Security Issues in Cloud Computing

Nischitha K C
Dept of Computer Science and Engineering
SJB Institute of Technology
Bangalore, India
nischithakc@gmail.com

Dr. K R AnandaKumar
Professor & HOD
Dept of Computer Science and Engineering
SJB Institute of Technology
Bangalore,India

Abstract: **Cloud Computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms. However, a major barrier for cloud adoption is real and perceived lack of security. By taking a holistic view of cloud computing security - spanning across the possible issues and vulnerabilities connected with virtualization infrastructure; software platform; identity management and access control; data integrity; confidentiality and privacy; physical and process security aspects; and legal compliance in cloud. By presenting and findings from the points of view of a cloud service provider, cloud consumer, and third-party authorities such as Govt. Important research directions in cloud security in areas such as Trusted Computing, Information Centric Security and Privacy Preserving Models. Finally, the set of steps that can be used, at a high level, to assess security preparedness for a business application to be migrated to cloud.**

I.INTRODUCTION

Cloud computing is fast becoming a popular option for renting of computing and storage infrastructure services called Infrastructure as a Service or IaaS for remote platform building and customization for business processes called Platform as a Service or PaaS and for renting of business applications as a whole called Software as a Service or SaaS. The cloud infrastructure has been further sub-divided into, Public cloud where the infrastructure resides totally outside of the tenant enterprises firewall. Hybrid cloud where the infrastructure and business processes reside partly within the enterprise and partly consumed from third party, and Private cloud where IT services are mounted on top of large-scale conglomerated and virtualized infrastructure within enterprise firewall and consumed in per transaction basis. The primary concerns for cloud security are around cloud infrastructure, software platform and user data as well as access control and identity management. Researchers also include broader issues of data integrity and compliance under security. Additionally physical data center security and processes play an important role.

There are three major groups involved in cloud security. First group is the providers of Public and Hybrid clouds. Second group is the individuals organizations which use cloud services either by migrating and hosting their applications binaries data to cloud, or by having an interface or a pipe connected to an external cloud to do some activities like downloading cloud public data modules or to route messages through cloud. The third group is the Government and other third-party regulatory entities that may have fiduciary roles audit, forensic etc.

Multi-tenancy and elasticity are two key characteristics of the cloud model. Multi-Tenancy enables sharing the same service instance among different tenants. Elasticity enables scaling up and down resources allocated to a service based on the current service demands. Both characteristics focus on improving resource utilization, cost and service availability.

Today Small and Medium Business (SMB) companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best business applications or drastically boost their infrastructure resources, all at negligible cost. Gartner defines cloud computing as a style of computing where massively scalable IT enabled capabilities are delivered as a service to external customers using Internet technologies. Cloud providers currently enjoy a profound opportunity in the marketplace. The providers must ensure that they get the security aspects right, for they are the ones who will shoulder the responsibility if things go wrong. The cloud offers several benefits like fast deployment, pay for use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low cost disaster recovery and data storage solutions, on demand security controls, real time detection of system tampering and rapid re-constitution of services. While the cloud offers these advantages, until some of the risks are better understood, many of the major players will be tempted to hold back. Cloud computing moves the application software and databases to the large data centers, where the management of the data and services are not trustworthy. This unique attribute, however, poses many new security challenges. These challenges include but not limited to accessibility vulnerabilities, virtualization vulnerabilities, web application vulnerabilities such as SQL (Structured Query Language) injection and cross site scripting, physical access issues, privacy and control issues arising from third parties having physical control of data, issues related to identity and credential management, issues related to data verification, tampering, integrity, confidentiality, data loss and theft, issues related to authentication of the respondent device or devices and IP spoofing.

