ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

A Survey on Secure Sharing In Cloud Computing

Aakanksha maliye, Sarita Patil

Department of Computer Engineering, G.H.Raisoni College of Engineering & Management, Wagholi, India

ABSTRACT: Cloud computing is a quickly growing technology with usage of virtualized resources as a service through the internet. These facilities prove to be of great use in various fields such as health care industry, education, and research & development etc. for better communication therefore we need to assure the data security for data used in communication. So, to provide security to cloud from intruders & unknown hacking attacks many existing systems have been developed but most of them are providing security on the basis of private keys. In such cases if hacker knows the private key our whole data can be in trouble. In [1] we consider shortcomings of current e-health solutions and standards, but they do not address the client platform security. In [2] we show that an efficient system can be buildwhich allows patients both to share fractionaladmission rights with others, and to perform explorations over their records. But after formalizing we realize that it results in different set of properties whereas in proposed system we use two algorithms for encryption & decryption of network data [5]. Here we use DES for data transmission and RSA for encrypting the keys generated by DES for data transmission. Therefore even in case of intruder's attack all data including key is in encrypted form so our data will not be able to decrypt easily by intruders.

KEYWORDS: Cloud computing, DES, RSA, Intruders

I. INTRODUCTION TO EXISTING SYSTEMS

Cloud computing moves the processing efforts from the local devices to datacentered a facility which enables the users to create and edit files online. It fluctuates from the typical client-server model as it provides application that clients can perform and manage through their explorer. This ability allows for much more effective computing by clusteringthe storage, processing and bandwidth. The phrase “software as a service” (SAAS) is sometimes used to describe application programs offered through cloud computing [7]. Cloud computing provides a better safety by means of different encryption techniques than a scattered network and that is one of the reasons why clouds are working. SAAS is one of the practices of Cloud Computing, which is based on a "one-to-many" model in which an application is shared across different clients. The SAAS model can add effectivenessand it is cost savings for the both the service provider and users. To make effective communication in cloud computing we use web services [7]. Web service is a software system designed to support interoperable node to node interaction within the network.when the web service is located once we can ask it to define itself and tell what processes it supports and how to invoke it, which is handled by the Web Service Description Language (WSDL). Web Services are platform independent. Moreover, majority of the web services uses SOAP protocol for transferring the message. In existing system data is transferred from sender to receiver by means of encryption & decryption. To do this task various algorithms has been proposed in various papers i.e. In[1] we point out several shortcomings of current e-health solutions and standards, but this paper is not considersthe client's datasecurity, which is an important aspect for the overall security of e-health system. In[2] we can build an efficient system which allows patients both to share fractional access rights with others, and to perform explorations over their data. We authenticate the requirements of a Patient's Encryption scheme, and give several results, based on existing cryptographic primitives and procedures, each achieving a different set of properties. In [3] we are going to develop a newcryptographicfor Fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, cipher texts are provided with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. In [4] we look into two important data security issues: secure distributed storage, and clearlydispersed data access control for delicate and private patientsRecord. We consider various practical issues that need to be taken into account while fulfilling the security and privacy requirements.In [5] we propose an IBE scheme that significantly improves key-update efficiency on the side of the trusted party, while staying up to date for the users. Our system builds on the ideas of binary tree data structure, and is safe. In [6] we propose a solution which uses decentralized approach, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making attribute based encryption (ABE) more usable in practice. In [7] we use decentralized approach for Data storage i.e. instead of storing the data in single central system, it is scattered among different sub servers and it will be available to user on demand. Before storing & retrieval, encryption & decryption will be performed by using MD5 algorithm. According to [4] we break the password into two parts and encrypt separately. After encryption we put both the parts of password in two different sub servers & the data will be decrypted only on user request [9].

II. LITERATURE SURVEY

A. Service oriented architecture

The protocol used to maintain the backup of system is Simple Object Access Protocol (SOAP),WSDL or UDDI. SOAP is a stateful protocol used to hold & transfer the backup contents. In current system we are maintaining the backup of system database for efficient functioning of search engine even during failure of any node[7].

