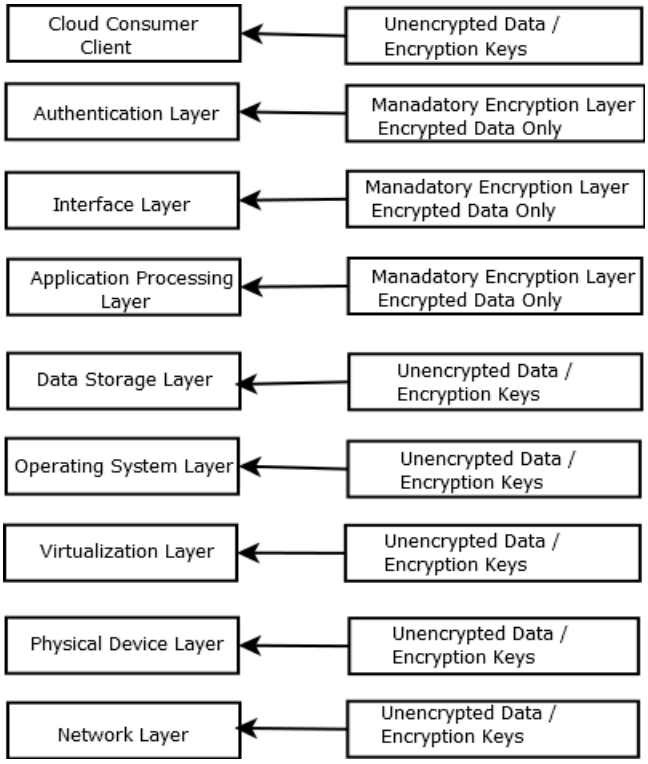

FIG 3. Secure Environment for Paas Model

4. Provenance security can be provided either by authorization or by authentication.
5. Data lineage: It means mapping of data flow from one path to another or Data Path Visualization. In this security is provided by claim based access control such as Geneva as Microsoft Windows Azure.
6. Data reminisce: Residual representation data, such as data in trash or Recycle bin. In the data reminisce security is provided Clearing and Sanitization.

TABLE 1. Functions of CSP over Public Cloud and Private Cloud

	Public Cloud	Private Cloud
PaaS (platform as a service)	The following are limited to customer applications deployed in PaaS (CSP is responsible for the PaaS platform): •Availability management • Access control •Vulnerability management •Patch management •Configuration management • Incident response •Monitoring system use and access	The following functions typically managed by your IT department or managed services: •Availability management •Access control •Vulnerability management •Patch management •Configuration management • Incident response •Monitoring system use and access

VI. PAAS AVAILABILITY MANAGEMENT

In a typical PaaS service, customers (developers) build and deploy PaaS applications on top of the CSP supplied PaaS platform. The PaaS platform is typically built on a CSP owned and managed network, servers, operating systems, storage infrastructure, and application components (Internet services). The customer PaaS applications are assembled with CSP-supplied application components and, in some cases, third-party web services components (mash-up applications), availability management of the PaaS application can be complicate for example, a social network application on the Google App Engine that depends on a Facebook application for a contact management service. In that mashed-up software deployment architecture the onus of availability management is shared between the customer and the CSP. The customer is responsible for managing the availability of the customer developed application and third-party services, and the PaaS CSP is responsible for the PaaS platform and any other services supplied by the CSP. For example, Force.com is responsible for the management of the AppExchange platform, and customers are responsible for managing the applications developed and deployed on that platform.

By design, PaaS applications might believe on other third-party web services components that don't seem to be a part of the PaaS service offerings; thus, understanding the dependency of your application on third-party services, including services supplied by the PaaS vendor, is important (e.g., your web 2.0 application using Google Maps for geo mapping). PaaS providers may also offer a collection of internet services, including a message queue service, identity and authentication service, and database service, and your application may depend on the availability of those service components (an example is Google's BigTable). Hence, your PaaS application availability depends on the robustness of your application, the PaaS platform on which the application is made, and third-party internet services components.
End consumer responsibility: In Paas application customer ought to analyze the dependencies of third party internet services. Such considerations are as follows:

1. PaaS platform service levels: End consumer should carefully review the terms and conditions of cloud service provider SLA.
2. Third party internet services provider service levels: it is troublesome to grasp the SLA if PaaS application depends on third party levels.
3. Network connectivity parameters for the network platforms; End consumer ought to verify the Latency and QoS factors.