II. COMMON CONCERNS ABOUT CLOUD SECURITY AND IMPLICATIONS

The common security issues around cloud computing divided into four main categories:
1) Cloud infrastructure, platform and hosted code. This comprises concerns related to possible virtualization, storage and networking vulnerabilities. This cover vulnerabilities that may be inherent in the cloud software platform stack and hosted code, which gets migrated to cloud. It also discuss the physical data- center security aspects here.
2) Data. This category comprises the concerns around data integrity, data lock in, data remanence, provenance, and data confidentiality and user privacy specific concerns.
3) Access. This comprises the concern around cloud access (authentication, authorization and access control or AAA), encrypted data communication, and user identity management.
4) Compliance. Because of its size and disruptive influence, the cloud is attracting attention from regulatory agencies, especially around security audit, data location; operation trace-ability and compliance concerns.

This categorization will cover almost all common cloud security issues. To provide a perspective on why these issues are important from cloud consumer enterprises, providers, and third party points of view should first lay out the paramount top-level security concerns mainly on part of consumers and third party agencies and sub levels thereof with anecdotal evidences. Then discuss the technological implications mainly on part of the cloud providers of each of these concerns and related research issues.

A. Concern C1: Is my cloud services providers physical and software infrastructure secured?

Migrating applications to cloud and hosting those in remote multi-tenant environment raise concerns like:
1) C11: Are the cloud data centers physically secured against security breaches?
2) C12: How is my application secured in shared virtualized infrastructure against malicious attacks?
3) C13: Since my application is hosted with common software stack, how does potential common-stack vulnerability affect me?
4) C14: In hybrid cloud my internal applications may interact with cloud-based ones in a common workflow. How do I ensure security isolation?
5) C15: Can I trust the APIs and interfaces provided by cloud providers?
6) C16: Since I relinquish execution control, how can it be ensured that no illegal operations happen?
Implication I1: Secure physical computing, storage and network access environment.

Typical data-center related security measures related to physical access, layouts of racks, servers and network redundancy and isolation, intrusion detection and prevention systems, backup and disaster recovery contingency, HVAC related issues are required. It is expected for sensitive and critical customers to come into public cloud, the cloud must meet these criteria adequately to address concern C11. It is often noted that major security breaches and threats come from internal staff. A stringent set of checks and audit processes are required for this purpose.

To tackle C12, the IaaS cloud providers should ensure that virtualized infrastructure is secure against anyone exploiting known and emerging vulnerabilities. These are vulnerable to exploitations and attacks. Malicious code can detect presence of a hypervisor and launch attacks such as denial of service or even exit from the protected environment to garner higher privileges. Concerns (C13, C14) around shared resources and workflow are particularly important for hybrid PaaS and SaaS providers. Active monitoring of any unexpected configuration changes and vulnerability scanning of any shared resources are required.

B. Concern C2: What happens to my data in cloud?

Data is the primary asset enterprises and individuals possess. In cloud computing, foremost concern is about data integrity, confidentiality and privacy, and provenance. There is a growing worry about the confidentiality of data stored in public cloud server side infrastructure. Unless the cached data is effectively secured and purged regularly, it can become a treasure trove for data theft. The concerns are listed as below:
1) C21: What ensures integrity and prevents loss of my data in cloud?
2) C22: Will my business data remain confidential? How do I protect privacy of my users?
3) C23: How do I prevent my data getting locked out in case the provider is likely to fail?
4) C24: How do I ensure that data is not remanent in storage ?
5) C25: How do I know that updates to my data are tracked properly and I get the correct copy each time a request is made?
6) C26: How to maintain data confidentiality and integrity where multiple cloud parties are involved in processing?
Implication I2: Ensure effective data management including integrity, confidentiality and privacy.

