International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

Security and Privacy Issues in Cloud Computing Environment

Dr. S. S. Manikandasaran
Director,
Christhuraj Institute of Computer Applications,
Tiruchirappalli, Tamil Nadu, India

K. Balaji
Research Scholar,
Dept. of Computer Science, Christhu Raj College,
Panjappur, Tiruchirappalli, Tamil Nadu, India

Abstract- **Cloud computing is a paradigm which is providing rent based service for the on-demand request for cloud users. It reduces a large amount of investment for many organizations. Cloud environment plays a vital role in minimizing management effort for computational, storage of data, and other services. Cloud environment facilitates anything as a service for consumers. Many organizations move towards cloud computing environment for outsourcing their business through the internet at the same time major issues are available in different service levels. Many types of research are going on in different levels. One of the major issues is security and privacy. This paper presents a review of issues in cloud and summarizes security and privacy related issues and also discusses different techniques used for securing the cloud. The motivation of this paper is to provide some useful background information for organizations considering the cloud computing environment to take advantage of this new computing paradigm.**

Keywords- Cloud Computing; Services; data security; privacy; confidentiality; availability; Cryptography;

I. INTRODUCTION

Cloud computing technology is providing a flexible and dynamically, scalable computing infrastructure for many applications. This recent technology totally reshaping the entire information technology field and occupied a good position in the marketplace because of the service provides the on-demand request from the consumer the concept of pay-as-you-use flexibility, if the consumer need not tie up with the cloud provider, at any time withdraw their connection. So this provision helps to many organizations for reducing the cost and also an avoiding large investment. A small scale industry getting business from outsourcing market with the minimum period of time the organization can't invest servers, software's, computers and so on. The cloud computing environment satisfies all the organization needs where they want to do business. This technology gifted for many consumers. The only thing is the organization connected through internet facility with a broad access network.

According to NIST (National Institute of Standards and Technology) defined cloud computing as:" a model for enabling ubiquitous, convenient , on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [1]. From the NIST definition of cloud computing describes five essential characteristics of on-demand self-service, Broad network access, resource pooling, rapid elasticity and measured services are enabled.[2]

A. Five essential characteristics of cloud computing:

- *On-demand self-service:* It refers to the service provided by cloud vendors that enable the provision of cloud resources on demand whenever they are required.
- *Broad network access:* It refers to resources are available for access from wide range of devices (i.e.) Smartphones, tablets, computers etc.)
- *Resource pooling:* It is a set of resources available for different locations with shared pool data centers including storage, processing, memory, and network bandwidth.
- *Rapid elasticity:* It provisioning scalable services for computer resources. The consumer can be expanding the quantity at any time without restrictions.
- *Measured Services:* It refers the cloud providers can monitoring the services for storage, processing, bandwidth and billing for effective use of resources.

B. Deployment models in cloud computing:

- *Private Cloud:* A private cloud is built within the domain of an intranet owned by a single organization. The organization owned and managed its access limited the owning partners.
- *Public cloud:* A public cloud is built on the Internet and can be accessed by any users, and resources are controlled by service providers. Many public clouds are available (e.g. Google App Engine (GAE), Amazon web services (ASW), Microsoft Azure, IBM Blue Cloud, and Sales force.com's Force.com) for commercial providers that offer publicly.
- *Community cloud:* A community cloud is a collaborative shared between several organizations from same community with specific requirements. (e. g. such as schools within University).
- *Hybrid cloud:* A hybrid cloud is built with both public and private clouds. A hybrid cloud provides access to clients with the partner's network and third parties.

C. Service models in cloud computing:

- *Infrastructure –as-a- Service (IaaS):* The service enabling user to use virtualized IT resources for computing, storage, and networking. The user can deploy and run his application over OS environment. The user needs not to control the cloud infrastructure, but control over the OS, storage, and deployed applications and networking components. This service encompasses

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

storage as a service, compute instance as a service, and communication as a service.

- *Platform – as-a- service (PaaS):* This model enables users to develop and deploy their user applications. The PaaS integrates of both hardware and software infrastructure. The user's application can be developed on virtualized cloud platform using some programming languages and software tools supported by the service providers. (e. g. java, Python, NET). The user needs not to manage service, the cloud provider supports user application development and testing on a well-defined platform.
- *Software – as-a- service (SaaS):* This model enables browser initiated application software over thousands of cloud customers. The SaaS provides software applications as a service the customer can use the licensing software with minimal investment. This model facilitates the reduction in software cost and enables all up do date updates are provided by the cloud service provider. The customer can utilize the services and need not to buy the new software. The end user can also benefit from software maintenance because of the service provider takes the responsibility of software updates and current versions. This model facilitates scaling up of applications based on user needs [3].

II. RELATED WORK

Ankit Grover et al. [4], authors proposed a new model used for data compression before encryption enhancing faster encryption due to reducing the size. The AES algorithm used for encryption and compression of data using Blowfish algorithm used. In the result, the security approaches so far not considered. The approach used for time and space required into account.