Service-oriented architecture (SOA) is an evolution of distributed computing based on the request/reply design paradigm for synchronous and asynchronous applications [13]. An application's business logic or individual functions are modularized and presented as services for consumer/client applications. The service interface is self-governing of the execution. Application developers can build applications by composing one or more services without knowing the services' underlying implementations. For example, a service can be implemented either in .Net or J2EE, and the application consuming the service can be on a different platform or language.

Service-oriented architectures have the following key characteristics:
1. SOA services have self-describing interfaces in platform-independent XML documents. Web Services Description Language (WSDL) is the standard used to describe the services.
2. SOA services communicate with messages formally defined via XML Schema (also called XSD). Communication among consumers and providers or services typically happens in heterogeneous environments, with little or no knowledge about the provider. Messages between services can be viewed as key business documents processed in an enterprise.
3. SOA services are maintained in the enterprise by a registry that acts as a directory listing. Applications can look up the services in the registry and invoke the service. Universal Description, Definition, and Integration (UDDI) is the standard used for service registry. Following figure 1. Shows a typical Service Oriented Architecture

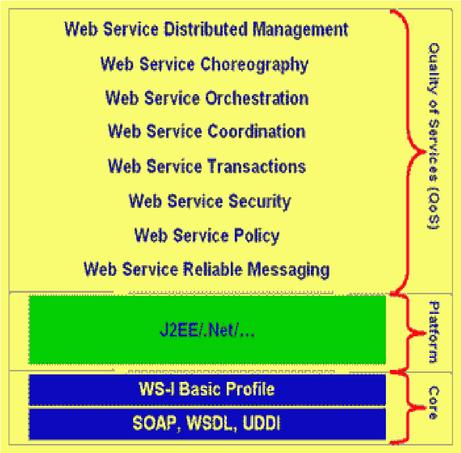

Figure 1. A typical SOA infrastructure.

Figure 2 shows the example of typical service oriented architecture. In this example user will interact to the web server using stateful protocol like service oriented architecture protocol. This protocol will hold the state of any information which we would like to get access at client side i.e. different search engine will hold different data & maintain the integrity checksum of required data at client as well as on server side. Through web service we can put any client based data on server to access it from anywhere.

