ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Efficient Security for Energy Efficient Load Balancing and Application Enhancement for the Stable and Reliable Cloud

Mr. Nikhil k k[1], Mr.I.Gobi[2]

Research Scholar, Dept of Computer Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Assistant Professor, Dept of Computer Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: Cloud computing is a freshly industrializing new technology for multipart systems with large-level services distribution among various users. Therefore, verifying and validating of both users and services is a important issue for the confidence and protection of the cloud computing. SSL Authentication Protocol, once implemented in cloud computing, will become so complex that users will experience high overloaded issues in both calculation and communication. The proposed research is, based on the Attribute-based hierarchical method for cloud computing and its equivalent cryptographic and signature methods, presented a new Attribute-based security protocol for cloud computing and services. Through simulation testing, it is shown that the security protocol is more significant and capable than SSL Authentication Protocol, especially the more significant on user side.

Keywords: Cloud computing, ER system, Energy efficient, Load balance, Attribute-based hierarchical, SSL Authentication Security, networking, Cryptography, Encryption and Decryption.

1. INTRODUCTION

1.1 Introduction about Cloud Computing

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet). Clouds can be classified as public, private or hybrid Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning; Rackspace, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications. The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model (buy the dedicated hardware and depreciate it over a period of time) to the OPEX model (use a shared cloud infrastructure and pay as one uses it).

Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.

The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing have led to a growth in cloud computing. Cloud vendors are experiencing growth rates of 50% per annum

1.2 Origin of the Cloud

The origin of the term cloud computing is unclear. The expression cloud is commonly used in science to describe a large agglomeration of objects that visually appear from a distance as a cloud and describes any set of things whose details are not inspected further in a given context.

In analogy to above usage the word cloud was used as a metaphor for the Internet and a standardized cloud-like shape was used to denote a network on telephony schematics and later to depict the Internet in computer network diagrams. With this simplification, the implication is that the specifics of how the end points of a network are connected are not relevant for the purposes of understanding the diagram. The cloud symbol was used to represent the Internet as early as 1994, in which servers were then shown connected to, but external to, the cloud.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

References to cloud computing in its modern sense can be found as early as 1996, with the earliest known mention to be found in a Compaq internal document. The popularization of the term can be traced to 2006 when Amazon.com introduced the Elastic Compute Cloud.

1.3 parallel Technologies

Cloud computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles.

The main enabling technology for cloud computing is virtualization. Virtualization software allows a physical computing device to be electronically separated into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system–level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. Autonomic computing automates the process through which the user can provision resources on-demand. By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors.

Users routinely face difficult business problems. Cloud computing adopts concepts from Service-oriented Architecture (SOA) that can help the user break these problems into services that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way.

Cloud computing also leverages concepts from utility computing in order to provide metrics for the services used. Such metrics are at the core of the public cloud pay-per-use models. In addition, measured services are an essential part of the feedback loops in autonomic computing, allowing services to scale on-demand and to perform automatic failure recovery.

Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

Grid computing — "A form of distributed and parallel computing, whereby a 'super and virtual computer' is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks."

Mainframe computer — Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as: census; industry and consumer statistics; police and secret intelligence services; enterprise resource planning; and financial transaction processing.

Utility computing — The "packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity."

Peer-to-peer — A distributed architecture without the need for central coordination. Participants are both suppliers and consumers of resources (in contrast to the traditional client–server model).

1.4 Characteristics features of Cloud Computing

Agility improves with users' ability to re-provision technological infrastructure resources.

Application programming interface (API) accessibility to software that enables machines to interact with cloud software in the same way that a traditional user interface (e.g., a computer desktop) facilitates interaction between humans and computers. Cloud computing systems typically use Representational State Transfer (REST)-based APIs.

Cost: cloud providers claim that computing costs reduce. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state-of-the-art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere. Maintenanceof cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

Multitenancy enables sharing of resources and costs across a large pool of users thus allowing for:

centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

peak-load capacity increases (users need not engineer for highest possible load-levels)

utilisation and efficiency improvements for systems that are often only 10–20% utilized.