Priya Anand et al. [5], the authors describes Pattern-Based-cloud framework for security and privacy. This model proposed various ways for getting connecting in a cloud environment. The model enables security authentication protocols to prevent unauthorized access to the client's data stored in a cloud server. The secure connections established between both ends. In result, Pattern-Based-approach anyone can easily understand without experience in the field of IT security to get a good understanding of security requirement and ways to implement it. The benefits of this model for system designers while developing or maintaining the software. This model provides an idea to connect security patterns in a cloud computing environment.

Ali azougaghe et al. [6], author provide a simple, secure and privacy-preserving architecture for inter-cloud data sharing based on an encryption/ decryption algorithm. The proposed model aims to protect the data stored in the cloud from the unauthorized access. The AES algorithm used for encryption, and encrypted files stored in the server using ElGamal algorithm. The results are to improve the security of the storage of data and data security. The unauthorized user intentionally captures the data but can't decrypt it.

Xiaolong Xu et al. [7], the authors proposed the model of distributed virtual machine agent provides unique and credible monitoring of virtual machines for a cloud user. This model addressed the issues of data availability and integrity. The proposed model focuses on solving problems that remote data integrity verification at the system level, virtual machine agent mechanism applied to system security, stability, and reliable data storage, and update, audit and security attacks. This model also provides virtual machine agent audit layer between user virtual machine and hypervisor. The virtual machine can copy a pre-configuration virtual machine image with the specific requirement. The virtual machine proxy (VPA) required a unique sign, composed of the unique serial number from cloud service provider and user sign enables the cloud system track the location identification. The VPA mechanism is used to data upload, authentication, and authorization, update and data integrity verification in the cloud data storage system. The technology optimizes the allocation of resources, and improves the efficiency of resource utilization.

Napoleon Paxton [8], author reviews of three critical cloud security threats i.e. data breaches, Hijacking of accounts and multitenancy. The data breaches protected encryption and key management technique is used where unauthorized users will not be able to access the unencrypted data, used by data loss prevention (DLP) tools. The account Hijacking prevent by multi-factor authentication is used to secure the authentication is recommended. The multitenancy threats issues addressed by API have been created to proper segmentation, isolation, and protection for tenant resources.

Sunny Singh et al. [9] authors present only privacy issues associated with the cloud environment. The major privacy issues to be addressed and also he provides extracted the privacy principles, about the existing framework. The extracted privacy principles are concerns related to the cloud computing, this will help cloud service provider to serve better way. In future, all the extracted privacy principles coupled together to create a new framework which helps to prevent the transparency issues.

Rachna Jain et al. [10] proposed homomorphic encryption technique is used. The work carried out only for data security issues. The model performed on cipher text and to generate an encrypted result which will be same as result of operations performed on the plaintext when decrypted. This model enables three phases. The first phase deals with the process of encryption of data at client machine used by homomorphic encryption. The second phase deals with the equality testing on the authentication server. The third phase deals with decryption at the client side. This technique benefits the authorized person can allow all the phases. In result, observed data traveling over the network and stored on the server side is encrypted and safe. The work is done only fully homomorphic encryption (FHE) scheme, in future, the work carried out the combination of string and integers.

Mehdi Hojabri et al. [11] proposed Kerberos authentication service model to prevent cloud data storage security and manage user's data. The authors introduced third party auditing with Kerberos in cloud computing server. The ticket-granting algorithm used to authenticate on a network. The session key used to encrypt data streams over on IP network. The user wants to connect with cloud data, they

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

should register with the third party. Once the registration completes the user gets ID and hashed password to connect with the cloud environment. The user register in the third party it should send the requested access for a ticket-granting it sends user's ID to the authentication server. The TGS is identifying information for the client, the requested time value, and flags that reflect the status of the ticket and request. The Kerberos operation with the use of DES algorithm to enhancing the issues of security in cloud computing.

Ting-ting Yu et al. [12] the authors focuses security issues in cloud computing environment. The security issues and countermeasures analyzed from their view the three major challenges are identified. I.e. Cloud computing security in service level, stability, and performance. The author also describes security risks and remedies taken while implementing into the cloud environment. The VM-level attacks threats arise overlooked by developers during the coding of hypervisors. The issues arise data loss during the encryption. The Hijacking of data "man-in-the-middle attack" he mitigates sharing of account credential between user and services should not be allowed, instead of multi-factor authentication is recommended. The unknown risk issues mitigated while sharing the infrastructure and network are redirected immediately by the cloud user.

Komal Singh Gill et al. [13] proposed Intrusion Detection and Prevention Systems (IDPS) over the virtual network to finds efficient solution for providing security issues in the cloud environment. This technique secures the networks over cloud environment to prevent the malicious activities. The model implemented separate hardware systems, virtualization techniques used and get the result in an efficient manner, but not implemented in the multi-tenant environment. It arises issues in data privacy and security issues.

Khalid El Makkaoni et al. [14] the authors proposed new cloud security and privacy model (CSPM) into service layers by cloud providers in all stages. This technique overcomes the confidentiality and security services. This new model describes physical and environmental security, cloud infrastructure security, Network security, data access control security and management security. In result, this model achieved to identifying the security and privacy issues, identifying threats, and ensuring availability and security of cloud services.

