Integration of the Data Reliability in the Field of Cloud Computing with Wireless Sensor Network

Manjushree H R
M.tech scholar.:Dept. of Computer Science & Engg.
Akshaya Institute of Technology
Tumkur, India

Shivamurthy R C
Professor.: Dept. of Computer Science & Engg.
Akshaya Institute of Technology
Tumkur, India

***Abstract*— Cloud computing is one of the most emerging technologies which plays an important role in the next generation architecture of IT Enterprise. It has been widely accepted due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. In the cloud computing system, both application software and databases are moved to the large data centers, where the data should not be secure in the hands of providers. IT organizations have expressed concerns about the various security aspects that exist with the widespread implementation of cloud computing. These types of concerns originate from the fact that data is stored remotely from the customer's location. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. This paper describes an enhancement for the already existing data security model in cloud environment. The proposed data security model provides user authentication and data protection. It also ensures fast recovery of data.**

Keywords*: AES Algorithm, Byzantine fault tolerance, Data Security Model, Distributed Denial of Service (DDoS)

I. INTRODUCTION

A typical cloud-computing environment is characterized by the networking of tens of thousands of servers. Once deployed, such datacenters experience a relatively stable hardware and networking environment. Smartphone's offer considerable processing, memory, storage and sensing resources, and are handheld, pocket-sized devices that users generally carry with them at all times. The vision for cloud computing could foster more flexible models, whereby general users, including mobile ones, could participate in the cloud as both providers and consumers of resources. If the cloud is to computing what the Internet is for data, the opportunity for mobile computers to participate in service provision should be investigated.

The motivation for this dissertation is threefold. First, it explores the forces that resulted in the emergence of cloud computing. Second, the implications of mobile server nodes within a cloud environment are considered. Finally, the dissertation focuses on implementing a mobile storage cloud. Moreover, inherited from cloud computing (CC), which is a new computing paradigm enabling users to elastically utilize a shared pool of cloud resources (e.g., processors, storages, applications, services) in an on-demand fashion, mobile CC (MCC) further transfers the data storage and data processing tasks from the mobile devices to the powerful cloud Thus, MCC not only alleviates the limitations (e.g., battery, processing power, storage capacity) of mobile devices but also enhances the performance of a lot of traditional mobile services (e.g., mobile learning, mobile gaming, mobile health). For instance, mobile gaming can exploit MCC to move the game engine that requires substantial computing resources (e.g., graphic rendering) from mobile devices to powerful servers in the cloud to greatly reduce the energy consumption of the mobile devices and improve the gaming performance (e.g., refresh rate, image definition, sound effect). Recently, motivated by the potentials of complementing the ubiquitous data gathering capabilities of WSN with the powerful data storage and data processing abilities of MCC, the integration of WSN and MCC is attracting increasing attention from both

and transmits the sensory data to mobile users on demand. During the whole data transmission process, if the data transmissions from the sensor nodes to the gateway or from the gateway to the cloud or from the cloud to the mobile user are not successful, data are retransmitted until they are successfully academia and industry. Data storage and data processing are transmitted first to the WSN gateway in a hop-by-hop manner. The gateway then further stores, processes and transmits the received sensory data to the cloud. Finally, the cloud stores, processes delivered. For this new WSN-MCC integration paradigm, the WSN acts as the data source for the cloud and mobile users are the data requesters for the cloud. With just a simple client on their mobile devices, mobile users

can have access to their required sensory data from the cloud, whenever and wherever there is network connection. Evolving as the concept of "sensor-cloud", the integrated WSN-MCC is "an infrastructure that allows truly pervasive computation using sensors as an interface between physical and cyber worlds, the data-compute clusters as the cyber backbone and the internet as the communication medium" For years the Internet has been represented on network diagrams by a cloud symbol until 2008 when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing.

.

II . ISSUES RELATED WITH DATA RELIABILITY IN CLOUD

Cloud Deployments Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. The Cloud Computing model has three main deployment models which are:

1. Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

2. Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

3. Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure.

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. Security: It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet
as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.

B. Costing Model: Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, on demand computing makes sense only for CPU intensive jobs.

C. Charging Model: The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developing multi tenancy within their offering can be very substantial. These include: re-design and redevelopment
of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Consequently, SaaS providers need to weigh up the trade-off between the provisions of multi tenancy
and the cost-savings yielded by multi-tenancy such as reduced overhead through amortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viable charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud providers.