- Access Control

In PaaS model, the cloud service provider is responsible for managing access control over the network. cloud service consumers are responsible for access control to the application deployed on a Paas Platform. Users access control is sufficient due to dynamic variation on the cloud. So it is conceivable for cloud service provider to offer a standard API just like OAuth and Federation standard like as SAML (Security Assertion Markup Language).

1. Vulnerability management: Vulnerability management is a crucial threat management component to assist shield hosts, network devices, and applications from attacks against known vulnerabilities.
2. Patch management: Patch management may be a very important threat management component in protecting hosts, network devices, and applications from unauthorized users exploiting a known vulnerability.
3. Configuration Management: Configuration management is another vital threat management practice to protect hosts and network devices from unauthorized users exploiting any configuration weakness.

- PaaS VPC management

PaaS VPC management focuses on VPC management in the CSP-managed infrastructure, also the customer infrastructure interfacing with the PaaS service

I. PaaS provider responsibilities:

The PaaS CSP is responsible for VPC management of the infrastructure that is operated by the CSP, as well as third-party services that they will suppose. The subsequent list represents SaaS VPC scope:
• Systems, networks, hosts, applications, and storage that are owned and operated by the CSP
• Systems, networks, hosts, applications, and storage that are managed by third parties
• Personal computers and smart phones owned by the PaaS workers and contractors

II. PaaS client responsibilities:

PaaS customers are also chargeable for VPC management of their systems that interface with the PaaS service. These systems include:
• Personal computers of a PaaS user
• Browsers used for accessing the PaaS service
• Applications placed at the customer's premises that interface with the PaaS service.

- Intrusion Detection and Incident Response

Intrusion and incident management are basic functions within a corporate information security management domain to mange and mitigate risks, including loss of intellectual property, regulatory non-compliance, brand erosion, and fraud
ISO 27002 provides the subsequent management for incident response and detection:

1. Reporting information security events and weaknesses
2. Management of data security incidents and enhancement.

I. Monitoring use ca

TABLE 2. Instrusion detection & Incident Response

PaaS Model	Provider responsibilities	Consumer Responsibilities
Instrusion detection	Monitoring shared network/system/ application/database infrastructure, including a PaaS platform runtime engine and supported services; e.g., a privilege escalation attack on a PaaS runtime engine	Monitoring intrusions of applications deployed on a PaaS platform. Ex NIDS
Incident Response	Notifying the customer about intrusions specific to their applications and data or when their users are compromised	Informing the affected users (internal and external) • Responding to the incident by performing forensics and remediating the application

To manage the availability of your application you will have to measure, monitor, and manage service levels from your perspective. In cloud environment four types of monitoring ought to be done

1. Network monitoring: Cloud service Providers responsibility
2. Host monitoring: Cloud service Providers responsibility
3. Database monitoring: Cloud service Providers responsibility
4. Application monitoring: Monitor application logs for vulnerabilities.

Data Life Cycle: Data life cycle refers to the complete method from generation to destruction of the data. The data life cycle is split into seven stages.

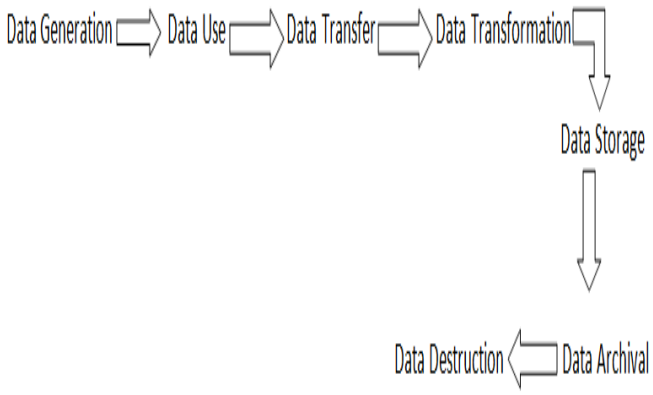

FIG 4. Data Life Cycle

TABLE 3. Data Life Cycle Vs Security Mechanism

Data Life Cycle	Security Mechanism
Data Generation	Privacy Policy, Access Control List
Data Use	Homomorphic Encryption
Data Transfer	Privacy Protection Framework
Data Transformation	HTTPS, SSL, TLS
Data Storage	Tokenization, Encryption Algorithm, Client Based privacy management tool
Data Archival	Single Sign on, Claim Based access control
Data Destruction	Complete, Santization

Interface Security:

Interface Security: (Securing API) APIs are the front entrance into any application and it is critical that they are properly secured. In some ways, API security for cloud applications is analogous to API security for internet applications hosted in information centers. For securing API multiple functions are outlined as follows

TABLE 4. Paas API Security

Paas API	Security
Web Application API	Authenticated Secure socket layer(SSL)
File Based API	Single Sign on(OAuth2)
Block based API	Host based IDS
Other API	Threat Security model, Secure SDLC Model

Description -

Trusted Compute Pools (TCP), conjointly stated to as trusted pools, is either physical or logical groupings of calculate resources/systems in an information center that share a security posture. These systems offer measured verification of the boot and runtime infrastructure, typically the BIOS and VMM/Hypervisor or OS using protocols and ways as represented in the TCG (Trusted Computing Group) standards and the NIST Interagency Report 7904 for measured launch and trust verification. The measurements are kept in an exceedingly trusted location on the system (usually a TPM) and verification happens when an agent, service or application requests the trust quote from the TPM. The measurements will then be validated via a verification service or system that verifies the measurements against well- known smart values also validity of the signature of the quote. The employment and propagation of the "Platform Trust" attribute(s) by datacenter/cloud management and security systems permit for the establishment of Trusted Compute Pools which will be assign workloads/applications to trusted systems also to audit of the trust for a given system. TCP is used to aggregate trusted systems and segregate them from untrusted resources, which ends within the separation of higher-value, sensitive workloads from commodity applications/workloads.

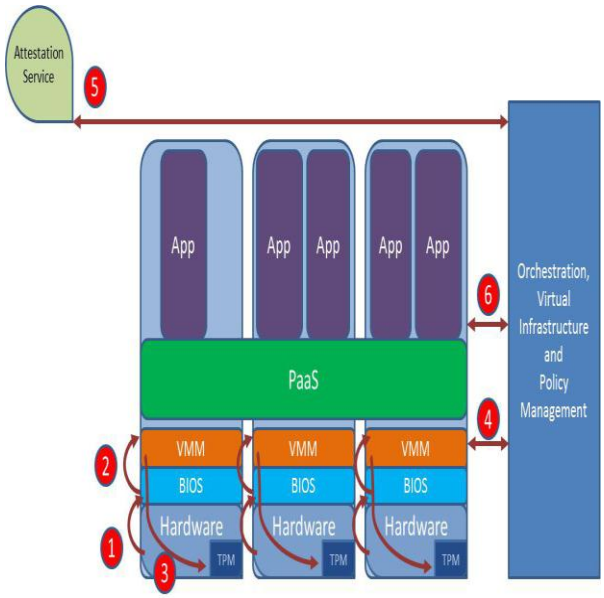

FIG 5. Trusted Compute Pools[12]

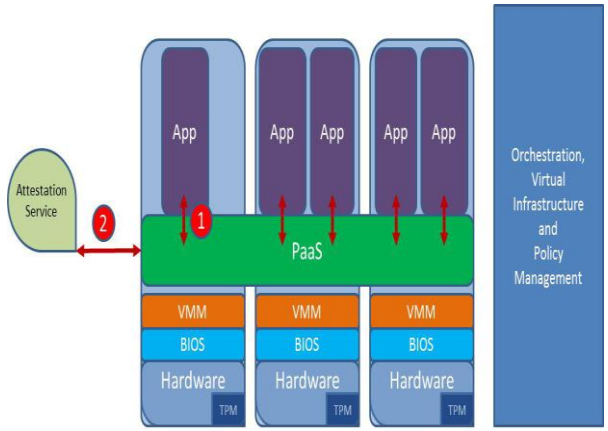

FIG 6. Trusted Compute Pools and Paas Applications[12]

VII. OTHER SECURITY

- Security of sensitive data:
- Sensitive Data

Data is taken in to consider sensitive if it must not be created known to the overall public and should only be made known within a specific context. Data may be deemed sensitive by a company, an industry or a government and every of these entities would specify the necessities for a way to handle and protect the sensitive data. Examples of sensitive data include:
• Intellectual Property (IP) and alternative business sensitive data (e.g., client lists)
• Payment Card Industry (PCI) information such as a credit card number
• Personally Identifiable Information (PII) such as a U.S. Social Security Number (SSNs), and
• Protected Health Information (PHI) such as medical records

Depending upon the sort of sensitive information and the necessities for protecting that data, it may not be possible to generate or store the data within cloud environments. For example, an organization may not wish to generate and store intellectual property in a cloud environment not under its control. There may also be government or regional requirements that may prevent sensitive data from being stored outside the boundaries of the country of origin and would limit the data to be generated and keep at within a cloud environment that is operating in that country of origin.