Aaysha Shaikh et al. [15] the authors proposed a new model for securing privacy and identity of owners and its data. The framework refers Privacy Preserving Authentication Privilege Access Data Integrity (PP-AP ADI) enhancing authorization and privilege access control. The Ciphertext Attribute-Based Encryption (CP-ABE) used for data access control with random key signature. This method helps cloud data for public auditing, file sharing, recovery and replacement in a multi-tenant environment. In the result, the data sharing, authorization, data access control threats efficiently worked, but when going for public auditing the data leak arise.

Abderrahim Abdellaoui et al. [16] proposed the multi-agents system for securing user's privacy issues when different node communicates with each other. The author described mobile cloud computing issues are arises at three levels, in that addressed mobile network security issues. To overcome this issue implements third-party agent for authenticating with different levels. In the result, the device speed up, performance efficiency and energy cost are achieved. The device is preserving with privacy and integrity of user's data.

Jun-Hak Park et al. [17] suggest a novel model and approach for cloud forensic in SaaS environment. This paper visualized collecting of digital proofs for forensics in cloud computing environment, and also possibilities of service level agreements (SLA). In that recovering and investigating of past crime is possible to analyze Intrusion Detection System (IDS) already existed, but some challenging issues are arises when storage of data, storage of location, and access data should be focused on strong technique is needed. The crimes are increased day by day in the cloud environment so that the cloud forensic recommended a strong SLA model.

Matthias Flittner et al. [18] present cloud inspector of providing more transparency for tenants in cloud systems. The interdisciplinary approaches of system design are hard to access. The virtualization technique implies losing control and transparency over data in the cloud. The cloud inspector to be implemented in Transparency- as – a Service to overcome the lack of transparency and legal issues in cloud computing. The paper addressed strong designed solution with respect to legal needs. The technique implemented in OpenStack and VM ware enables the tenants should verify their cloud instances at runtime. So that cloud inspector is highly valuable and strengthens the legal proving position of tenants, fulfill data subject rights as requested by data protection law. The accurate cloud-related failures are detected a maximum independence of auditing and reliable. In the result proved that effective less than 5% CPU overhead on compute nodes.

Bhale Pradeepkumar Gajendra et al. [19] proposed security trade-off and improve the performance of data transmission and increase the security through Third-Party Auditor and Identity-Based Encryption. The security and privacy issues concerned to data transmission, integrity control, access control, identity management, logging, and auditing etc. The security of data in cloud storage implements Identity-Based Encryption algorithm and MD5 authentication algorithm used. The first phase of IBE algorithm used for key generation, Encryption and Decryption. For authentication MD5 algorithm is used. This paper proposed the server generates the hash value of each user uploaded data by using the MD5 algorithm. This model enables user-facing software as a service application i.e. word processing, email, social networking and security application. This paper implements a new hybrid algorithm (IBE and MD5) for securing stored data. The security analysis of original RSA and Hybrid algorithm investigates Brute Force, mathematical and timing attacks. In the result, the third party auditing makes security harder and ensured security and integrity of data. It is a trusted third party go gives confidence in user's and service provider's data is safe.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

Hojjat Baghban et al. [20] introduced a new method for finding fault tolerant decreases the latency and detecting the number of faults. The Byzantine Fault Tolerant algorithm used for finds these issues. The security issues of availability, integrity, and confidentiality are achieved by improving with State Machine Replication (SMR) with Byzantine Faults tolerant algorithm. In the result, the security and fault tolerance issues are achieved initial phase itself.

Ezz El-Din Hemdan et al. [21] described data security issues where data damaged with criminals and attackers. This paper proposed a new procedure for the digital investigator and experts for investigation of cyber crimes in effective and efficient manner. The Digital Forensic is the process of collecting and extracting digital evidence when the crime is happening. The investigation of crimes looked up two sides. The cloud service provider and cloud user can save time and cost. The investigation achieved in the effective and efficient way. The digital forensics and cloud forensics to be handled and managed the digital evidence in very short time.

Bowen Tian et al. [22] proposed secured HDFS to improving data replication in Hadoop File System. A storage assurance model is developed to evaluate the quality of security to be considered in secured HDFS (SecHDFS). This model includes multiplication principle, probability theory, and combinatorics. In the result, a secure data allocation is improved storage security in heterogeneous Hadoop system and maintains the system performance.

W.Delishiya Moral et al. [23] proposed fragmentation and sole replication (FASR) technique which is improved security, replication, and availability of data. This technique to improve the security and data retrieval time compared with the traditional cryptographic model. The fragment is considered every single node is performed sole replication i.e. every fragment is replicated only once, to enhance the security. The node is through hotbed measure, and selection of node placement of other fragment is done through T-colouring technique. This technique is impacting with reducing leakages of data. In the result, FASR improved security and performance in the cloud through data retrieval time and reduce the repeated storage similar content in the cloud.

Zeineb BEN YAHYA et al. [24] proposed a new distributed access control model based on Mobile Agent. This model to achieving security services i.e. authentication, identification, confidentiality, and integrity. This model also enables reliable, adaptable, flexible and robust access control model for cloud computing environment and agents. The Multi-or BAC model allows specifying in a homogeneous framework the several security policies are initiated. The user cannot play multiple roles in the organization so that the new model introduced the concept of "Role in Organization" (RIO) to achieve the access control purposes. The results guarantee to a secure communication between the organization and satisfy the security requirements.