D. Service Level Agreement (SLA): Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources

when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS,
and SaaS) will need to define different SLA met specifications. This also raises a number of implementation problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework.

E. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%),Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result reveals that organizations still have security/privacy concerns in moving their data on to the Cloud. Currently, peripheral functions such as IT management and personal applications are the easiest IT systems to move. Organizations are conservative in employing IaaS compared to SaaS. This is partly because marginal functions are oftenoutsourced to the Cloud, and core activities are kept in-house. The survey also shows that in three years time, 31.5% of the organization will move their Storage Capacity to the cloud. However this number is still relatively low compared to Collaborative Applications (46.3%) at that time.

F. Cloud Interoperability Issue: Currently, each cloud offering has its own way on how cloud clients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. This severely hinders the development of cloud ecosystems by forcing vendor locking, which prohibits the ability of users to choose from alternative vendors/offering simultaneously in order to optimize resources at different levels within an organization. More importantly, proprietary cloud APIs makes it very difficult to integrate cloud services with an organization's own existing legacy
systems (e.g. an on-premise data centre for highly interactive modeling applications in a pharmaceutical company).The primary goal of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. There are a number of levels that interoperability is essential for cloud computing. First, to optimize the IT asset and computing resources, an organization often needs to keep in-house IT assets and capabilities associated with their core competencies while outsourcing marginal functions and activities (e.g. the human resource system) on to the cloud. Second, more often than not, for the purpose of optimization, an organization may need to outsource a number of marginal functions to cloud services offered by different vendors. Standardization appears to be a good solution to address the interoperability issue. However, as cloud computing just starts to take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors.

III. RELATED WORK

Gartner 2008 identified seven security issues that need to b addressed before enterprises consider switching to the cloud computing model. They are as follows: (1) privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water, (2) regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't (3) data location – depending on contracts, some clients might never know what country or what jurisdiction their data is located
(4) Data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider. (5) recovery - every provider should have a disaster recovery protocol to protect user data (6) investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation (7) long-term viability - refers to the ability to retract a contract and all
data if the current provider is bought out by another firm.[2] The Cloud Computing Use Case Discussion Group discusses the different Use Case scenarios and related requirements that may exist in the cloud model. They consider use cases from different perspectives including customers, developers and security engineers.[3] ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in the cloud computing may lead to such risks.[4] Balachandra et al, 2009 discussed the security SLA’s specification and objectives related to data locations, segregation and data recovery.[5] Kresimir et al, 2010 discussed high level security concerns in the cloud computing model such as data integrity, payment and privacy of sensitive information.[6] Bernd et al, 2010 discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology-related, cloud characteristics-related, security controls related.[7] Subashini et al discuss the security challenges of the cloud service delivery model, focusing on the SaaS model.[8] Ragovind et al, (2010) discussed the management of security in Cloud computing focusing on Gartner’s list on cloud security issues and the findings from the International Data Corporation enterprise.[9] Morsy et al, 2010 investigated cloud computing problems from the cloud architecture, cloud offered characteristics, cloud stakeholders, and cloud service delivery models perspectives.[10] A recent

survey by Cloud Security Alliance (CSA)&IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth.[11] Several studies have been carried out relating to security issues in cloud computing but this work presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing deployment types and the service delivery types.

IV. RESEARCH ISSUES

Security is one of the most important areas to be handled in the emerging area of cloud computing. If the security is not handled properly, the entire area of cloud computing would fail as cloud computing mainly involves managing personal sensitive information in a public network. Also, security from the service providers point also becomes imperative in order to protect the network, the resources in order to improve the robustness and reliability of those resources. Trust 30 Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan International Journal on Advances in ICT for Emerging Regions 04 September 2011 management that models the trust on the behavior of the elements and entities would be especially useful for the proper administration of cloud system and cloud services. Several leading research groups both in academia and the industry are working in the area of trust management in cloud computing. This section takes an in depth look at the recent developments in this area with the objective of identifying and categorizing them for easy reference. Khan and Malluhi have looked at the trust in the cloud system from a users perspective. They analyze the issues of trust from what a cloud user would expect with respect to their data in terms of security and privacy. They further discuss that what kind of strategy the service providers may undertake to enhance the trust of the user in cloud services and providers. They have identified control, ownership, prevention and security as the key aspects that decide users‘level of trust on services. Diminishing control and lack of transparency have identified as the issues that diminishes the user trust on cloud systems. The authors have predicted that remote access control facilities for resources of the users, transparency with respect to cloud providers actions in the

