Understanding the Security, Privacy and Trust Challenges of Cloud Computing

Debabrata Nayak

Huawei, Bangalore; e-mail: debu.nayak@huawei.com

Abstract

The overall objective of this paper is to understand the Security, Privacy and Trust Challenges and to advise on policy and other interventions which should be considered in order to ensure that Indian users of cloud environments are offered appropriate protections, and to underpin Indian cloud ecosystem. Cloud computing is increasingly subject to interest from policymakers and regulatory authorities. The Indian regulator needs to develop a pan-Indian 'cloud strategy' that will serve to support growth and jobs and build an innovation advantage for India. However, the concern is that currently a number of challenges and risks with respect to security, privacy and trust exist that may undermine the attainment of these policy objectives. Our approach has been to undertake an analysis of the technological, operational and legal intricacies of cloud computing, taking into consideration the Indian dimension and the interests and objectives of all stakeholders (citizens, individual users, companies, cloud service providers, regulatory bodies and relevant public authorities). This paper represents an evolutionary progression in understanding the implications of cloud computing for security, privacy and trust. Starting from an overview of the challenges identified in the area of cloud, the study builds upon real-life case study implementations of cloud computing for its analysis and subsequent policy considerations. As such, we intend to offer additional value for policymakers beyond a comprehensive understanding of the current theoretical or empirically derived evidence base. which will understand the cloud computing and the associated open questions surrounding some of the important security, privacy and trust issues.

Journal of Cyber Security and Mobility, Vol. 1, 277–288.

Keywords: cloud, security, privacy, trust.

1 Introduction

We identified a number of issues in the literature relating to technological and legal challenges confronting privacy, security and trust posed by cloud computing. Regarding the challenges in the technological underpinnings of cloud computing. There are a number of challenges posed by a range of legal and regulatory frameworks relevant to cloud computing. These include the viability of legal regimes which impose obligations based on the location of data Service models for cloud computing. establishing consent of the data subject; the effectiveness of breach notification rules; the effectiveness of cyber-crime legislation in deterring and sanctioning cyber-crime in the cloud and finally difficulties in determining applicable law and jurisdiction. From an operational perspective, the study uncovered issues relating to the effectiveness of existing risk governance frameworks, whether cloud customers can meet their legal obligations when data or applications are hosted how to be compliant and accountable when incidents occur; whether data will be locked into specific providers; the complexities in performing audit and investigations; how to establish the appropriate level of transparency and finally measuring security of cloud.

Compliance: *Greater harmonization of relevant legal and regulatory frameworks* to be better suited to help provide for a high level of privacy, security and trust in cloud computing environments. For example: *establishing more effective rules for accountability and transparency* contributing to a high level of privacy and security in data protection rules and *expansion of breach notification regimes* to cover cloud computing providers.

Accountability: Improvement of rules enabling cloud users (especially consumers) to *exercise their rights* as well as *improvement of models of Service Level Agreements (SLAs)* as the principle vehicle to provide accountability in meeting security, privacy and trust obligations.

Transparency: Improvement of the way in which levels of security, privacy or trust afforded to cloud customers and end-users can be discerned, measured and managed, including *research into security best practices, automated means for citizens to exercise rights* and *establishment of incident response guidelines*.

Governance: The *European Commission could act as leading customer* by deploying cloud computing solutions as part of its e-Commission initiative and indirectly supporting the improvement of existing operational risk control frameworks. Research funding could be assigned to *improving Security Event and Incident Monitoring* in the cloud amongst other things.

2 Defining Security, Privacy and Trust

Security concerns the confidentiality, availability and integrity of data or information. Security may also include authentication and non-repudiation.

Privacy concerns the expression of or adherence to various legal and nonlegal norms regarding the right to private life. In the European context this is often understood as compliance with European data protection regulations. Although it would be highly complex to map cloud issues onto the full panoply of privacy and personal data protection regulatory architectures, the globally accepted privacy principles give a useful frame: consent, purpose restriction, legitimacy, transparency, data security and data subject participation.