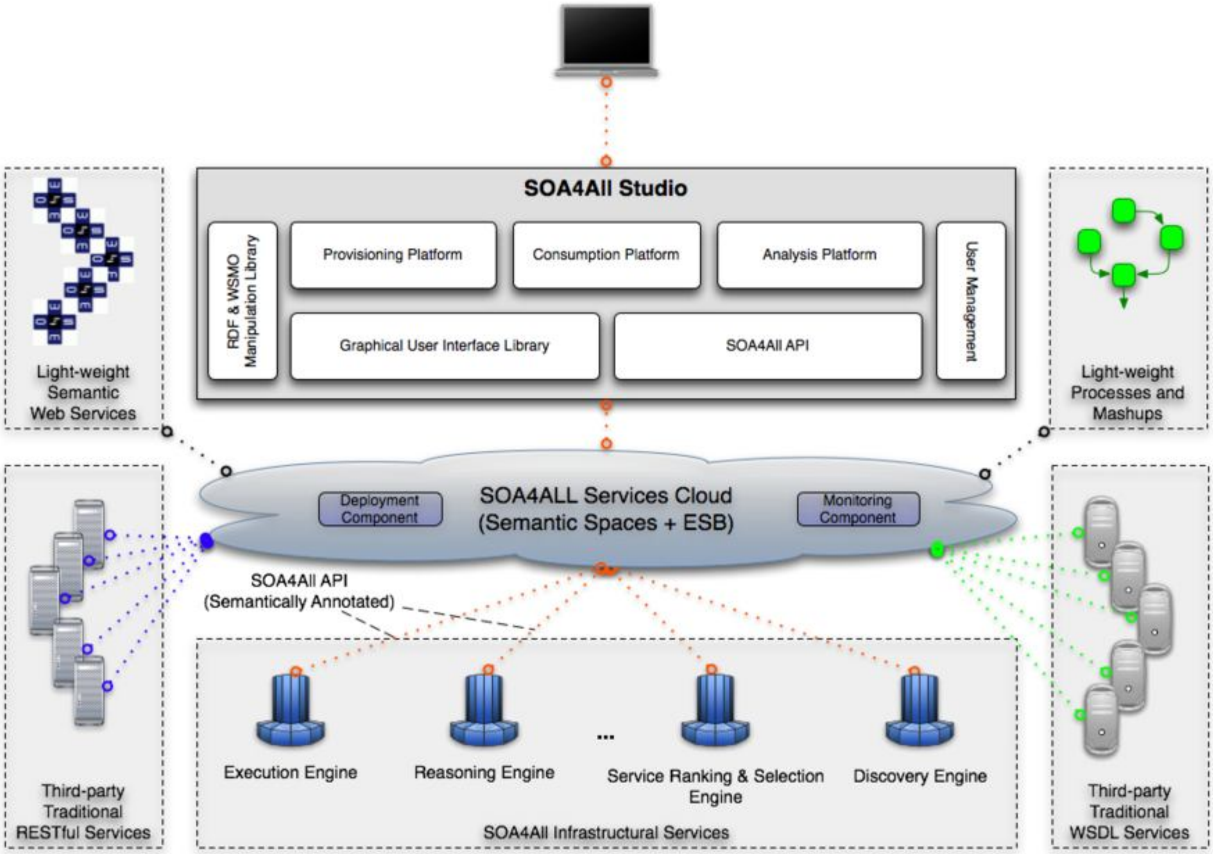
SOA4All Studio
RDF & WSMO Manipulation Library
Provisioning Platform
Consumption Platform
Analysis Platform
User Management
Graphical User Interface Library
SOA4All API
Light-weight Semantic Web Services
Light-weight Processes and Mashups
Deployment Component
SOA4ALL Services Cloud (Semantic Spaces + ESB)
Monitoring Component
SOA4All API (Semantically Annotated)
Execution Engine
Reasoning Engine
...
Service Ranking & Selection Engine
Discovery Engine
SOA4All Infrastructural Services
Third-party Traditional RESTful Services
Third-party Traditional WSDL Services

Figure 2. An Example Service oriented architecture.

Along with this, in our proposed system we focus on hybrid encryption technique with the help of two algorithms i.e. RSA &DES. We use DES algorithm for data transmission which uses common secret key at sender and receiver end and the common secret key will be encrypted using RSA algorithm.

B. Algorithms mostly used for encryption & decryption

1. Diffie-Hellman Key Exchange Protocol

Diffie–Hellman establishes a common covert that can be used for secret interactions while exchanging data over a public network. To implement Diffie-Hellman, the two end users X and Y, while communicating over a conduit they jointly have the same opinion on two positive whole numbers q and g, such that q is a prime number and g is a generator of q. The generator g is a number that, when raised to positive whole-number powers less than q, never produces the same result for any two such whole numbers. The value of q may be large but the value of g is usually small.

Once X and Y have agreed on q and g in private, they choose random positive whole-number m and n, Next, Alice and Bob compute public keys A and B based on their personal keys according to the formulas

1) A =gm mod q

2) B = gn mod q

3) The two users can share their public keys A and B over a communications medium assumed to be insecure, such as the Internet or a corporate wide area network (WAN). From these public keys, a number x can be generated by either user on the basis of their own personal keys. Alice computes K1 using the formula

4) K1 = (B) m mod q

5) Y computes K2using the formula

6) K2 = (A) n mod q

ObviouslyK1=K2.So this will be shared secret key among X and Y.

2. RSA Algorithm

Key Generation

RSA has a public key and a private key. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key[4].