Data governance, including all the issues above, perhaps has most important implications for providers. C21 is relatively straightforward to address through strong encryption mechanisms like AES and DES. The management can be done through common PKI infrastructure. Labels are placed on repositories encrypted with a public key that is associated with each user. The user possesses the private part of the key and is the only one that can decrypt the labels encrypted with the public part. This form of encrypted data in cloud is good for storage or archival but is rather costly to process. However a new form of encryption called Homomorphic Encryption enables the ciphertext to be processed in public cloud without decrypting it. The common procedure of masking data for individual customer record confidentiality (C22) is data anonymization. In the context of risks such as health, research is being performed to better common anonymization techniques like k-anonymization with distributed anonymization. Several concerns like C23 can be resolved by publishing and maintaining a standard set of data interfaces and transformation logic. Storage Network Industry Association (SNIA) has suggested a set of remedial mechanism for data remanence problem C24. One of the suggestion is to encrypt the data and then shred the key Finally, device management becomes a critical function in data remanence. Things like

remote management of mobile devices, remote wipe-out or remote disabling of a device need to be factored into the cloud eco-system. C25 essentially highlights the important issue of data provenance. Cloud employs identifier based data objects such as S3 objects in Amazon cloud. Multi-cloud information processing activities (C26) like distributed data mining would require sophisticated privacy preserving models.

C. Concern C3: Are users accessing cloud- services really mine and can all my genuine users get seamless and secure accessibility?

Another fundamental cloud security concern is that of user authentication, authorization and access control (AAA). The first question is that of access management mapping of traditional enterprise directory structure like LDAP and Active Directory for providing organizational role-based access to a cloud PaaS or SaaS provider. The second question is that of identity management like authentication, identity theft and phishing. Some such concerns are:

1) C31: How do I ensure that there is no un-authorized access to my cloud by a disgruntled employee, who has left the organization or by an identity thief?

2) C32: How to ensure proper levels of authentication to cloud services? How do I manage multi-device access?

3) C33: In multi-cloud scenario, how do I ensure that I provide delegate access to users to different security domains so that the end-to-end workflow is seamless? Similarly, in hybrid cloud, how do I create a minimum common access control and identity structure?

Implication I3: Ensure proper access control and identity management.

Synchronizing enterprise and external cloud services access control lists in the context of C31 to ensure right access roles is a very important challenging issue as PaaS and SaaS platforms have complex hierarchies and many fine-grained access capabilities tenant org level, sub-tenant, and individual user levels. This assumes importance as users, who are no longer part of an enterprise, may still potentially exploit access provided in cloud unless those credentials are revoked quickly. Use of standard languages like Service Provisioning Markup Language promoted by OASIS, can enable faster user account provisioning and de-provisioning. Cloud service authentication (C32) presents some interesting problems. There is a growing chorus on 'inter cloud' hand-offs and federated identity management (C33), possibly through assertion tokens like Security Assertion Markup Language (SAML) or privilege management infrastructure based on x.509 certificates. Cloud federations need to establish a set of common security token services and identity providers.

III. ADVANCED ISSUES IN CLOUD COMPUTING SECURITY

Cloud brings out a set of unique challenges like:

A. Abstraction: Cloud provides an abstract set of service end-points. For a user, it is impossible to pin-point in which physical machine, storage partition (LUN), network port MAC address, switches etc. are actually involved. Thus, in event of security breach, it becomes difficult for a user to isolate a particular physical resource that has a threat or has been compromised.

B. Lack of execution controls: The external cloud user does not have fine-gained control over remote execution environment. Hence the critical issues like memory management, I/O calls, access to external shared utilities and data are outside the purview of the user. The client would want to inspect the execution traces to ensure that illegal operations are not performed.

C. Third-party control of data: In cloud, the storage infrastructure, and therefore, the data possession is also with the provider. So even if the cloud provider vouches for data integrity and confidentiality, the client may require verifiable proofs for the same.

D. Multi-party processing: In multi-cloud scenario, one party may use part of the data which other party provides. In absence of strong encryption, it becomes necessary for participating cloud computing parties to preserve privacy of respective data.

To build a strongly secure cloud computing model and tackle issues such as above, it is to postulate that cloud groups will need to address the issues of trust, create context specific access model within data and preserve privacy. There are three specific areas of security research namely Trusted Computing, Information Centric Security and Privacy Preserving Models and show the implications for cloud computing.