Trust revolves around ‘assurance’ and confidence that people, data, entities, information or processes will function or behave in expected ways. Trust may be human to human, machine to machine (e.g., handshake protocols negotiated within certain protocols), human to machine (e.g., when a consumer reviews a digital signature advisory notice on a website) or machine to human (e.g. when a system relies on user input and instructions without extensive verification). At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives.

3 Risk Control Frameworks

Physical access controls: how can the cloud user achieve requirements for physical access control given the cloud service provider establishes and controls the when who, why and how of physical access measures?

Application development and maintenance: is it possible to assure the development and maintenance of applications in a cloud environment when external parties cloud service provider or other third parties are responsible?

Vulnerability management: assigning responsibility for patch management and the deployment of software and hardware updates between the cloud service provider and cloud user is especially complex given virtualisation and the dynamic reconfiguration of software and infrastructures.

Monitoring: how to establish effective, timely and accurate monitoring of levels of security and privacy in business-critical infrastructure when those responsible for the infrastructure may not be prepared to share such information under standard service level agreement.

Identification and authentication: the integration and control of identity and access management infrastructures in a cloud environment where the cloud service provider might have different approaches and tolerance for risks to identity infrastructure, in addition to the complexities of providing for identity across distributed cloud environments.

Access control: how can the cloud user govern access control risks when the levels and types of access control to key ICT assets deployed by the cloud service provider are unknown.

Encryption – how can the cloud user manage encryption and key infrastructures and assign responsibility across the boundary between their own organisation and the cloud service provider.

Continuity and incident management: how can the cloud user determine appropriate thresholds and criteria for responding to incidents (e.g. agreeing on what constitutes an incident) and policies and processes for responding and achieving assurance of the evidential chain.

4 Solving the Challenges: Observations and Recommendations

Compliance: ensuring that a cloud deployment meets the requirements imposed by the applicable normative framework, including general legislation, sector-specific rules and contractual obligations; the challenges in complying with data protection rules are a key example of this.

Accountability: ensuring that security or privacy breaches in the cloud deployment are correctly addressed, including through appropriate compensation mechanisms towards any victims.

Transparency: ensuring that the operation of the cloud deployment is sufficiently clear to all stakeholders, including service providers and users, both professional businesses and private consumers; this can be witnessed, for example, in the difficulty of determining who/where a cloud service provider is, and where his responsibilities/liabilities end.

Governance: ensuring that the European Commission's policy objectives and actions of the European Commission are well aligned with ongoing stakeholder activities, including by actively participating in the establishment and promotion of standards and best practices, and in interactions with cloud service providers.

5 Growing Focus on Security, Privacy and Trust Concerns in Cloud Computing

Given that the need for public policy depends on the way cloud computing is designed, deployed and used, what is the optimal combination of cloud service provision and governance, taking into account the existing legal and market contexts and the costs, complexity and uncertainties associated with these issues.

Taking into account the incentives of different stakeholders, what is required to ensure that this optimal arrangement can be achieved without adversely distorting the impacts of cloud computing.

6 Identifying Key Issues and Possible Enablers for Security, Trust and Privacy in the Cloud

Assurance of the hypervisors' ability to isolate and establish trust for guest or hosted virtual machines is critical, as this forms the root node for multitenant machine computing and thus could prove to be a single point of failure, since the hypervisor can potentially modify or intercept all guest OS processing.

The same properties of the hypervisor, which enable it to inspect and monitor all processing within and between guest OSs, give the potential for enhanced security monitoring, but will require that current security controls based on dedicated appliances can be migrated to virtual machine architectures. They could also lead to a potential loss of individual customer privacy and security.

For economic purposes, the ability of large-scale instances of virtual machines to be dynamically moved and re-provisioned is vital. It is unclear at this point how adequate the lifecycle management of those instances between hardware and across clouds is, and whether trust can be established to an adequate level, if at all.