M.Saraswathi et al. [25] addressed An Efficient Schema Shared Approach for Cloud-Based Multitenant Database with Authentication and Authorization Framework and A Non-Intrusive Multi-Tenant Database for large scale applications. The problem identified on multitenancy- enabled SaaS application i.e. database, customization, a performance of the system and security issues to be achieved by two new proposed solutions. The first is optimizing the database schema for efficient use of space, Kerberos technique is used to achieving authentication and authorization. The second multitenant database enablement technology to supports database clustering, routing and load balancing for scalability. The optimization of the result is achieved by Filter-Based Pattern technique is used in application level and permission based pattern is used in DBMS level. This paper addressed on the theoretical level but not implemented at the system level.

R.S. Shariffdeen et al. [26] addressed the issues of peak loads and over provisioning during other timings. To overcome these issues proposed an error-based ensemble technique for workload prediction. The ensemble-based prediction algorithm is implemented in R language and used for time series and machine learning model implements in the forecast package. In the result, offline training is not possible due to workload history data not being available at the beginning of the prediction process. The auto scalar operation gets accumulate based on the user's workload requirements. The prediction method able to predict the future time horizon based on the initially available datasets. After the initial predictions, the actual data will be available for the next time periods, so that accumulate the latest actual data into the workload history and used for next forecast horizon. The prediction technique provides the best prediction results for several datasets. The proposed forecasting method should generate the forecast within a bounded time, and limit the size of the input training window.

Parathkumar Patel et al. [27] authors addressed the security issues during service delivery and reliability over the network. The new technique proposed Software Defined Network, Network Function Virtualization (SDN and NFV) integrates into Open stack cloud to minimize network attacks, and improve network services. This paper describes two different networks i.e. cloud traditional network and software defined network analyzed with network traffic in SDN improved network services. The throughput analysis made by the iperf tool, and latency analysis made by Wireshark and TCP connection. In the result SDN architecture enables more security, flexibility, capability, and functionality increases network capability using virtualize programmatic control logic.

Anitha K L et al. [28] addressed security issues and vulnerabilities in the cloud present Smart Cloud Architecture to be handled these issues. This architecture assures a customer, cloud vendors, to provide in service level agreements (SLA). The different levels of security and complexity of each level based on services to provide to customers should understand of security policies are implemented in SLA. This architecture builds a standardized way to avoiding irrespective to the providers. In the result, the user needs to register with the user details, company details with the biometric id number. The smart cloud data manager generates a token equivalent numeric value and adds a random number. The token is received by the user for login

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

and do the computations with the data. The data access control verifies the token, and authorization enables the system administrator. The features provided on data called Data Splitting for securing the sensitive data from unauthorized access by cryptographic encryption. The service provider handles a secure backup of data from the users by virtualized environment to do the computations.

Chung K wan Law et al. [29] addressed the issue of how to ensure that clouds communicate with each other effectively and efficiently. This paper introduced an InterCloud Communications Protocol (ICCP) allowed clouds to communicate with each other using a common protocol, which is Trans parenting to the applications programming interfaces of different clouds. This technique enables security functions of confidentiality and integrity. The inter-cloud communications protocol is using XML commands to support inter-cloud operations. The intercloud Gateway communicates with each other by exchanging XML-based messages of Request and Response with Version and ID attributes. The version specifies the version number of the protocol, and ID identifies the request-and-response for session identification purposes. In the result inter-cloud Gateway prototype with ICCP to be achieved for transferring securely storing and retrieving data objects.

Jiangchun Ren et al. [30] addressed the issues of security and privacy. This paper presents issues for both cloud tenants and cloud service providers (CSPs). The tenants to worry about losing the control over their codes and data hosted on the remote server. The public cloud providers having the fear that the application uploaded by tenants may carry vicious codes which may cause serious violations of security and privacy on their cloud platform. This trust issues may cause slow down the cloud deployment of public clouds and hindered the promises of cloud computing for both CSPs and Cloud consumers. The model presents Ta-TCS a novel system framework for two-phase tenants attested trust validation and trust management over the remote VMs and cloud service executions. The Minimal Trust Environment (MTE) in VMM and an Integrity verification and Report service (IVRS) hosted in the control Domain (DomO) deployed in cloud service provider side. At the tenant side deployed an Integrity Configuration and Attestation Service (ICAS) can configure and attest the integrity of service, and cloud provider can verify codes running on a guest VM by introspection. The tenants also check whether the basic platform of Domain (DomO) is trusted or not. This two-phase trust model increases the level of mutual trust between tenants and its CSPs. In the result CSP and tenants to verify the trustworthiness of remote services at runtime. This enables transparent to the guest OS, and also tenants to configure and attest their remote services to get integrity verification report from ICAS. The ICAS implemented with Trust Third-party (TTP) enables CSP to monitor and audit cloud services in VMs. The test conducted the static codes in memory; it gives the guarantee that the processes run their original codes at runtime. The transferred instruction also measured and detects some attacks of restructuring the existing codes.