Trusted computing: It is a set technology being developed and promoted by Trusted Computing Group (TCG). To tackle the concern of un-trusted execution environment, trusted platform modules enable a strong endorsement key to attest users to a host and host to users. This is called remote server attestation. All subsequent execution on an attested host-user pair can then be validated through trusted path mechanism. Integrity and confidentiality of data stored in cloud can either be secured through sealed storage or by making authenticity checks when accessing data. Checksums are useful mechanisms for this. However, checksums are costly to compute and can only be used after transmission of full data to the client (costly for network). New techniques such as Provable Data Possession (PDP) in untrusted cloud may be a more efficient mechanism as it generates a probabilistic proof for data integrity based on only a small portion of the file.

Information centric security (ICS): As information in the public cloud is stored outside of organizational boundaries, it is necessary to insert context specific access metadata in the information itself. Strong encryption of the entire data may not be useful as the data is often processed in cloud in un-encrypted form which makes it vulnerable. One way of achieving ICS would be to use Policy based or Role based access controls which can be defined in a language like Extensible Access Control Markup Language (XACML) which governs context-based access rules in policy enforcement point of the data.

Privacy preserving models: In cloud computing data processing collaboration is often required across sources which have complementary sources of data like distributed data mining. In multi-party processing, the data hosting parties may even be passive adversaries they trust each other and fulfill the contracts, but may want to gain extra information out of other parties data. Research around secure multi-party computation seeks to create a randomized bit-level partition scheme for the

data. The random data even if aggregated at the other party site does not elicit any useful information.

IV. THE CLOUD COMPUTING ARCHITECTURE SECURITY IMPLICATION

The Cloud Computing model has three service delivery models and main three deployment models. The deployment models are:

A. *Private cloud:* a cloud platform is dedicated for specific organization.
B. *Public cloud:* a cloud platform available to public users to register and use the available Infrastructure.
C. *Hybrid cloud:* a private cloud that can extend to use resources in public clouds. Public cloud are the most vulnerable deployment model because they are available for public users to host their services who may be malicious users.

The cloud service delivery models, include:

A. *Infrastructure as a service (IaaS):* Cloud providers deliver computation resources, storage and network as an internet based services. This service model is based on the virtualization technology. Amazon EC2 is the most IaaS provider.
B. *Platform as a service (PaaS):* Cloud providers deliver platforms, tools and other business services that enable customers to develop, deploy, and manage their own applications, without installing any of these platforms or support tools on their local machines. The PaaS model may be hosted on top of IaaS model or on top of the cloud infrastructures directly. Google Apps and Microsoft Windows Azure are the most known PaaS.
C. *Software as a service (SaaS):* Cloud providers deliver applications hosted on the cloud infrastructure as internet based service for end users, without requiring installing the applications on the customer computers. This model may be hosted on top of PaaS, IaaS or directly hosted on cloud infrastructure. SalesForce CRM is an example of the provider.

V. CLOUD COMPUTING SERVICE DELIVERY MODELS AND SECURITY IMPLICATIONS

The key security issues vulnerabilities are given in each service delivery model. Some of these issues are the responsibility of cloud providers while others are the responsibility of cloud consumers.

A. *IaaS Security Issues*

VM security securing the VM operating systems and workloads from common security threats that affect traditional physical servers, such as malware and viruses, using traditional or cloud-oriented security solutions. The VM security is the responsibility of cloud consumers. Each cloud consumer can use their own security controls based on their needs, expected risk level, and their own security management process.

Securing VM images repository unlike physical servers VMs are still under risk even when they are offline. VM images can be compromised by injecting malicious codes in the VM file or even stole the VM file itself. Secured VM images repository is the responsibilities of the cloud providers. Another issue related to VM templates is that such templates may retain the original owner information which may be used by a new consumer.

B. *PaaS Security Issues*

SOA related security issues the PaaS model is based on the Service oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man in the middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks. Mutual authentication, authorization and WS-Security standards are important to secure the cloud provided services. This security issue is a shared responsibility among cloud providers, service providers and consumers.