Performance is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.

Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.

Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

suitable for business continuity and disaster recovery.

Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time (Note, the VM startup time varies by VM type, location, os and cloud providers), without users having to engineer for peak loads.

Security can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

1.5 Applications of Cloud :

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

2. PROPOSED SYSTEM

As more and more organizations adopt electronic records , the case for cloud data storage be- comes compelling for deploying ER systems: not only is it inexpensive but it also provides the exible, wide-area mobile access increasingly needed in the modern world.

However, before cloud-based ER systems can become a reality, issues of data security, patient privacy, and overall performance must be addressed. As standard encryption (including symmetric key and public-key) techniques for ER encryption/decryption cause increased access control and performance overhead, the paper proposes the use of Attribute-Based Encryption to encrypt ERs based on providers' attributes or credentials; to decrypt ERs, they must possess the set of attributes needed for proper access. This paper motivates and presents the design and usage of a ATTRIBUTE based ER system based on ABE, along with preliminary experiments and analyses to investigate the exibility and scalability of the proposed approach

3. EXISTING SYSTEM

In this paper we introduce an energy-aware operation model used for load balancing and application scaling on a cloud. The basic philosophy of our approach is defining an energy-optimal operation regime and attempting to maximize the number of servers operating in this regime. Idle and lightly-loaded servers are switched to one of the sleep states to save energy. The load balancing and scaling algorithms also exploit some of the most desirable features of server consolidation mechanisms discussed in the literature. The realization that power consumption of cloud computing. centers is significant and is expected to increase substantially in the future motivates the interest of the research community in energy-aware resource management and application placement policies and the mechanisms to enforce these policies. Low average server utilization and its impact on the environment make it imperative to devise new energy-aware policies which identify optimal regimes for the cloud servers and, at the same time, prevent SLA violations. A quantitative evaluation of an optimization algorithm or an architectural enhancement is a rather intricate and time- consuming process; several benchmarks and system configurations are used to gather the data necessary to guide future developments. For example, to evaluate the effects of architectural enhancements supporting Instruction-level or Data-level Parallelism on the processor performance and their power consumption several benchmarks are used . The results show different numerical outcomes for the individual applications in each benchmark. Similarly, the effects of an energy-aware algorithm depend on the system configuration and on the application and cannot be expressed by a single numerical value.

4. LITERATURE REVIEW AND PREVIOUS WORK

1. Federal Financial Agencies Issue Cautionary Statement on Financial Institution Cloud Computing Services

Existing System are more significant about the Statement is that it reflects a discrete level of regulatory concern over the risks specifically associated with cloud IT environments, particularly in areas such as vendor management, information security, data integrity and business continuity planning. These specific concerns may be less relevant – but not totally irrelevant – to financial institutions that employ private cloud networks, but any financial institution that proposes to use any type of shared

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

cloud solution will need to be fully attentive to these regulatory worries. At a minimum, this would require the development and implementation of documented programs, policies and procedures to support a financial institution's selection and implementation of a particular cloud application, and demonstrate that the risks identified in the Statement have been specifically considered and addressed.

2. Authorized Private Keyword Search over Encrypted Data in Cloud Computing

We consider a cloud computing environment that hosts an outsourced database, based on which data sharing applications can be built. For illustration purposes, we will use an online PHR service as case study in this paper. The entities in the system are: data owners/users, trusted authorities, and the cloud server. In this paper, data owner refers someone who owns the information, e.g., a patient who encrypts her PHR data and wants them to be stored in the cloud server while preserving her privacy. The cloud server stores the encrypted data contributed by multiple owners in a database and performs search for the users. The "users" generally refer to those who can perform searches over the encrypted database. They could originate from various avenues, and usually need to search and access the data due to their professional responsibilities. We assume that the data contents are protected using separate, existing data encryption schemes , which is not the focus of this paper.

