A Design of Cloud Privacy Manager Algorithm

D.Veerabhadra Rao†, Prasad Reddy P.V.G.D††, and G.Appa Rao†††

†Faculty of Engineering, Information Technology ,GITAM University India
††Faculty of Engineering Computer Science & Systems Engineering ,AndhraUnivesity,India
†††Faculty of Engineering, Computer Science GITAM University India

Summary
Cloud Computing is a evolving Technology and new paradigm. The objective of this paper is to introduce the privacy concerns, related to cloud computing that will likely be the focus of discussion.In this paper we discuss the privacy in cloud computing ,its enchancement technologies to provide control of data by customer.Privacy issues were discussed along with case studies and a new approach of understanding data and privacy. Privacy by design plays a major role in addressing challenges of Cloud Computing .Solutions for assuring privacy of trusted information is verified.We proposed an Algorithm for Privacy Manger and Approaches for Challenges to Privacy in Cloud Computing .

Key words:
CloudComputing,PETs,Privacy,BigData component, FIPs

1. Introduction

Privacy may be defined as concealing ones own data and provide with user access control.In cloud computing privacy of the data should be provided by technologies, exist to enhance individuals privacy. Privacy can be done by encryption techniques, privacy policy setup and by privacy managers.Data privacy and data security risks are top barriers to overcome in Cloud Computing.Pivacy of personal informationas well as confidentiality of business information as significant impact on privacy of Cloud Computing. In health information,video piracy protection,bankruptcyefforts should their to maintain secrecy.India did not had a dedicated privacy laws.Our task in cloud computing is to provide privacy to data as it resides in the cloud controlled by Cloud Provider. Fig1but The economic value of information continues to rise and much of that information relates to us as individuals. Big data is ,huge information which is increasing in organizations which provide a valuable insight for them and as it contains personally identifiable information, increased responsibility and care is required to manage this information.Their are innumerable ways in which big data useful for value in universal economy personaly should be protected.

Privacy Enhancing technologies (PETs)

PETs are technologies protects and enhances individualprivacy. Pseudonymisation tools are software and systems that allow individuals to withhold their true identity from those operating electronic systems or providing services through them, and only reveal it when absolutely necessary. Federated identity management systems potentially allow individuals to access the services of organisations without having to provide information to them. They involve one trusted organisation verifying the identity of an individual and then vouching for them using an electronic token that also specifies their particular entitlements. This allows the individual to access the services provided by third parties using the token without having to disclose.examples where PETs are used is electronic biometric access systems,secure online access systems ,software that allows browsers to automatically detect the privacy policy of websites and sticky's electronic privacy policies .The benefits of PET,s are they can save you money ,reduce risk,and build trust.The different queries which arise in design to protect individual privacy is :

Do I need to collect any personal data at all?
- If so, what is the minimum needed?
- Who will have access to which data?
- How can accesses be controlled to allow only those which are for the
purposes stated when the data was collected, and then only by those
employees and processes that have an essential need?
- Can individuals make total or partial use of the system anonymously?
- How can I help individuals to exercise their rights securely?

Who will have access to my data?

Privacy by Design

Privacy by design shows how ,why privacy protections to be embedded in technolgy .It is used in sense making for decisionmaking,sensemaking capabilities of this new technology are inspired by the human decision-making process and how individuals process and relate new observations to previous observations – drawing on this

Manuscript received July 5, 2012
Manuscript revised July 20, 2012

rich context-accumulating process to enhance decision-making.

Data owners are the admins i.e were able to provide access controls through username and passwords .Privacy by Design applys knowledge and way of implanting privacy in design s specification of various technologies. This may be delivered by building the standards of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems. As a broad overarching concept, Privacy by Design encompasses many elements in practice:

1. Recognition that privacy interests and concerns must be addressed proactively;
2. Application of core principles expressing universal spheres of privacy protection;
3. Early mitigation of privacy concerns when developing information technologies and systems, throughout the entire information life cycle —end to end;
4. Need for qualified privacy leadership and/or professional input;
5. Adoption and integration of privacy-enhancing technologies (PETs);
6. Embedding privacy in a positive-sum (not zero-sum) manner so as to enhance both privacy and system functionality; and
7. Respect for users' privacy.