API Security PaaS may offer APIs that deliver management functions such as business functions, security functions, application management. Such APIs should be provided with security controls and standards implemented, such as Oauth to enforce consistent authentication and authorization on calls to such APIs. Moreover, there is a need for the isolation of APIs in memory. This issue is under the responsibility of the cloud service provider.

C. *SaaS Security Issues*

In the SaaS model enforcing and maintaining security is a shared responsibility among the cloud providers and service providers. The SaaS model inherits the security issues discussed in the previous two models as it is built on top of both of them including data security management and network security.

Web application vulnerability scanning web applications to be hosted on the cloud infrastructure should be validated and scanned for vulnerabilities using web application scanners. Such scanners should be up to date with the recently discovered vulnerabilities and attack paths maintained in the National Vulnerability Database (NVD) and the Common Weaknesses Enumeration (CWE). Web application firewalls should be in place to mitigate existing discovered vulnerabilities (examining HTTP requests and responses for applications specific vulnerabilities).

VI. CLOUD COMPUTING SECURITY ENABLERS

A. *Identity & Access Management (IAM) and Federation*

Identity is a core of any security aware system. It allows the users, services, servers, clouds, and any other entities to be recognized by systems and other parties. Identity consists of a set of information associated with a specific entity. This information is relevant based on context. Identity should not disclose user personal information privacy. Cloud platforms should deliver or support a robust and consistent Identity management system. This system should cover all cloud objects and cloud users with corresponding identity context information. It should include Identity Provisioning and deprovisioning, identity information privacy, identity linking, identity mapping, identity federation, identity attributes federation, single sign on, authentication and

authorization. Such system should adopt existing standards, such as SPML, SAML, OAuth, and XACML, to securely federate identities among interacting entities within different domains and cloud platforms.

B. Key Management

Confidentiality is one of key objectives of the cloud computing security (CIA triad). Encryption is the main solution to the confidentiality objective, for data, processes and communications. Encryption algorithms either symmetric keybased or asymmetric are key based. Both encryption approaches have a major problem related to encryption key management how to securely generate, store, access and exchange secrete keys. Moreover, PaaS requires application keys for all APIs and service calls from other applications. The applications keys must be maintained securely along with all other credentials required by the application to be able to access such APIs.

C. Security Management

Based on the huge number of cloud stakeholders, the deep dependency stack, and the large number of security controls to deliver security requirements, the cloud security management becomes a more complicated research problem. Security management needs to include security requirements and policies specifications, security controls configurations according to the policies specified, and feedback from the environment and security controls to the security management and the cloud stakeholders. Security management should function as a plug-in for CML.

VII. CLOUD-BASED TRUSTED IDENTITY ATTRIBUTE SERVICE

Because of the information security contradiction of the users real identity between business application system and users, and the huge quantity of users, cloud-based trusted identity attribute service model will separate users real identity management from the business account management, entrust official management departments to maintain the real identity service separately and manage the real identity in the official management domain. And it can provide the cloud-based trusted support of users real identity for the virtual business account. For the virtual business account, it can give the universal service interface to all kinds of applications with the appropriate account management service.