3. How cloud computing will shake up the banking industry

To achieve and sustain high performance in the future, traditional commercial banks across the world will need to master two fundamental changes:

1. The transformation of their product offerings, channels and customer service to reflect the demands of the "changing consumer"—connected, impatient, empowered, and demanding of services that meet their individual and social needs.
2. The reshaping and reinvention of their core banking operations to enable a more competitive, customer-centric, efficient and sustainable business model.
3. A failure to achieve either of these imperatives will expose banks to disintermediation by nimble, low-cost online and mobile providers of personal financial management and payments services—resulting in loss of relevance to customers and, therefore, their prominence in the financial services value chain.

4 .cbEHR: Secure Cloud Storage, Auditing, and Access Control for Electronic Health Records

Hosted systems are a convenient way to deliver economies of scale to diverse users. These solutions include services such as social networking and cloud computing that have been very active areas of research. Driven by the pressure from the government to increase IT penetration on one side, and the pressure from the market to decrease costs on the other side, healthcare organizations have recognized the advantages of outsourcing storage of medical records and related data to third parties. The traditional model of access control mechanisms being enforced by the trusted host raises several concerns in context of outsourced health records. Such concerns include when the host is unable to meet its obligations, limitations on data mobility put by regulations (e.g., Technical Safeguards section in the HIPAA Security Rule), complex access control policies composed of varying policies specified by each interested party (such as healthcare providers and individuals), and others. Integration of encrypted EHRs and other access control mechanisms present additional challenges. Furthermore, service providers may desire to reduce their responsibility of handling user data in order to limit their liability if they are compromised. Privacy and security guarantees must be provided to enable healthcare industry and end users to leverage hosted systems.

5 .Secure and Scalable Cloud-based Architecture for e-Health Wireless sensor networks

Scalability is a challenge that WSNs for medical applications should tackle. Indeed, the sampling of medical sensors is performed at high frequency which increases the amount of collected data. In addition, the frequency of sensor sampling is often increased if the condition of patients being monitored gets worse. The important size and heterogeneity of data drives a need for an increasing storage and processing capacities. Besides scalability issues, medical data could be life saving and must be accessible at any time and from everywhere. Existing solutions rely on a centralized paradigm to store and process sensed data thus cannot tackle the aforementioned challenges. We definitely need new innovative solutions to meet the great challenges of handling the exponential growth in data generated by sensors

6. Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings

Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios.
In this paper, we propose a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained and scalable access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patients' PHR data. To reduce the key distribution complexity, we divide the system into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically.

4.1 Existing System

4.1.1 Drawback
CHISTAR adopts the Cloud Component Model approach for application design described in our previous work . Cloud component model allows identifying the building blocks of a cloud application which are classified based on the functions performed and type of cloud resources required. Each building block performs a set of actions to produce the desired outputs for other components.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Less Scalability: Cloud-based EHRs such as CHISTAR have better scalability as compared to client-server EHRs. CHISTAR adopts the Cloud Component Model approach for application design which provides better scalability by decoupling application components and providing asynchronous communication mechanisms. Since components are designed to process requests asynchronously, it is possible to parallelize the processing of requests. Using Cloud Component Model, CHISTAR can leverage both horizontal and vertical scaling options.

Less Maintainability: CHISTAR has better maintainability as compared to client-server based EHR systems. The functionality of individual components of CHISTAR can be improved or upgraded independent of other components. Loose coupling allows replacing or upgrading components, without changing other components. Since CHISTAR has loosely coupled components, it is more resilient to component failures. In case of client-server based EHR systems with tightly coupled components, failure of a single component can bring down the entire application.

Less Portability: Cloud-based EHR systems such as CHISTAR have better portability. By designing loosely coupled components that communicate asynchronously, it is possible to have innovative hybrid deployments in which different components of an application can be deployed on cloud infrastructure and platforms of different cloud vendors.