2. Theoretical Consideration

Privacy in Cloud

Personal data contains the identity which should be used effectively with minimum disclosure of biological ,genelogical ,historical,,transactional, locational ,reputional information in cloud and exercising of control over it.evloution of consumer computing is from standalone pc,web and now cloud, were users depend entirely on data and applications in interenet. Personal identity remain in cookies and ip addresses which be protected.The strengths of cloud is well utilized by young generation since it offers limitless flexibility,better reliability and security,enhanced collaboration,portabilityand simpler devices.

Cloud Offers	
Properties	***Tools***
Flexibilty	Online games,virtual worlds
Reliabilty Security	Data Storage
Simpler Devices	PDA,Cellphone ,Online Game Console

Informational self-determination refers to the ability of individuals to exercise personal control over the collection, use and disclosure of their personal information by others. It forms the basis of modern privacy laws and practices around the world.

Informational self-determination has become a challenging concept to promote and protect in a world of unlimited information passing from individuals to organizations, and from organizations to each other, often described as 'Web 2.0

Various solutions are provided by IBM such as IBM InfoSphereOptim and InfoSphereGaurdium for privacy of enterprises data which supported different data types .Organisations contain sensitive data both in structured and unstructerd formats which is well protected by IBM InfoSphereOptim . IBM InfoSphere solutions for data security and privacy support heterogeneous enterprise environments including all major databases, custom applications, ERP solutions and operating platforms .

IBM InfoSphere Guardium can help support your cloud and virtualization strategy with:

- Virtualized database activity monitoring, database vulnerability assessments, data redaction and data encryption
- Automatic discovery and classification of data the cloud
- Static and dynamic data masking to ensure a least privileged access model to cloud resources
- Audit and compliance reports customized for different regulations to demonstrate compliance in the cloud

Privacy Challenges in Cloud Computing Environments

Cloud computing supports multidomain environments, in which each domain can use different security, privacy, and trust requirements and potentially employ various mechanisms, interfaces, and semantics,multidomain policy integration should be developed.

Authentication and Identity Management

An identity management (IDM) mechanism should be developed Which protect private and sensitive information of users aswell As processes.An IDM system should address Multijursidiction ,interoperability draw backs. Authentication and IDM components should also be easily integrated with other security components.

Access Control and Accounting

Generic access control interfaces should be ensured by cloud delivery models for proper interoperability, which demands a policy-neutral access control specification and enforcement framework that can be used to address cross-domain access issues. Heterogeneity and diversity of services, as well as the domains' diverse access requirements in cloud computing environments, demand fine-grained access control policies. The access control models should also be able to capture relevant aspects of SLAs Hence, utilizing a privacy-aware framework for access control and accounting services is crucial, and it should be easily amenable to compliance checking.

Trust Management and Policy Integration

Trust Management and Policy Integration Frameworks should be developed to address semantic heterogeneity, secure interoperability, and policy-evolution management to ensure that such a dynamic collaboration is handled securely and that security breaches are effectively monitored in the interoperation process, and policy integration.

Secure-Service Management

An dynamic and systematic service provisioning and composition framework that considers security and privacy issues is important .

Privacy and Data Protection

Privacy-protection mechanisms must be included in all security solutions ,which also support trace back ,auditing and history based access control, ensuring balance between data provenance and privacy.

Organizational Security Management

Cloud implementation by enterprise make their existing security management and information security life-cycle models change. Organizational perimeters, shared governance issues should be addressed appropriately to ensure business continuity and disaster recovery plans. Evaluation of best practices and Standards, security metrics should be developed to answer economical instability of the provider and addressing customer risks.

Consumer Economics

Consumer economic standards should be leveraged by adopting cloud by ensuring trust on Providers and services.

Technological Changes

Technological advancements in terms of Hardware and software should be utilized fully with PETs.

Privacy Approaches

The approaches provide a trust worthy Cloud requirements addressing Cloud Providers,ServiceIntegrators and Environments .

Authentication and Identity Management

User-centric IDM and federated IDM solutions could be developed to ensure users control their digital identities and which reduces complexities for enterprises, which can focus on their core functions.

