ISSN:0975-9646

A Study of Cloud Privacy and Privacy Patterns

D.Veerabhadra Rao
Information Technology
GITAM University
Visakahapatanam,India

G.Appa Rao
Computer Science
GITAM Univesity
Visakahapatnam ,India

Prasad Reddy P.V.G.D
Computer Science & Systems Engineering
AndhraUnivesity
Visakahapatnam ,India

Abstract—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 and also regarding various Privacy Patterns .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. In

IndexTerms—CloudComputing ,PETs, Privacy, Big Data component, FIPs

PRIVACY

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 ersonaly 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 decsionmaking 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 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 adeliverd 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.

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

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.

CLOUD PRIVACY PATTERNS

What is a Pattern

A pattern may defined as characteristic form, style,model which can be used as an arche type.The advantages of Patterns

- speed up the development process by providing tested, proven development paradigms .
- Reusing patterns helps to prevent subtle issues that can cause major problems, and it also improves code readability for coders and architects who are familiar with the patterns.
- Patterns provide general solutions, documented in a format that doesn't require specifics tied to a particular problem.
- •In addition, patterns allow developers to communicate using well-known, well understood names for software interactions. Common design patterns can be improved over time, making them more robust than ad-hoc designs
- a standard solution to a common programming problem enable large scale reuse of S/W

Patter ns may be classified as Infrastructure Patterns,Securiy Patterns .In this paper we discuss regarding Security patterns .It is classified as Trust Boundary Patterns:This pattern provide trust, Applications developed from this can engage in secure communication after establishing trust.This pattern presents the following advantages:Security,Trust and Confidentiality.

Hardening Patterns:These patterns describe the required steps and actions to harden security code, including detailed information on how and where to inject the security code .

This patterns help in elaborating security hardening patterns and plans to common security hardening practices, applying them to secure applications,and for testing the hardened applications. This hardening Patterns can be classified as:

Code-level hardening

Code-level hardening constitutes changes in the source code in a way that prevents vulnerabilities without altering the design Software process hardening is the addition of security features in the software build process without changes in the original source code

Design-level hardening

Design-level hardening is the re-engineering of the application in order to integrate security features that were absent or insufficient.

PRIVACY & CONFIDENTIAL DATA EXCHANGE PATTERNS

A Cloud Data Pattern describes a reusable and implementation technology-independent solution for a challenge related to the data layer of an application in the Cloud for a specific context. Cloud Data Patterns address both the migration of a data layer hosted traditionally to the Cloud as well as enabling access to the data layer in the Cloud. "Traditionally" denotes not using any Cloud technology Confidentiality Patterns provide solutions for avoiding disclosure of confidential data. Confidentiality includes security and privacy. Confidentiality

we consider the data to be kept private and secure as "critical data". For instance, critical data are business secrets of companies, personal data, and health care data.The presentation of the patterns did not go into technical details. For instance, scalability and single point of failure has not been treated.

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

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

In this Paper will also discussed regarding Cloud Security Patterns.In Future study will represent detail case study regarding Cloud Security Patterns.

REFERENCES

Certificates and Authentication
http://docs.redhat.com/docs/en-US/Red_Hat_Certificate_System/8.0/html/Deployment_Guide/Introduction_to_Public_Key_Cryptography-Certificates_and_Authentication.html
http://www.tandfonline.com/doi/pdf/10.1080/19331680802425479
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*
http://ibmprivacy.com/
Accounting help for small businesses
https://help.waveaccounting.com/customer/portal/articles/6574-who-will-have-access-to-my-data-
http://www.hunton.com/files/Publication/6acf0d97-7c21-42d1-ab48-315a04601152/Presentation/PublicationAttachment/37dc2129-4f0c-45a0-8417-651e05dc423f/CloudComputing_Bruening-Treacy.pdf
Privacy in the clouds A White Paper on Privacy and Digital Identity: Implications for the Internet Ann cavoukian,. information and privacy commissioner of Ontario
http://www.ipc.on.ca/images/resources/privacyintheclouds.pdf
Privacy Enhancing Technologies: A Review Yun Shen, Siani Pearson
http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf
Privacy Management in Cloud ComputingComputing Presentation by Jason Ho
http://www.cs.uwaterloo.ca/~kmsalem/courses/CS848W10/presentations/Privacy-proj.pdf
Security and Privacy in Cloud Computing: A Survey Minqi Zhou†, Rong Zhang§, http://meminagaoglu.yasar.edu.tr/wp-ontent/uploads/2012/04/05663489.pdf
From Hype to Future KPMG's 2010 Cloud Computing Survey
http://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CH8QFjAE&url=http%3A%2F%2Fwww.kpmg.com%2FES%2Fes%2FActualidadyNovedades%2FArticulosyPublicaciones%2FDocuments%2F2010-Cloud-Computing-Survey.pdf&ei=aYTuT5LWPMqmrAealNG-DQ&usg=AFQjCNE7p5kAJqq09MO-xQMbgKLRcFVEiQ&sig2=DqPqMNjZTrOxTtkzQAhd-Q
CLOUD COMPUTING AND PRIVACY REGULATIONS:AN EXPLORATORY STUDY ON ISSUES AND IMPLICATIONS Dr. Mohammed A. T. AlSudiari1
http://airccse.org/journal/acij/papers/0312acij16.pdf
http://asmarterplanet.com/blog/2012/06/tune-in-june-27-for-live-blogging-from-d-c-big-data-the-new-natural-resource.html
The Global Information Technology Report 2012 Living in Hyperconnected World Soumitra Dutta and Beñat Bilbao-Osorio, editors
The Global Information Technology Report 2012 Living in Hyperconnected World Soumitra Dutta and Beñat Bilbao-Osorio, editors
http://www3.weforum.org/docs/Global_IT_Report_2012.pdf
Privacy and Digital Identity:*Implications For The Internet* Ann Cavoukian, Ph.D. Information and Privacy Commissioner Ontario
http://ipc.on.ca/images/Resources/2008-05-24-IDIS-Maggiore.pdf
Context-Aware Privacy Design Pattern Selection Siani Pearson, Yun Shen
An aspect-oriented approach for the security hardening of code5 Azzam Mourad*, Marc-Andre´ Laverdie`re, Mourad Debbabi