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q in random way.
2. Compute n=pq
3. Compute φ(n) = φ(p)φ(q) = (p − 1)(q − 1) = n - (p + q -1), where φ is euler's function
4. Choose an integer e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1; i.e., e and φ(n) areco-prime
5. Solve for value d given d.e ≡ 1 (mod φ(n)) where *d* is the multiplicative inverse of *e* (modulo φ(*n*)).

Encryption & Decryption

Compute the cipher text c as

$$c \equiv m^e \pmod{n}$$

For decryption use

$$m \equiv c^d \pmod{n}$$

III. PROPOSED SYSTEM

In case of cloud computing we are using a decentralized approach, so the personal health record (PHR) of users is placed on third party server such as cloud providers. Since, the data is outside the system so security concern is more as personal health information (PHI) could be visible to those third party servers and to unauthorized parties. For assuring the patients control over access to their personal health information, it is a promising method to encrypt the PHRs before outsourcing. But still the issues such as risks of privacy exposure, scalability in key management, have continued the most important tasks toward achieving cryptographically enforced data access control. Here we present the scheme for patient centric framework for data access control to personal health reports stored at third party server. To achieve the fine grained & scalable data access control we use Attribute based encryption technique. In attribute based encryption technique we sets the priority for every user on the basis of attributes such as categorization on the basis of diseases, ages etc. here we also focus on multiple data owner scheme and we divide the users into multiple security domains which reduces key management complexity. Maximum patient privacy is guaranteed simultaneously by exploiting multi consultant ABE[6]. Here, we can also change the priority policies by setting different constraints. For high priority data we provide hybrid encryption method[4],[5] i.e. use of two encryption algorithm such as DES and RSA. We will use one of the algorithms for data transmission purpose and other for encryption of key which is generated through first algorithms. So, intruders can't get access of data by just decryption of one algorithm.

Methodology used

To implement the system we have to focus more on following aspects

i. System setup & key distribution
ii. PHR Encryption and access
iii. Policy update

In this system we will setup a private cloud and as per the DES & RSA algorithms public keys are generated. After generation of keys we will encrypt the PHR with the help of secret key and after encryption the data will be stored on third party server. The secret key will be encrypted through RSA algorithm. While encryption of PHR we are categorizing the data on the basis of their attribute i.e. ABE [6]. The attribute selection policy & priority can be changed with the help of policy update mechanisms. Following figure 3. Shows the block schematic of proposed system.