Less Reduced Costs: Client-server EHR systems with dedicated hosting require a team of IT experts to install, configure, test, run, secure and update hardware and software. With cloud-based HER systems, organizations can save on the upfront capital investments for setting up the computing infrastructure as well as the costs of managing the infrastructure as all of that is done by the cloud provider. Though hardware maintenance overhead

4.2 Proposed System

Advantages

- Cloud computing provides tremendous benefits to organizations of all sizes. Formal and mid-sized businesses, cloud computing allows time-constrained IT teams to operate more efficiently. For large enterprises, the cloud provides the ability to scale up or down to respond quickly to changing market conditions. Businesses of all sizes can leverage the cloud to increase innovation and collaboration. Yet many organizations are hesitant to fully leverage the benefits of the cloud, citing concerns regarding data loss and unauthorized access, and are reluctant to rely on cloud providers to solve these challenges.
- Proposed IBCC Cloud Security helps organizations safely and confidently leverages secure cloud computing services and solutions. Rather than adopting the unique — and sometimes unknown — security practices and policies of each cloud vendor, IBCC Cloud Security allows businesses to extend and apply their own access and security policies into the cloud by securing all the data traffic moving between the enterprise and the cloud, as well as data being stored in the cloud.
- When companies start relying on cloud-based services, they no longer need complex disaster recovery plans. Cloud computing providers take care of most issues, and they do it faster that businesses used the cloud were able to resolve issues in an average of 2.1 hours, nearly four times faster than businesses that didn't use the cloud (8 hours). The same study found that mid-sized businesses had the best recovery times of all, taking almost half the time of larger companies to recover.
- a company doesn't use the cloud, workers have to send files back and forth over email, meaning only one person can work on a file at a time and the same document has tons of names and formats.
- Cloud computing keeps all the files in one central location, and everyone works off of one central copy. Employees can even chat to each other whilst making changes together. This whole process makes collaboration stronger, which increases efficiency and improves a company's bottom line.

5. CONCLUSION

Cloud computing is a freshly industrializing new technology for multipart systems with large-level services distribution among various users. Therefore, verifying and validating of both users and services is a important issue for the confidence and protection of the cloud computing. SSL Authentication Protocol , once implemented in cloud computing, will become so complex that users will experience a high overloaded issues in both calculation and communication. The proposed research is , based on the Attribute-based hierarchical method for cloud computing and its equivalent cryptographic and signature methods, presented a new Attribute-based security protocol for cloud computing and services. Through simulation testing, it is shown that the security protocol is more significant and capable than SSL Authentication Protocol, especially the more significant on user side. As more and more organizations adopt electronic records (ERs), the case for cloud data storage be- comes compelling for deploying ER systems: not only is it inexpensive but it also provides the exible, wide-area mobile access increasingly needed in the modern world. However, before cloud-based ER systems can become a reality, issues of data security, patient privacy, and overall performance must be addressed.

REFERENCES

[1]. Beak, J., Newmarch, J., Safavi-Naini, R., Susilo, W.: A Survey of Attribute-Based Cryptography. In: Proc. of the 10th Annual Conference for Australian Unix User's Group (AUUG 2004), pp. 95–102 (2004)

[2]. Boneh, D., Franklin, M.: Attribute-based Encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 433–439. Springer, Heidelberg (2001)

[3]. Chappell, D.: A Short Introduction to Cloud Platforms, http://www.davidchappell.com/CloudPlatforms–Chappell.pdf

[4]. Cocks, C.: An Attribute-based Encryption Scheme Based on Quadratic Residues. In: Proceeding of 8th IMA International Conference on Cryptography and Coding (2001)

[5]. Crampton, J., Lim, H.W., Paterson, K.G.: What Can Attribute-Based Cryptography Offer to Web Services? In: Proceedings of the 5th ACM Workshop on Secure Web Services (SWS 2007), Alexandria, Virginia, USA, pp. 26–36. ACM Press, New York (2007)