Access Control Needs

Role-based access control (RBAC) ,RBAC extensions such as generalized temporal ,location based ,credential based are accepted in providing modeling constructs and capabilities to capture context-based fine-grained access requirements constructs and is best suited for policy-integration needs

Secure Interoperation

Multidomain access control policies and policy integration issues, which can be adopted to build a comprehensive policy management framework in clouds. Global access policies would be solution to address secure interoperation and policy engineering mechanisms to integrate access policies of different domains. Specification frameworks are required to ensure that the cross-domain accesses are properly specified, verified, and enforced. Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML), and Web services standards are viable solutions toward this.

Secure-Service Provisioning and Composition

Virtualization technologies for secure provisioning, The Open Services Gateway Initiative (OSGi) service platform to cooperatively develop, deploy, and manage services , Declarative OWL-based language be adopted to develop an agent-based collaboration system for automatic service provisioning. Collaboration systems should include dynamic access control to resources shared by agents and controlling collaborative actions that are geared toward a collaboration goal to ensure Secure-Service Composition.

Trust Management Framework

One possible approach is to develop a comprehensive trust-based policy integration framework that facilitates policy integration and evolution based on interdomain- and service-access requirements,. Efficient cryptographic mechanisms for trust delegation to include in service composition frameworks.

A Privacy Manager for Cloud Computing

A privacy manager for cloud computing, helps in storing the consumer private data in the cloud server securely using the technique of obfuscation adhering privacy law. And features, called preferences and personae. The preferences feature allows users to set their preferences about the handling of personal data that is stored in an unobfuscated form in the cloud. . The persona feature allows the user to choose between multiple personae when interacting with cloud services.

The different possible architectures for privacy management in cloud computing.

Privacy Manager in the Client

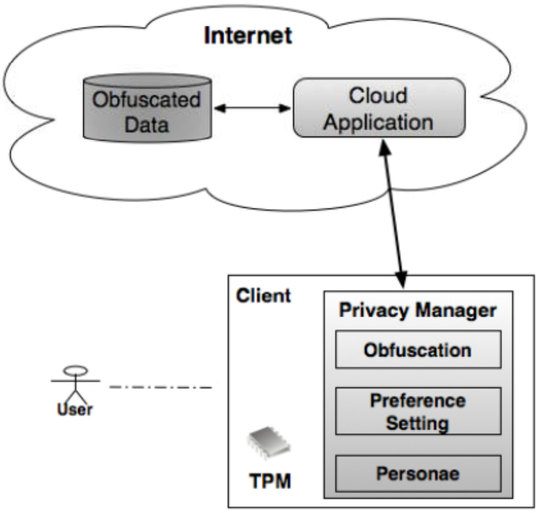

Figure 1. Client-Based Privacy Manager

Privacy Manager software on the client helps users to protect their privacy when accessing cloud services. A central feature of the Privacy Manager is that it can provide an obfuscation and de-obfuscation service, to reduce the amount of sensitive information held within the cloud.

Privacy Manager in a Hybrid Cloud

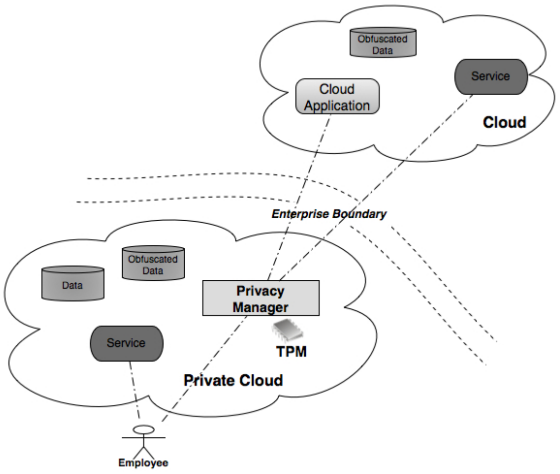

Figure 2. Enterprise-focused Privacy Manager

The Privacy Manager may be deployed in a local network,or a private cloud, to protect information relating to multiple parties.