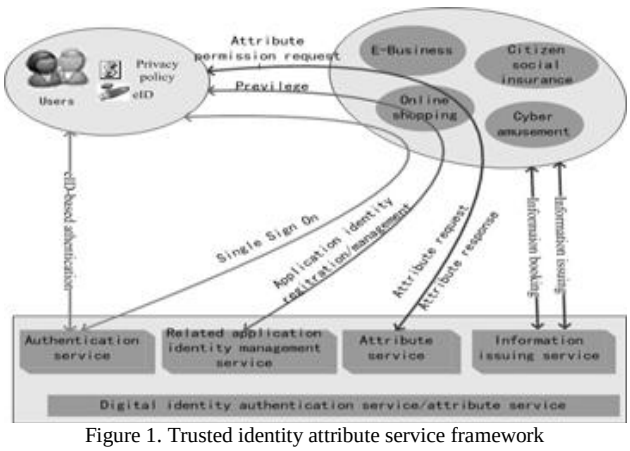

Figure 1. Trusted identity attribute service framework

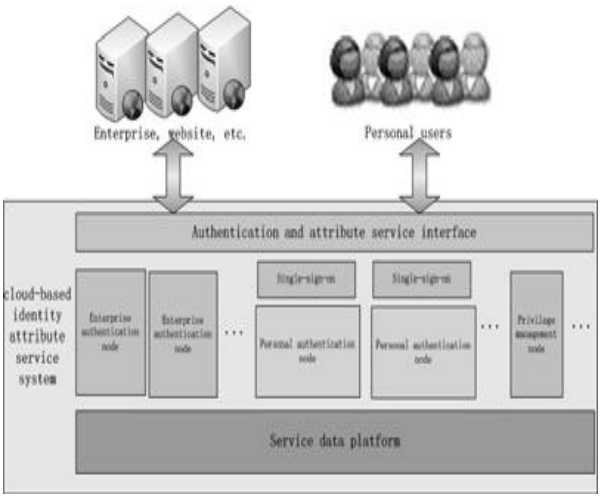

Figure 2. Cloud-based trusted identity service architecture

Figure 1 shows the general cloud-based trusted identity attribute service architecture mainly includes the identity authentication and attribute service interface, enterprise authentication node, single sign on, personal authentication node, privilege management node, and the service data platform. The identity authentication and attribute service interface is in charge of the user's cloud-based identity service, including enterprise, website and personal users. And the cloud-based service is realized by the enterprise authentication node and the personal authentication node. And the service data platform as the trusted party manages the users real identity information and provides the identity service data for the enterprise authentication node and the personal authentication node through the service interface to provide the business applications with all kinds of identity management service.

Figure 2 shows the identity authentication service based on the digital identity management platform and eID (electronic identity) mainly include authentication service, real-name registration service with the application, attribute service, and information issuing service. The user registers on the digital identity platform by the public security department, and gets the digital identity eID binding with the real identity. And the digital identity uses as the token of authentication and application identity management, and according to the user's privacy policy, providing the privilege for the application attribute request.

VIII. MECHANISM OF MULTILEVEL PRIVACY PROTECTION

The mechanism of multilevel privacy protection creates the user privacy policy formulation and policy fusion mechanism to realize the administrable and controllable function of the user attribute privacy information issuing, as shown in Figure 3.