Meryeme ALOUANE et al. [31] author's addressed security issues on hypervisors and proposed own model to increases security in hypervisor related to architecture. The hypervisor is the key component to the virtualization architecture to helps the provider creating the illusion of working on his own computer. The hypervisor is one of the most attacked elements in the virtualization architecture, and compromising its security gives the access to all the VMs sharing resources. The proposed hybrid architecture it gives the provider and the guest user possibilities of working any architecture based on SLA agreements. In the result, a single platform gives measured solution and answer the security request to the user, and same time provider does not lose of resources while more than one user asked the same performances. This model recommended with all possible elements in the SLA. This technique leaves the possibility of mistakes so that automatic classification of SLA is required for great benefits.

From literature study, it is observed that security and privacy are a most important concern in cloud computing environment. Many authors were tried to address this security and privacy issues using different cryptography techniques. Table 1 listed different cryptography techniques used for securing a cloud environment.

TABLE I. SECURITY AND PRIVACY TECHNIQUES USED IN CLOUD FOR SECURITY

S.No	Technique name	Observation	Advantage	Disadvantage
1	AES and Blow Fish Algorithm.	Data compression before encryption enhancing faster encryption due to reducing the size. The AES algorithm used for encryption and compression of data using Blowfish algorithm used. The approach used for time and space required into account.	• Securing the data before storing • Reduce file storage size	• Key authentication needs more secure. • Process slowly when file size is increased.
2	Pattern-Based Approach	Pattern-Based-cloud framework for security and privacy. Enable security authentication protocols to prevent unauthorized access to the client's data stored in a cloud server. The secure connections established between both ends.	•Authentication required at all levels.	An unauthorized user can easily identify without any IT experience.
3	AES and ElGamal algorithm	Secure and Privacy-preserving architecture for inter-cloud data sharing based on an encryption/ decryption algorithm. To protect the data stored in the cloud from the unauthorized access. The AES algorithm used for encryption, and encrypted files stored in the server using ElGamal algorithm.	•Unauthorized user intentionally captures the data but can't decrypt it. •Comparison with RSA algorithm, the ElGamal algorithm gives better performance.	Computational time process is high.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

4	Distributed virtual machine agent	Addressed the issues of data availability and integrity. The data integrity verification at the system level, virtual machine agent mechanism applied to system security, stability, and reliable data storage, and update, audit and security attacks. Virtual machine agent audit layer between user virtual machine and hypervisor. The VPA mechanism is used to data upload, authentication, and authorization, update, and data integrity verification in the cloud data storage system.	•Integrity verification mechanism for remote cloud combined with virtual machine agent. •Both hash values are monitored and compared while storing and retrieving data.	•The small size of data only achieved. •The size of data increases when data damage happens.
5	Homomorphic encryption	Cipher text and generate an encrypted result which will be same as result of operations performed on the plaintext when decrypted. The process of encryption of data at client machine used by homomorphic encryption, the second phase deals with the equality testing on authentication server and decryption at the client side.	•The client encrypts with the password with homomorphic and server performs equality test. •Guarantee of authorized user can access the data.	Achieved fully homomorphic data, not strings and integers.
6	Kerberos	Prevent cloud data storage security and manage user's data. The ticket-granting algorithm authenticates on a network. The session key used to encrypt data streams on IP network. The user register with the third party sends the requested access for a ticket-granting it sends user's ID to the authentication server. The TGS identifying information for the client, the requested time value, and flags that reflect the status of the ticket and request.	Authentication required at all levels.	Each user performs within in a minimum time period.
7	IDPS	Secures the networks over cloud environment to prevent the malicious activities. The model implemented separate hardware systems, and virtualization techniques used.	•Detecting and preventing attacks. •Power consumption is reduced.	In multi-tenant environment raises data privacy and security issues.
8	PP-AP ADI CP-ABE	Privacy Preserving Authentication Privilege Access Data Integrity (PP-AP ADI) enhancing authorization and privilege access control. The Ciphertext Attribute-Based Encryption (CP-ABE) used for data access control with random key signature. The cloud data for public auditing, file sharing, recovery and replacement in a multi-tenant environment.	•Support access control in the real environment. •Security consideration at files and data level. • Traceability and immediate rekeying benefits.	Public auditing data integrity may leak the privacy.
9	Multi-Agent system	Securing user's privacy issues when different node communicates with each other. Third-party agent for authenticating with different levels. The device preserving with privacy and integrity of user's data.	The device speed up, performance efficiency and energy cost are achieved.	The EA can enable to record every activity occurs diagnose problems.
10	IBE algorithm	The performance of data transmission and increase the security through Third-Party Auditor and Identity-Based Encryption. The IBE algorithm used for key generation, Encryption and Decryption. The authentication purpose MD5 algorithm used. Implements a new hybrid algorithm (IBE and MD5) for securing stored data. The security analysis of original RSA and Hybrid algorithm investigates Brute Force, mathematical and timing attacks.	•Third-party auditing ensures the security and integrity. •Safe data transmission. •Faster uploading and downloading	Computing complexity is high compared with RSA algorithm.
11	Byzantine Faults tolerant algorithm	The Byzantine Fault Tolerant algorithm used for finding fault tolerant decreases the latency and detecting the number of faults. Availability, integrity, and confidentiality are achieved by improving with State Machine Replication (SMR) with Byzantine Faults tolerant algorithm.	•Security and fault tolerance achieved initial phase itself. •Server crashes data not lost because it is available on the other machine.	Commission faults occur the message not send correctly to operating node, so faults are difficult to resolve.
12	FASR and T-colouring	Fragmentation and sole replication (FASR) improve the security and data retrieval time compared with the traditional cryptographic model. Selection of node placement of other fragment is done through T-colouring technique.	• Improved security, replication, and availability of data. • Reducing leakages of data	Parameter increase number of fragments than the nodes affects the storage and the performance.
13	Multi-or BAC	The Multi-or BAC model allows specifying in a homogeneous framework the several security policies are initiated. The user cannot play multiple roles in the organization.	Achieved security services i.e. authentication, identification, confidentiality, and integrity.	There is overhead involved in managing the distributed authorities.
14	SDN and NFV	Software Defined Network, Network Function Virtualization integrates into Open stack cloud to minimize network attacks, and improve network services. The analysis made by the iperf tool, and latency analysis made by Wireshark and TCP connection.	•Enables more security, flexibility, capability, and functionality. •Increases network capability using virtualize programmatic control logic.	Performance varies in terms of network flow, open flow, and Linux system.