7 Security, Privacy and Trust Challenges Inherent to the Legal and Regulatory Aspects of Cloud Computing

The technologically orientated challenges introduced in the previous chapters, it is clear that there are also substantial legal aspects to be taken into consideration for the provisions of cloud computing services. While these challenges are global in nature, the normative response may vary substantially from region to region or even from service to service. Diverging interpretations and legal uncertainties could well endanger the development of innovative cloud service models, as they can adversely affect the trustworthiness of such services: how can users invest in the cloud without a clear perspective on the compliance of the chosen solution with the applicable legal framework, or on the guarantees offered by the service provider.

8 Regulatory Frameworks

In the regulatory framework we should consider the following factors in to account.

- In what country is the cloud provider located
- Is the cloud provider's infrastructure located in the same country or in different countries
- Will the cloud provider use other companies whose infrastructure is located outside that of the cloud provider
- Where will the data be physically located
- Will jurisdiction over the contract terms and over the data be divided
- Will any of the cloud provider's services be subcontracted out

8.1 Regulatory Issues to Be Considered for Cloud

- Indian government Regulation of Investigatory Powers Act
- Stored Communications Act of Indian government
- National Security Letters for investigation
- HIPPA (health-related information)
- GLB (financial services industry)
- state privacy laws
- Video rental records
- Fair Credit Reporting Act

8.2 Establishing the Legal Foundation of Trust: How to Determine Applicable Law in the Cloud

Applicability of the law remains linked to the geographical location of the information society service provider, and in a cloud model it may be difficult to identify this entity or its geographical location. Finally, certain issues, including contractual consumer protection clauses and intellectual property protection, are to be handled very carefully by the regulators.

8.3 Handling Disputes in the Cloud: How to Reinforce Trust by Building in a Mechanism for Accountability

Regulation is linked to the physical location of the stakeholders (typically the place of establishment of the defendant), and certain areas of law are excluded from its scope. Thus, here too, alternative mechanisms of deciding the competent jurisdiction (principally voluntary choice by the parties) will need to be considered, as well as alternative conflict resolution mechanisms, including mediation and binding or non-binding arbitration.

8.4 Cloud Offers the Same Protection of Intellectual Property Rights and Provision of Confidentiality and Data Portability

Software and Database Directives, the IP Rights Enforcement Directive, and several parts of the aforementioned eCommerce Directive, but it is also worth noting that these regulatory measures primarily address intellectual property rights, with rules relating to know-how, trade secrets or confidentiality still being determined largely at the national level.

8.5 Meeting Security Obligations and Responding to Cybercrime

In order for end users to trust cloud services, they must be secure, which implies robustness, reliability and availability. Cloud service providers will need to offer the required guarantees in this regard, by protecting their services against internal threats and against external attacks

9 Cloud Security Advantages

- Exposure of internal sensitive data reduced by shifting public data to a external cloud.
- Cloud homogeneity simplifies security auditing/testing.
- Clouds enable automated security management both internally and externally.
- Redundancy/Disaster Recovery.
- Reduces in-house IT security administration.

9.1 Cloud Security Challenges to Be Taken Care of by the Regulators

- *Trust*

  - Putting too much trust to vendor's security model
- *Auditing and investigation*
  - Customer may be out of loop in audit events and findings
  - Obtaining support for investigations at mercy of the provider
  - Logging Challenges
- *Administration*
  - Indirect security administrator accountability
  - Security configurations
  - Identity management
- *Implementation*
  - Black box implementations can't be examined
  - Public cloud vs internal cloud security
- *Data*
  - Regulatory differences and difficulties across national boundaries
  - Data retention issues
  - Data protection in storage and transit
  - Ownership

9.2 Regulator Should Take Care of the Following Points When Locking down the Cloud

- *Securing the cloud*
  - trust
  - multi-tenancy
  - encryption
  - compliance
- *Achieving goals*
  - privacy
  - secure access
  - transparency
- *Trust*
  - Platform trust and trusted computing
  - identity management, user provisioning and access control
  - Federation, control of privileges, SSO
  - Authentication, authorization and auditing