form of automatic traceability facilities, certification of cloud security properties and capabilities through an independent certification authority and providing security enclave for users could be used to enhance the trust of users in the services and

service providers . Zhexuan et al., have taken a look at the security issues SaaS might create due to the unrestricted access on user data given to the remotely installed software. The authors have presented a mechanism to separate software from data so that it is possible to create a trusted binding between them. The mechanism introduced involves four parties namely the resource provider, software provider, data provider and the coordinator. The resource provider hosts both data and software and provides the platform to execute the software on data. The software provider and data provider are the owners of the software and data respectively. The coordinator brings the other parties together while providing the ancillary services such as searching for resources and providing an interface to execute the application on the data. The operation of the model is as follows:

Software provider and data provider upload their resources to the resource provider. These resources will be encrypted before stored and the key will be stored in the accountability vault module of the system. A data provider searches for and finds the required software through a coordinator and then runs the software on the data uploaded to the resource provider‘s site. Once the execution has started an execution reference ID is generated and given to the data provider. When the execution of the software is over, the results are produced only on the data provider‘s interface which can be viewed, printed or downloaded. Data provider will then pay for the service that will be split between the software provider and resource provider. An operation log has been created and posted to the software provider without disclosing the data provider‘s identity or the content on which software was run. This helps the software provider know that his software has been used and the duration of use. Even though the authors claim that this model separates the software and data, there is no assurance that the software cannot make a copy while the data is being processed as only the algorithm or description of the software is provided to the data owner. Without the source code, there is no assurance that the code will not contain any malicious code hidden inside. Also, since the software runs on data owner‘s rights and privileges, the software would have complete control over data. This is a security threat and the audit trail even if it is available, will not detect any security breaches. The authors do not address the question of trust on the proposed platform as this would be another application or service hosted on the cloud. Both application providers and data providers need some kind of better assurance as now they are entrusting their data and software to a third party software.

The multiple stakeholder problems addresses the security issues created due to the multiple parties interacting in the cloud system. As per the authors, three parties can be clearly identified. They are namely, the client, the cloud service providers and third parties that include rivals and stakeholders

in business. The client delegates some of the administration/operations to cloud providers under a Service.

V. CONCLUSION

Cloud computing has been the new paradigm in distributed computing in the recent times. For cloud computing to become widely adopted several issues need to be addressed. Cloud security is one of the most important issues that have to be addressed. Trust management is one of the important components in cloud security as cloud environment will have different kinds of users, providers and intermediaries. Proper trust management will help the users select the provider based on their requirements and trust worthiness. Also, trust management would help the providers select the clients who are trustworthy to serve. In the paper, a comprehensive survey has been carried out on the trust management systems implemented on distributed systems with a special emphasis cloud computing. There are several trust models proposed for distributed systems. These models were mainly proposed for systems like clusters, grids and wireless sensor networks. These models have not been used or tested in cloud computing environments. Hence the suitability of these models for use in cloud computing cannot be recommended without an extensive evaluation. The authors propose to evaluate these models in future work. The trust management systems proposed for cloud computing have been extensively studied with respect to their capability, their applicability in practical heterogonous cloud environment and their implementation.The theoretical basis required can be achieved by adapting the trust models proposed for other distributed systems.

VI. REFERENCES

[1] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. "Wireless sensor networks: a survey." Computer networks 38, no. 4, pp.393-422, 2002

[2] Li, Mo, and Yunhao Liu. "Underground coal mine monitoring with wireless sensor networks." ACM Transactions on Sensor Networks (TOSN) 5, no. 2, 2009

[3] Benharref, Abdelghani, and M. Serhani. "Novel Cloud and SOA Based Framework for E-health Monitoring Using Wireless Biosensors.",1-1, 2014

[4] Tan, Kian-Lee. "What's NExT?: Sensor+ Cloud!?." In Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, pp. 1-1. ACM, 2010.

[5] Mr.K.Sindhanaiselvan #1, Ms.T.Mekala , "A Survey on Sensor Cloud: Architecture and
Applications", International Journal of P2P Network Trends and Technology (IJPTT) – Volume 6 – March 2014

[6] A.M. Riad, M. Elmogy, A.I. Shehab, " A Framework for Cloud P2P VoD System based on User's Behavior Analysis", International Journal of Computer Applications (0975 – 8887) Volume 76– No.6, August 2013

[7] Battistelli, Giorgio, Alessio Benavoli, Luigi Chisci, A. Benavoli, B. Noack, A. Benavoli, A. Benavoli et al. "Data-driven strategies for selective data transmission in sensor networks." In CDC, edited by Thierry Denoeux, pp. 800-805. 2012

[8] Nath, Suman, and Phillip B. Gibbons. "Communicating via fireflies: geographic routing on duty-cycled sensors." In Proceedings of the 6th international conference on Information processing in sensor networks, pp. 440-449. ACM, 2007.