Privacy Infomediary within the Cloud

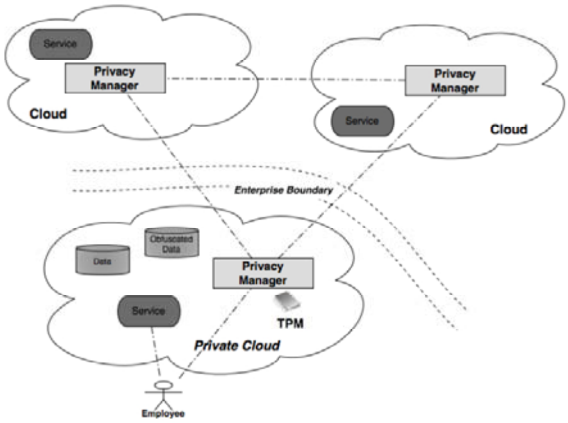

Figure 3. Privacy Manager within the Cloud

Service Agreements

A service agreement defines the terms and conditions for access and use of the services offered by the cloud provider. The complete terms and conditions for a cloud service agreement are usually stipulated in multiple documents, which can typically include a Service Level Agreement (SLA), privacy policy, acceptable use policy, and terms of use. The privacy policy documents information handling practices and the way consumer information is collected, used, and managed by the cloud provider, while the acceptable use policy identifies prohibited behaviors by cloud consumers.Privacy and security risks depend to a great extent on the terms established in the service agreement. Potential areas of improvement where organizations may derive security and privacy benefits from transitioning to a public cloud computing environment include the following: Staff Specialization ,Resource Availability, Backup and Recovery,. Mobile Endpoints and Data Concentration.

Proposed Algorithm for Privacy Manager in CloudComputing

L=Level of data 0,1,2 represents low,medium ,high sensitivity,

T=Total quantity of data, S=Sensitive data

OB=objuscated Data,

F=Function of Objuscation

SID=Server ID

R=Replication Count[0 to n]

Primary Server=PS

CID=Client machine ID

Dob is the Deobjuscation

Client side Obfusaction

If the Level of Data =0

```
Then  no obfuscationprocess of DataGoto I
If  L=1
Do objuscationprocess (OB=  F( Not (T=T-S))  Goto II
Else
            OB=F(S)
            Transmit OB toPS ,RC
I :         If  Transmit T to PS,RC
II :        Transmit OB
Sensitivity is directly proportional to Obfuscation
Provider Side Storage
If L=0      store T
Elseif      L=2  and RC=0
 Store OB in PS
Else
 If L=2 and RC >1 Store in PS+N Servers,
            Copy SID
             If L=3 and RC=0 Store in PS
Else
            L=3 and RC>1 store in N Servers
            Copy SID
```

Clientside Deobfuscation

```
Client Request OB to PS
PS  Receives OB Request,CID
PS calculates SDN= SDA [CID,N]->Nth SID
PS verifies ServerStatus for fault

If Fault=0
             Nth SID->OB to CID
             CID Dob[OB]
            Else Calculate SDN for Next N-1
```

This proposed algorithm has following advantages:
Speed Retreival of data
Ensures privacy Of Senstive Data
Decreases DownlOad Time
Consumes Less Bandwidth
Decreases Traffic
Quality Data is Received
Corrupted data is Rejected At Server Side
Resource usage is minimized by using Quality Server

3. Experimental Consideration

Case studies In Privacy
User Centric Identity Management is used to protect name and kept separate form medical records ,insurance claims and drug prescriptions. IBM's Identity Mixer technology, or Microsoft's U-Prove technology supports wide variety of privacy and various security properties, ranging from from low-security password-based one-factor authentication to high-end, attribute-based systems deploying state-of-the-art privacy-enhancing certificates .Identity can be done by certificate and authentication. A certificate is an electronic document used to identify an individual, a server, a company, or other entity and to associate that identity with a public key. Identity can also be done by Authentication like client side and server side Authentication .Authentication is the process of confirming identity There are two main forms of client authentication:

- Password-based authentication . Almost all server software permits client authentication by requiring a recognized name and password before granting access to the server

Certificate-based authentication . Client authentication based on certificates is part of the SSL protocol. The client digitally signs a randomly generated piece of data and sends both the certificate and the signed data across the network. The server validates the signature and confirms the validity of the certificate . The most important concerns for cloud users is privacy ,security and anonymity. Furthermore, cloudcomputing is a global service, crossing multiple governments and their differing sets of regulations and servicing users across the world; it will also have to account for the privacy concerns of different cultures and the privacy laws of numerous countries.To protect the privacy of cloud users, care must be taken to guard both users' data and applications from manipulating that data., it from all other records such as name in their users personal and financial information.Pew Internet Survey specifies 98 percent of cloud application users are concerned whether their data has been used by third party,80 percent of the people are concerned whether their photos were used in marketing campaign and 68 percent are concerned whether their information is analzed for further marketing.World Economy Forum 2010 study on Global Coud Computing Deployment reveals Cloud provided economic benefits,flexibility,innovation,efficiency but major barriers are privacy 63 percent and security with 50 percent and data governance 56 percent.