- Tokenization of Sensitive Data
- Tokenization

Tokenization was at the start introduced by the Payment Card trade as a way to save credit card information; however tokenization is currently used to protect all types of sensitive information. In an example tokenization solution, the sensitive data (e.g. credit card number) is encrypted when it is created or captured and transmitted to a secure central system. The system generates a substitute worth for the sensitive data, well known as *token* that is used as a replacement for the sensitive data within the environment in which it is processed and kept. Tokens are also be single-use or multiple-use and that is chosen relies on the nature of the sensitive data being replaced and whether or not the sensitive data must be tracked because it is passed within the environment.

Development of Cloud Applications
The sensitive data is secured within the central system which might be protected with multiple layers of protection and acceptable redundancy for disaster recovery and business continuity. Access to the sensitive information may be restricted to applications within the environment that need to process the particular sensitive data. There in case the token may be changed at the central system for the corresponding sensitive data.

Multiple preparation choices exist for tokenization solutions. Tokenization may be offered as an on-premise solution one deployed within a merchant environment or it is going to be offered as a service (SaaS) by a provider like a payment processor.

Advantages of the tokenization approach include:
• Reduction within the risk of exposure of the sensitive information, since it is resident in fewer places.
• Systems that don't contain the particular sensitive information might not have to be compelled to go with data protection necessities defined by organizational, industry and government regulations.
• The impact to applications to support tokenization is commonly a lot of but that of alternative data protection ways (e.g. encryption), since the token size and format may be adjusted to suit the existing data fields of the sensitive data being replaced.

1. Token Generation

Tokens should be generated employing a technique wherever somebody is in possession of solely the token it is computationally unworkable to recover the sensitive data that the token represents. Techniques used to generate tokens include the use of cryptographic algorithms or unidirectional irreversible functions (e.g., hash functions). Token generation implementations are ordinarily configurable giving the token size and format to be adjusted to satisfy the information format and schema necessities of the application into that the token are substituted for the sensitive data.

2. Token Mapping

To access the sensitive data related to a token, a mapping between a token and also the sensitive data needs to be maintained. This mapping table is generally kept within the same system wherever the sensitive data is firmly kept to confirm that appropriate protections are also applied to the mapping data itself. When the sensitive data have to be compelled to be retrieved the token is provided and used as an index into the mapping table to seek out the link to the associated sensitive data.

3. Data Masking

Data masking is an approach that disassociates data from the context or the identity that creates the information sensitive. In distinction with tokenization, that replaces entire items of sensitive data, data masking techniques involve commutation or obfuscating parts of a data set. Data masking is an approach that typically utilized in pre-production check system or in systems used to rectify a software application wherever one most work with a representative data set, however does not have to be compelled to have access to actual sensitive data. This approach permits the check and rectify systems to be exempt from sensitive data protection necessities.

- Data Encryption and Key Management
- Data Encryption:

Encryption is the most pervasive means that of protective sensitive information and will be applied in multiple eventualities. Encryption applied as data is moved within a scenario is stated as *data-in-motion* (or *data-in-transit* or *data-in-flight*), while encryption applied to the information resident within an application or infrastructure element is stated as *data-at-rest*. Data-in-motion and data-at-rest solutions may be enforced in multiple ways.

Data-in-motion is generally provided via secure communication protocols like as TLS/SSL or IPSec. Within cloud environments secure communications are often provided as part of the infrastructure, protecting data as it as it moves between infrastructure components, and as it passes between the enterprise and the cloud provider and contrariwise.

Data-at-rest solutions are a lot of varied since data also projected in multiple forms depending upon how it is being created, processed and stored within an environment. Within an application, data may be placed in a database or in a file, so encryption schemes that encrypt data within a database or which encrypt files may be used. In different approach, information will be encrypted as it is written to storage. This encryption will occur at the data departs the end users, in a switch within the network, or the complete disk in the storage array ought to be encrypted. Define the range of the data-at-rest implementations, these solutions is also on the market as part of the infrastructure or as part of an application running within the cloud.