III. DATA SECURITY AND PRIVACY ISSUES IN CLOUD

In cloud computing environment data security is a major concern because data is stored and delivered over the internet, the user or owner has no knowledge about where the data stored geographically. The main challenge in data security in the cloud environment includes threats, data loss, service disruptions, malicious attacks and multi-tendency issues are arises. This will leads to the data protection issues in cloud

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

storage. The major three data security is data confidentiality, availability, and integrity which lead to data loss preventions [32].

- Data Confidentiality: The protection of data from the unauthorized user. The information available only when the authorized user needs.
- Data integrity: The assurance that data received are exactly as sent by an authorized user (i.e. No modification, insertion, deletion or replay) can be provided using different encryption and decryption for securing data.
- Data availability: The information made available when the authorized user needs. It refers data available and usable upon the interest by the authorized user.

The data privacy is another security issue it refers the information privacy because all users store their data on cloud servers and to access them connected to cloud services. The information can be protected during the cloud accesses the sensitive information, management information, personal information should be considered the privacy of individual users. The major eight privacy issues take place.

- Compliance: It refers the laws, regulations, standard are framed in cloud computing data, because the law enforcement varies in different countries.
- Access: It refers the access rights of the user and the cloud service provider, it measures how much of data accessed by the user and provide the information by the cloud service provider.
- Storage: It refers the physical location where the data stored. Whether the data stored locally or geographically. Whether the cloud provider having sufficient data centers or not. Storing of data in the different location may lead to the unauthorized access.
- Retention: It refers the time. Which means that how much of time the user's access the cloud environment.
- Audit and monitoring: It refers getting assurance from the cloud service provider. This means that the user can monitor and assurance meets the privacy requirement of their personal data in the cloud environment.
- Destructions: It refers the confirmation from the cloud provider. It means that the process of deletion of personal data when the user withdraws his services from the cloud provider ensure that the data is entirely deleted and is not available to another cloud user.
- Privacy breaches: It refers unauthorized users or attackers access the data, it may result in data loss. If breaches occurred and ensure that the cloud provider will notify the user. When the breaches happen, who is responsible for managing the process of notifying breaches?
- Law: It refers the law enforcement security policies. The cloud provider should establish transparent policies so that the user can easily understand them.

IV. FINDINGS AND INTERPRETATIONS

Nowadays everyone talks about the cloud. The cloud computing is the delivery of services over the internet through a network of remote servers. These remote servers are busy storing, managing, and processing data. Many public clouds are available such as Google App Engine (GAE), Amazon Web Services (AWS), Microsoft Azure, IBM Blue Cloud, and Sales force.com. These organizations are active research and promoting their business through the cloud environment. The cloud offers benefits to users, but still, security risks are played a major role in all service levels. According to IDGs recently published, Enterprise Cloud Computing Survey 2016 found that by 2018 the typical IT department will have the majority of their apps and platform (60%) residing in the cloud. " In an effort to do everything from offer better in-store customer service to fully leverage advances in manufacturing, companies from even most traditional and change-resistant sectors are seeing the writing on the wall: Cloud technology strategies cut cost and risk"[33]. The organizations are facing challenges and how they are being addressed. The six current computing challenges are:

- Lack of resources/ expertise: Organizations are increasingly placing more workloads in the cloud while cloud technologies continue to rapidly advance. This factor influences to create better tools and also need for expertise's to handle these issues.
- Security issues: The user unable to see the exact location where the data is stored or being processed. The data breaches, authentication, hacking interfaces the APIs, account hijacking are mainly difficult to concerns the security issues. To overcome these issues to makes trusting sensitive and proprietary data to a third party auditing is required. The third party auditing helps the cloud provider and users issues are constantly improved. To ensure the organizations verify the SaaS provider has secure user identity management, authentication and access control mechanisms created with data security and privacy laws. While auditing the organization needs to frame the regulations and standards. The privacy law ensures the provider has strict data recovery and policies in place.
- Cost Management and Containment: The cloud computing provides the cost benefits. The organization can easily increase its processing capabilities without making large investments in new hardware. The cloud provides pay-as-you-go model enables public cloud providers. The on-demand and scalable of cloud computing services makes it sometimes difficult to define and project quantities and cost.
- Governance / Control: The proper IT governance is required for applying policies and procedures; ensuring that these assets are properly controlled and maintained, and ensures that these assets are supporting our organization's strategy and business goals. Nowadays IT does not have full control over the provisioning, de-provisioning, and operations of infrastructure. This factor increases difficulty for IT to provide the governance, compliance and risk management is required. To mitigate the various risks the IT must adopt its traditional governance and control processes to include the cloud.
- Performance: The organization moves to cloud it depends on the service providers. The provider should

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

serve with new and innovative technologies to users the business goes with right partnership. The performance of the organization and other cloud-based system is also tied to the performance of the cloud provider when it weakens. Make sure that provider has the right processes in place and alert if there are no issues. The SaaS provider has real time monitoring policies in place to help mitigate these issues.

- Segmented usage and adoption: Most organization did not have a robust cloud adoption strategy when they move to cloud. Instead of that ad-hoc strategy developed and run by several components, which led to altering cloud migration. The individual development teams using the public cloud for specific applications or projects. This strategy raises some additional issues: Isolated cloud projects lacking shared standards, Ad-hoc security configurations, and Lack of cross-team shared resources and learnings.

V. CONCLUSION

Cloud computing is provisioning on-demand request for cloud users. The cloud benefits many advantages in different deployment models, and service models. These services are deployed with different techniques the issues are arises such as security, privacy, storage, location, identity, boundary etc. These factors are influenced with the public cloud, private cloud, community cloud, and hybrid cloud. The cloud issues like security issues, privacy issues, risk management issues, access level issues are also identified. The service level agreement (SLA) issues and various access level issues also addressed. The Intercloud and intra-cloud standards are discussed in various perspectives in cloud interoperation in the open market. So Many organizations nowadays ready to move on to cloud environment. But still, some issues exist and must be focused. Particularly data storage in cloud server may cause data confidentiality, integrity and availability are discussed along with solutions in the literature and also addressed other security issues are given this paper. The overall motivation of this paper present the security and privacy issues and techniques related issues are identified related to cloud computing environment. This paper assures to take up to the next level of researcher drives success to the entire IT industry.

REFERENCES

[1] Mell, Peter, and Tim Grance, "The NIST Definition of Cloud Computing.", 2011, pp. 20-23

[2] ISO/IEC 17788, "Revised Final Text of ISO/IEC 17788 for ITU-T/SG 13 Review", ISO/IEC, 2014.5.

[3] Arockiam, L. and Monikandan, S. and Parthasarathy G. Cloud Computing: A Survey. International Journal of Internet Computing, Volume 1, No. 2, 2011, pp.26-33.

[4] Ankit Grover, Banpreet Kaur, "A Framework for Cloud data security", IEEE International Conference on Computing, Communication and Automation, ISBN: 978-1-5090-1666-2. 2016, pp. 1199-1203.

[5] Priya Anand, Jungwoo Ryoo, Hyoungshick Kim, " Addressing Security Challenges in Cloud Computing- a pattern-based approach", IEEE International Conference on Software Security and Assurance, , 2016, pp. 13-18.

[6] Ali AZOUGAGE, Zaid KARTT, "An efficient algorithm for data security in cloud storage", IEEE International Conference on Intelligent System Design and Application (ISDA-2015), 2015, pp. 421-427.

[7] Xiaolong Xu, Guangpei Liu, Jie Zhu, " Cloud data security and integrity protection model based on distributed virtual machine agent", IEEE International Conference on Cyber- Enabled Distributed Computing and Knowledge Discovery, 978-1-5090-5154-0,2016.

[8] Napoleon C.Paxton, "Cloud Security: A Review of current Issues and Proposed Solution", IEEE International Conference on Collaboration and Internet Computing,, 2016, pp. 452-455.

[9] Sunny Singh, Nithin Goel, " Efficient Framework Approach to Extract Privacy Issues in Cloud Computing", 2015 International Conference on Communication Systems and Network Technologies, 2015, pp. 698-701.

[10] Rachna Jain, Sushila Madan, Bindu Garg, "Homomorphic Framework to Ensure Data Security in Cloud Environment", IEEE International Conference on Innovation and challenges in Cyber Security (ICICCS-2016), 2016, pp. 177-181.

[11] Mehdi Hojabri, K. Venkat rao, "Innovation in cloud computing: Implementation of Kerberos version 5 in cloud computing in order to enhance the security issues", IEEE International Conference on Information Communication and Embedded Systems (ICICES), 978-1-4673-5788-3, 2013

[12] Ting-ting yu, Ying – GUO Zhu," Research on Cloud Computing and Security", IEEE International Symposium on Distributed Computing and Application to Business, Engineering, and Science, 2012, pp. 314-316.

[13] Komal Singh Gill, Anju Sharma, "IDPS based Framework for security in Green cloud computing and comprehensive Review on Existing Frameworks and Security Issues, IEEE International Conference on Computing, Communication and Security (ICCCS), 978-4673-9354-6, 2015.