  - Privileged user management
  - Web access management
- *Encryption*
  - Key management and provisioning
  - Data leak protection
  - Data storage and transit Security profile per network
- *Multi-tenancy*
  - Multi-tenant logging management
  - Network, VM, Application, process, and data isolation
  - Security, OS, and Resource Management
  - Security DMZ per virtual application
  - Security profile per compute profile
- *Compliance*
  - Auditing
  - Log management
  - Regional/national/international compliances and certification
  - Legal intercept
  - Data Privacy

9.3 Compliance and Certification Aspects to Be Taken Care of by the Regulators

- Security related Cloud-specific group
- ITU Cloud Focus Group
- ETSI cloud security group
- SAS70
  - Auditing compliance
- TIA942
  - US Data Center
- ISO 27001
  - Common Criteria certification and compliance
- ISO 15489
  - Records and Information Management
- LEED

  - Leadership in Energy and Environmental Design: green data center
- NIST FIPS 140-2
  - Security Requirements for Cryptographic Modules
- ISA's Security Assurance Certification
  - Embedded Device Security Assessment

10 Conclusion

In this paper we have discussed the pertinent of legal and regulatory domains as applied to cloud computing, most notably relating to legal obligations stemming from location of (personal) data in the cloud, accountability, transparency, consent, security and the definition of responsibilities of those using and processing data. Furthermore, we have discussed the regulatory of operational perspectives, some of the regulators are to manage security, privacy and trust challenges arising in cloud computing deployments. Finally, we discussed how to make cloud a viable and effective business.

References

[1] A. Bisong and S.M. Rahman. An overview of the security concerns in enterprise cloud computing. International Journal of Network Security & Its Applications (IJNSA), 3(1):30–45, 2011.

[2] B. Grobauer, T. Walloschek, and E. Stocker. Understanding cloud computing vulnerabilities. Security & Privacy, IEEE, 9(2):50–57, 2011.

[3] W.A. Jansen. Cloud hooks: Security and privacy issues in cloud computing. In Proceedings of 44th Hawaii International International Conference on Systems Science (HICSS-44 2011), Koloa, Kauai, HI, USA, 4–7 January 2011. IEEE Computer Society, Washington, DC, pp. 1–10, 2011.

[4] Debabrata Nayak. Collaborative security. Paper presented at the Bangalore Security Conference, 10 December 2010.

[5] Debabrata Nayak. Cloud security. Paper presented at Wireless Vitae Conference, Chennai, India, 28 February–3 March 2011.

[6] Debabrata Nayak. Key management in cloud security. Paper presented at ITU, Switzerland, 6–7 December 2010.

[7] Debabrata Nayak. Cloud security. Paper presented at China Shenzhen Conference, 10 December 2010.

[8] Debabrata Nayak. Mobile security. Paper presented at ASSOCHAM Security Conference, India, 1 April 2011.

[9] Debabrata Nayak. Private cloud. Paper presented at Korea-Japan-China Security Conference, 8 October 2010.

[10] Debabrata Nayak. Key management in cloud. Paper presented at IEEE Conference COMSNET, Bangalore, 4–8 January 2011.

[11] Debabrata Nayak. Hybrid cloud security management. Paper presented at Security Conference, China, 12 October 2010.

[12] Debabrata Nayak. Hybrid cloud security management. Paper presented at Security conference, India, 4 April 2011.

[13] Debabrata Nayak, D.B. Phatak, V.P. Gulati, and N. Rajendran. Mobile data networks security issues and challenges. Presented paper at the International Conference on Emerging Technology Bhubaneswar, India, 19–21 December, pp. 137–148, 2003.

[14] Debabrata Nayak, D.B. Phatak, V.P. Gulati, and N. Rajendran. Security issues in wireless local area network. In Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering, 2–5 May, pp. 108–111, 2004.