4. Conclusion

Analysis and Conclusion
The following measures could be adopted to implement privacy in cloud computing:
Providing user access controls

Protect Data against unauthorized instance copying

Protecting Against Unauthorized Access to Your Servers and Data

Adopting documented information security policies and supporting procedures

Using various data protection tools

Privacy issues should be specified in Service Level Agreements

A unified privacy protection should be adhered

Specifing controls on what cloud providers can and cannot do with users' data

Ensure visibility and auditability

Centralized control and visibility

A unified data protection foundation

Leverage central control and visibility

Protect more data in more locations

Ensure compliance—no matter what change

Miminize data traffic

In this paper we proposed an Algorithm for Privacy Manager and Approaches for Challenges to Privacy in Cloud Computing.Privacy protections are essential to building the customer trust needed for cloud computing and the Internet to reach their full potential.Customers also expect their data and applications stored in the cloud to remain private and secure.While the challenges of providing security and privacy are evolving along with the cloud

References

[1] Certificates and Authentication

[2] Privacy by Design in the Age of Big Data Report Addresses How Big Data & Privacy Can Successfully Coexist Dr. Cavoukian, Information and Privacy Commissioner of Ontario, Canada and IBM Chief Scientist and Fellow Jonas Release Report

[3] Accounting help for small businesses

[4] privacy in the clouds A White Paper on Privacy and Digital Identity: Implications for the Internet Ann cavoukian,. information and privacy commissioner of Ontario

[5] Privacy Enhancing Technologies: A Review Yun Shen, Siani Pearson

[6] Privacy Management in Cloud ComputingComputing Presentation by Jason Ho

[7] Security and Privacy in Cloud Computing: A Survey Minqi Zhou†, Rong Zhang§,

[8] From Hype to Future KPMG's 2010 Cloud Computing Survey

[9] CLOUD COMPUTING AND PRIVACY REGULATIONS:AN EXPLORATORY STUDY ON ISSUES AND IMPLICATIONS Dr. Mohammed A. T. AlSudiari1

[10] The Global Information Technology Report 2012 Living in Hyperconnected World Soumitra Dutta and Beñat Bilbao-Osorio, editors

[11] Security and Privacy Challenges in Cloud Computing Environments Hassan Takabi and James B.D. Joshi Arizona State University

[12] Privacy and Digital Identity:Implications For The Internet Ann Cavoukian, Ph.D. Information and Privacy Commissioner Ontario

[13] A Privacy Manager for Cloud Computing - HP Labs

[14] Guidelines on Security and Privacy in Public Cloud Computing Wayne Jansen Timothy Grance

PRASAD REDDY P.V.G.D Professor Department Of Computer Science & Systems Engineering College Of Engineering Andhra University over 24 years of Teaching Experience handled courses for B.Tech, M.Tech.Research Areas include Enterprise wide Computing, XML based object models and scalable web applications, soft Computing, Knowledge Discovery from Databases, Image Processing, Number theory & Cryptosystems. Has Papers in Journals : 51 in International Journals, 3 Patents Papers in Conferences : 43 No. of Ph.D's guided : 14 No. of M.Phil's guided : 18 M.E./M.Tech. Projects Guided : 259

G.Appa Rao., M.Tech., M.B.A.,Ph.D., in computer science and Engineering from Andhra Universiy. Over 15 Years of teaching experience with GITAM University, handled courses for B.Tech, M.Tech. Research areas include DataMining and AI. Published 20 papers in various National and International Conferences and Journals

Mr..D.Veerabhadra Rao., M.Tech., in Information Technology. Over 9 Years of teaching experience with GITAM University, handled courses for B.Tech and M.Tech .5 research paper was published in international journal and one conference