[14] Khalid El Makkaoni, Abdellah Ezzati, Ab derrahim Beni – Hssane, Cina Motamed, " Cloud security and privacy model for providing secure cloud services", 978-1-4673-8894-8. 2016- IEEE.

[15] Aaysha Shaikh, Jayant Gadge, "Framework for the security of shared data in Cloud Environment", IEEE International Conference on Computing Communication Control and automation (ICCUBEA), 978-1-5090-3291-4 , 2016.

[16] Abderrahim Abdellaoui, Anas Laksantini, Habiba Chaoui, " A Security Scheme for Mobile Cloud using Multi-Agents System" IEEE, 2016, pp. 615-620.

[17] Jun-Hak Park, Sang-Ho Na, Jun-Young Park, Eui-Nam Huh, Chul-Woo Lee, Hyoung-Chun Kim, "A Study on Cloud Forensics and Challenges in SaaS Application Environment", IEEE 2nd International Conference on Data Science and Systems, 2016, pp. 734-740.

[18] Matthias Flittner, Silvia Balaban, Roland Bless "CloudInspector: A Transparency-as-a-Service Solution for Legal Issues in Cloud Computing", 2016 IEEE International Conference on Cloud Engineering Workshop, 2016, pp. 94-99.

[19] Bhale Pradeepkumar Gajendra, Vinay Kumar Singh, More Sujeet, " Achieving Cloud Security using Third Party Auditor, MD5, and Identity-Based Encryption", IEEE International Conference on Computing and Automation ICCCA2016, pp.1304-1309.

[20] Hojjat Baghban, Mahdis Moradi, Ching-Hsien Hsu, Jerry Chou, Yeh-Ching Chung "Byzantine Fault Tolerant Optimization in Federated Cloud Computing ", IEEE International Conference on Computer and Information Technology, 2016, pp. 658-661.

[21] Ezz El-Din Hemdan, Manjaiah D.H, " A Cloud Forensic Strategy for Investigation of Cybercrime", IEEE International Conference on Emerging Technological Trends, 2016.

[22] Bowen Tian, Yun Tian, Yijie Sun, Trevor Hurt, Brandon Huebert, Waymon Ho, Yuting Zhang, Danqi Chen " A Secure Data Allocation Solution for Heterogeneous Hadoop System: SecHDFS", IPCCC 2016, IEEE, pp. 1-8.

[23] W. Delishiya Moral, B. Muthu Kumar "Improve the Data Retrieval Time and Security through Fragmentation and Replication in the Cloud ", International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), ISBN No.978-1-4673-9545-8, pp. 539-545.

[24] Zeineb BEN YAHYA, Farah BARIKA KTATA, Khaled GHEDIRA "Multi-Organizational Access Control Model Based on Mobile Agent for Cloud Computing ", 2016 IEEE/WIC/ACM International Conference on Web Intelligence, 2016, pp. 656-659.

[25] M. Saraswathi, T. Bhuvaneswari "Multitenant SaaS Model of Cloud Computing: Issues and Solutions ", IEEE International Conference on Communication and Network Technologies (ICCNT), 2014, pp. 27-32.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

[26] R.S. Shariffdeen, D.T.S.P Munasinghe, H.S. Bhathiya, U.K.J.U. Bandara and H.M.N. Dilum Bandara " Adaptive Workload Prediction for Proactive Auto Scaling in PaaS Systems", IEEE, ISBN: 978-1-4673-8894-8, 2016.

[27] Parthkumar Patel, Vineeta Tiwari, Manish Kumar Abhishek " SDN and NFV integration in OpenStack Cloud to Improve Network Services and Security", 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), ISBN No.978-1-4673-9545-8, pp. 655-660.

[28] Anitha K L, Dr. T.R. Gopalakrishnan Nair "A Smart Cloud Architecture to handle Security Issues and Vulnerabilities in Cloud ", IEEE International Conference on Inventive Computation Technologies (ICICT), 978-1-5090-1285-5, 2016.

[29] Chung Kwan Law, Wen Xie, Zheng Xu, Yi Dou, Chin Ting Yu, Henry C.B. Chan, and Daniel Wai Kei Kwong, "System Protocols for Secure Intercloud Communications", International Conference for Internet Technology and Secured Transactions (ICITST-2016), 2016, pp. 399-404.

[30] Jiangchun Ren, Ling Liu, Da Zhang, Qi Zhang, Haihe Ba " Tenants attested Trusted Cloud Service", IEEE International Conference on Cloud Computing, 2016, pp. 600-607.

[31] Meryeme ALOUANE, Hanan EL BAKKALI, "Virtualization in Cloud Computing: Existing solutions and new approach", 978-1-4673-8894-8, 2016-IEEE.

[32] Arockiam, L. and Monikandan S. Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. International Journal of Advanced Research in Computer and Communication Engineering, Volume 2, No. 8, 2013, pp. 3064-3070.

[33] Mona Leibed , 6 Cloud Computing Challenges Businesses are Facing in these days, Jan 13th, 2017 http://www.datapine.com/blog/top-6-cloud-computing-challenges/#