[9] Hou, Y. Thomas, Yi Shi, and Hanif D. Sherali. "Rate allocation and network lifetime problems for wireless sensor networks." IEEE/ACM Transactions on Networking (TON) 16, no. 2 (2008): 321-334.

[10] Nicholas N. Karekwaivanane1, Wilson Bakasa2, Kudakwashe Zvarevashe, "Reliability in MAC Protocols for Wireless Sensor Networks: A Survey", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization), Vol. 2, Issue. 7, 2014

[11] Gayathri K1, V.Ananthanarayanan, "Design of Secured and Efficient Wireless Sensor Network with Integration to Public Cloud for Big Data Analytics", International Journal of Recent Development in Engineering and Technology Website: www.ijrdet.com (ISSN 2347-6435(Online) Vol.3, Issue. 1, 2014

[12] Long Cheng, Jianwei Niu, Jiannong Cao, Sajal K. Das and Yu Gu "QoS Aware Geographic Opportunistic Routing in Wireless Sensor Networks", Retrieved 2014

[13] Kyuhyung Kim, Sungwon Lee, Hongseok Yoo, and Dongkyun Kim, "Agriculture Sensor-Cloud Infrastructure and Routing Protocol in the Physical Sensor Network Layer", International Journal of Distributed Sensor Networks Volume 2014

[14] Gopalakrishnan Nair, Nithyia, Philip J. Morrow, and Gerard Parr. "Design Considerations for a Self-Managed Wireless Sensor Cloud for Emergency Response Scenario." (2011).

[15] Sherin Mathew, S. Nandhini, " A Novel Approach for Sensory Data Collection in Wireless Sensor Networks with Mobile Sinks", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013

[16] Qinglin Luo, Wei Fang, Jinsong Wu and Qingchun Chen, "Reliable broadband wireless communication for high speed trains using baseband cloud", Journal on Wireless Communications and Networking 2012

[17] Ngai, Edith, Yangfan Zhou, Michael R. Lyu, and Jiangchuan Liu. "A delay-aware reliable event reporting framework for wireless sensor–actuator networks." Ad Hoc Networks 8, no. 7 (2010): 694-707.

[18] Biswajit Panja, Kevin Highley, and Priyanka Meharia, " Enterprise Mobile Security using Wireless Sensor Network: Extending a Secure Wireless Sensor Network to the Android Smart Phone Platform", Annual Symposium on Information Assurance (Asia), JUNE 7-8, 2011

[19] Raja Vara Prasad Y, Mirza Sami Baig, Rahul K. Mishra, P. Rajalakshmi4, U. B. Desai5 and S.N. Merchant, " REAL TIME WIRELESS AIR POLLUTION MONITORING SYSTEM", TIME WIRELESS AIR POLLUTION MONITORING SYSTEM, 2011

[20] Wan, Jiafu, Caifeng Zou, Sana Ullah, Chin-Feng Lai, Ming Zhou, and Xiaofei Wang. "Cloud-enabled wireless body area networks for pervasive healthcare." IEEE Network 27, no. 5 (2013): 56-61.

[21] Ding, Yong, Martin Alexander Neumann, Dawud Gordon, Till Riedel, Takashi Miyaki, Michael Beigl, Wenzhu Zhang, and Lin Zhang. "A platform-as-a-service for in-situ development of wireless sensor network applications." In Networked Sensing Systems (INSS), 2012 Ninth International Conference on, pp. 1-8. IEEE, 2012.

[22] Piyare, Rajeev, Sun Park, Se Yeong Maeng, Sang Hyeok Park, Seung Chan Oh, Sang Gil Choi, Ho Su Choi, and Seong Ro Lee. "Integrating Wireless Sensor Network into Cloud services for real-time data collection." In ICT Convergence (ICTC), 2013 International Conference on, pp. 752-756. IEEE, 2013.

[23] Jigarkumar Contractor and Shan Lin, "Poster Abstract: Exploring Cloud Services with Body Area Networks for Medical Care", Retrieved 2014

[24] Luka Celić, "Energy efficiency in wireless sensor networks for healthcare", Retrieved 2014