[15] Debabrata Nayak, D.B. Phatak, V.P. Gulati, and N. Rajendran. Security issues in mobile data network. In Proceedings of IEEE Vehicular Technology International Conference 2004-Fall on 'Wireless Technologies for Global Security', Los Angeles, CA, 26–29 September, pp. 45–49, 2004.

[16] Debabrata Nayak, D.B. Phatak, V.P. Gulati, and N. Rajendran. Modeling and evaluation of security architecture for wireless Local area Networks. In Proceedings of International Conference on Advanced Computing and Communication, Ahmedabad, 16–19 December, pp. 281–285, 2004.

[17] Debabrata Nayak and D.B. Phatak. Modelling and performance evaluation of security architecture for wireless local area networks. Transaction on Engineering Computing and Technology, 3, December 2004.

[18] Debabrata Nayak, D.B. Phatak, and V.P. Gulati. Modeling and evaluation of security architecture for wireless local area networks by indexing methods: A novel approach. In Proceedings of the First Information Security, Practice and Experience Conference (ISPEC2005), Lecture Notes in Computer Science, Vol. 3439, pp. 25–35. Springer, Berlin/Heidelberg, 2005.

[19] Debabrata Nayak, D.B. Phatak, and V.P. Gulati. Performance evaluation of security architecture for wireless local area networks by security policy method. In Proceedings of 2005 IEEE Sarnoff Symposium, Princeton, NJ, USA, 18–19 April, pp.37-40, 2005.

[20] Debabrata Nayak, D.B. Phatak, V.P. Gulati, and N. Rajendran. Policy based performance evaluation of security architecture for wireless local area networks. In Proceedings of 6th World Wireless Congress, San Francisco, USA, 24–26 May, pp. 51–57, 2005.

[21] Debabrata Nayak and D.B. Phatak. An adaptive and optimized security policy manager for wireless networks. In Proceedings of 2007 IEEE Asia Modelling Symposium, Phuket, Thailand, 27–30 March, pp. 155–158, 2007.

[22] Debabrata Nayak, D.B. Phatak, and Ashutosh Saxena. Evaluation of security architecture for wireless local area networks by indexed based policy method: A novel approach. International Journal of Network Security, 7(1):1–14, July 2008.

[23] Debabrata Nayak. Cloud security. Paper presented at ASSOCHAM Cyber Security Workshop, India, May 2012.

Biography

Debabrata Nayak has completed his PhD in wireless security from IIT Bombay. He has been working on security domain in last 18 years. He is a Chairman of Global ICT Forum of India SIG, Co-Chairman for Assocham Cyber Law and IT act, Chairman for Huawei Senior security Expert Consultant Group(R&D), Member of CII (Conferederation of Indian Industry member of International Association for Cryptological Research, Motorola information assurance forum for 3 year, WiMax Forum (GWRG Group), LTE Forum (BWA Group), 3GPP SA3 Security, Cloud Security Alliance, IEEE Security and privacy and Cryptology Research Society of India, and Key member of ITU SG17 Security (Cybex – deals with country specific security), China-Japan-Korea Security Committee, and the ITU Cloud Computing Group.

Debabrata Nayak obtained his Masters Degree from NIT Rourkela, specialized in Elliptic Curve Cryptography and Internet security. Covering wide areas such as Security system Performance evaluation, Design of secure cryptographic system, Wireless Security policy design and implementation. He designed Security solution for INFINET (Indian Financial Network for RBI). He has presented 62 papers in international conferences and technical journals. He was an active member of STIG (DoD) and reviewed guideline for Unix STIG and Network STIG. He has worked with Motorola as Senior Security Architect, Reserve Bank of India as Information Security officer, and with Tata Elxsi as Security expert. He has extensively worked on LTE Security and WiMax Security. He was consultant to various financial institutes for implementation of standards such as BS7799 and ISO 17799. He was also involved in Ministry of Communication and IT of India for Secure mCheque project in IDRBT.