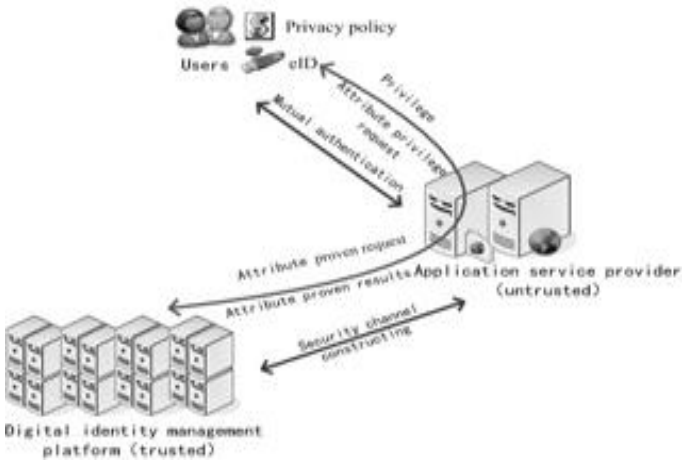

Figure 3. The mechanism of multilevel privacy protection

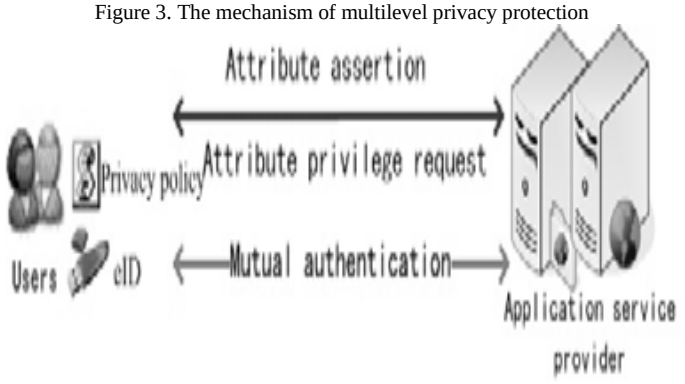

Figure 4.The user controllable attribute assertion (rapid mode)

The users virtual business account binding with the real identity can provide the account in the application system with trusted token. But for assuring user privacy security, the business account management system cant see the real identity information in the process of the identity binding. And for many cyber business applications, it requires the real identity information joining. Hence can provide user attribute information for the application by attribute issuing process to assure the business application system to operate regular. After the identity binding, the real identity service provider should assess the business type and the deploying security environment, and according to the formulated XACML attribute privacy policy, deciding to issue the attributes, attribute information proving, and provides the retrieval and issuing service of the user's identity information for the business account service level by the cyber business application requirement. And the forbidden issuing attribute information cant be seen by the account service level to realize the user attribute privacy protection. Also, attribute privacy policy should be constructed by assessing the account service level requirement and the deploying security environment and by the trusted party as the real identity administrator can forbid the application system by cheating way to get the extra user attribute information and to use other way which may lead to leakage of user privacy.

IX. CONCLUSION

Cloud computing as a platform for outsourcing and remote processing of application and data is gaining rapid momentum and categorize the key concerns and discuss the related technical implications and research issues, including some advanced security issues specific to the cloud. Firstly the security standardization activities, under aegis of many standard bodies and industry forums like CSA, OGF, W3C, SNIA etc. are fragmented. Proliferation of open community based identity management solutions also makes cloud identity management and integration difficult. Second quick provisioning of the users in cloud and mapping of their roles between enterprise and cloud has become somewhat complicated. Third Data anonymization and privacy preserving techniques will increasingly assume greater importance and more mainstream research is required in this area. Fourth migrating generic in-house software code to public cloud require thorough understanding of potential security risks. Finally adherence to the regulatory compliance by the cloud providers and better disclosure norms from them is imperative for commercial success of cloud.

The cloud computing model is one of the promising computing models for service providers, cloud providers and cloud consumers. But to best utilize the model block the existing security holes. The new cloud based trusted identity service method and the method based on the service model of multilevel cyber identity management provided user identity attribute service for cyber applications, and implemented the multilevel privacy protection mechanism, and presented the authentication service of the eID certificate and the coherence authentication service of the eID identity. And the system had been primary implemented and achieved good effects in actual applications.

REFERENCES

[1] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma's "Cloud Compting Security- Trends and Reasearch Directions".
[2] Mohamed Al Morsy, John Grundy and Ingo Muller's "An Analysis of The Cloud Computing Security Problem".
[3] S.Subashini, V.Kavitha's "A Survey on Security Issues in Service Delivery Models of Cloud Computing".
[4] Xiang Zou, Bing Chen, Bo Jin's "Cloud Based Identity Attribute Service with Privacy Protection in Cyberspace".
[5] Amazon Elastic Compute Cloud web services, http://aws.amazon.com/ec2
[6] SalesForce Force.com Platform as a service, http://developer.force.com
[7] NetSuite SaaS portal, http://www.netsuite.com
[8] Gartner DataQuest Forecast on Public Cloud Services DocID G00200833, June 2, 2010
[9]Chow,R.,Gotlle,P.,Jakobsson, E.S.,Staddon,J., Masuoka,R., and Molina,J. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. Proceedings of the 2009 ACM workshop on Cloud computing security, 2009
[10] Gellman, R., Privacy in the Cloud: Risks to Privacy and Confidentiality in Cloud Computing. Technical Report prepared for World Privacy Forum, 2009