VIII. CONCLUSION

Paas save countless dollars on one, large-scale software development project. Paas will create infrastructure a lot of valuable that may lower the skill requirement to new engineers and might lower risk by taking advantage of technologies. Thus Paas security is incredibly necessary relating to all kind of functionality of cloud computing. in this paper as we proposed tokenization and masking approach that fulfill the security issues of FISMA Act and SPI service delivery model additionally as National Institute of Standards and Technology. Thus this secure model can fruitful for cloud model developers over worldwide and additionally as researchers for future concern in cloud computing security objectives.

REFERENCES

[1] Ankit Kumar Singh, Saroj Kumar, Abhishek Rai "Secure Cloud Architecture based on YAK and ECC" International Journal of Computer Applications (0975 – 8887) Volume 90– No.19, March 2014.

[2] The NIST Definition of Cloud Computing, Special Publication 800-145

[3] Gartner® Says 2011 Will Be the Year of Platform as a Service, March 14, 2011, Gartner Newsroom.

[4] Sosinsky B, Cloud Computing Bible. 1st ed. Wiley; 2011.

[5] S. Subashini and V. Kavitha, "A Survey on Security Minimal issues in service delivery models of cloud computing" Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[6] Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA).

[7] Ayesha Malik, Muhammad Mohsin Nazir "Security Framework for Cloud Computing Environment: A Review" Journal of Emerging Trends in Computing and Information Sciences, ISSN 2079-8407, VOL. 3, NO. 3, March 2012.

[8] A. Buecker, M. Borrett, C. Lorenz, and C. Powers. Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security. *http://www.redbooks.ibm.com/redpapers/pdfs/redp4614.pdf*.

[9] Deyan Chen, Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 International Conference on Computer Science and Electronics Engineering.

[10] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory and implementation. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the

16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 43.54. [doi:10.1145/1655008.1655015].
[11] Practical Security Stories and Security Tasks for Agile Development Environments; http://www.safecode.org/publications/SAFECode_Agile_Dev_Security0712.pdf.
[12] NIST Interagency Report 7904: Trusted Geolocation in the Cloud: Proof of Concept Implementation (Draft) http://csrc.nist.gov/publications/drafts/ir7904/draft_ nistir_7904.pdf.
[13] Tokenization: What's Next After PCI?, 2012, EMC Corporation http://www.emc.com/collateral/white-papers/h11918-wp-tokenization-rsa-dpm.pdf.
[14] F. Hao."ON ROBUST KEY AGREEMENT BASED ON PUBLIC KEY AUTHENTICATION" Proceedings of the 14th International Conference on Financial Cryptography and Data Security, Tenerife, Spain, LNCS 6052, pp. 383-390, Jan 2010.
[15] Arjun Kumar, Byung Gook Lee,Hoonjae Lee,Anu. "SECURE STORAGE AND ACCESS OF DATA IN CLOUD COMPUTING " IEEE 2012 P.336339.
[16] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.
[17] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, JinLi ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol.22, No. 5, 2011
[18] S. Kamara and K. Lauter. Cryptographic cloud storage. In Financial Cryptography and Data Security (FC'10), volume 6054 of LNCS, pages 136{149. Springer, 2010
[19] http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
[20] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCC, Bangalore 2009, pp. 109-116.
[21] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues in Cloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.
[22] Ruj S, Nayak A, Stojmernovic I. DACC: distributed access control in clouds. 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, IEEE Computer Society, 2011: 91-98
[23] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." IEEE Xplore, pp 23-31, Jun. 2009
[24] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 201
[25] G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551,
[26] Security Alliance (CSA) "Security Guidance for critical Areas of Focus in Cloud Computing" ,April 2009
[27] Sze Ming Chow "New Privacy Preserving Architecture for Identity/Attribute Based Encryption" ,New York University 2010.
[28] Kaufman, Lori M. "Can public-cloud security meet its unique challenges?."Security & Privacy, IEEE 8.4 (2010): 55-57.
[29] Ren, Kui, Cong Wang, and Qian Wang. "Security challenges for the public cloud." Internet Computing, IEEE 16.1 (2012): 69-73
[30] Bao Zhang, Changgen Peng, Zhipin Xu "Identity-based distributed cloud storage encryption scheme", IEEE 2011, pages 610-614.

Authors Profile

Mr. Saroj Kumar, PhD Scholar from Maharishi University of Information Technology, Lucknow had completed his M.Tech form NIT – Allahabad and served more than 10 year in academic in different colleges in India.

Dr. Santosh Kumar, Associate Professor and Head, Maharishi School of Computer Science in Maharishi University of Information Technology, Lucknow. Serving more than 10 year in Academic Field and Guided more than 10 PhD Scholar in Computer Science Department