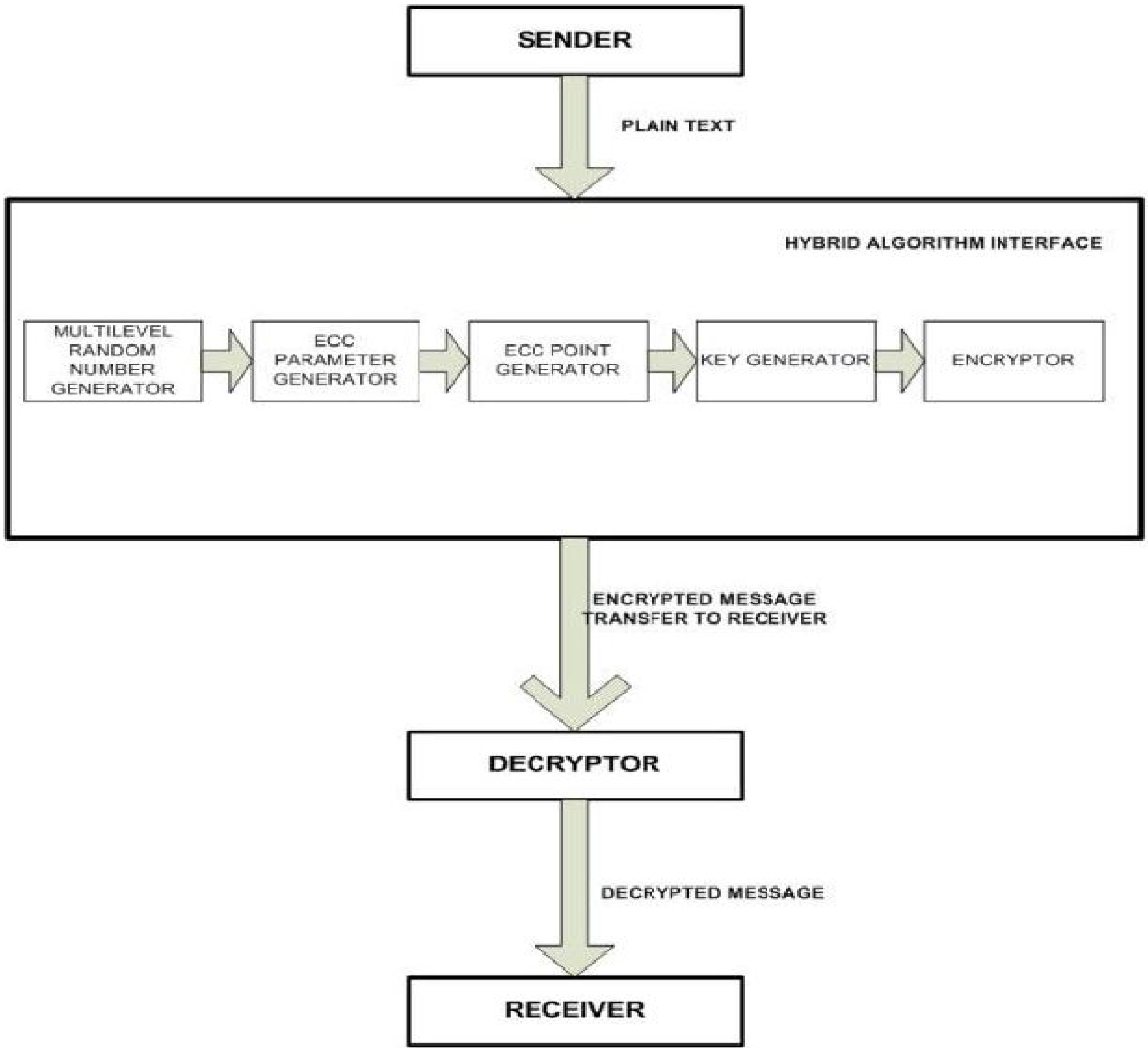

Figure 3. Block schematic of proposed method

IV. CONCLUSION

Thus, to provide the security for cloud data we had undergone various schemes. Each scheme is provide a new approach. Some approach are focusing on encrypting the data before storing into third party server and some will categorize the data on the basis of attribute contained within the data. The System will sustain more in dynamic environment if hybrid encryption algorithms are used along with attribute based Encryption (ABE).

REFERENCES

[1] Securing the E-Health Cloud, H. Lohr (Proc. First ACM Int'l Health Informatics Symp. (PHI '10),pp. 220-229, 2010).
[2] Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records(Proc. ACM Workshop Cloud Computing Security(CCSW '09),pp. 103-114, 2009).
[3] Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data(Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),pp. 89-98, 2006).
[4] Data Security and Privacy in Wireless Body Area Networks(IEEE Wireless Comm. Magazine, vol. 17,no. 1, pp. 51-58, Feb. 2010).
[5] Identity-Based Encryption with Efficient Revocation(Proc. 15th ACM Conf. Computer and Comm. Security (CCS),pp. 417-426, 2008).
[6] Improving Privacy and Security in Multi-Authority Attribute-Based Encryption(Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009).
[7] C. Branigan (2001), Wireless, handheld solutions prevail at NECC 2001, retrieved January10, 2007.
[8] F. Turiso and J. Case, "Wireless and Mobile Computing", First Consulting Group, 2001. Retrieved January10, 2007
[9] W. Pratt, K. Unruh, A. Civan and M. Skeels, "Personal health information management," Communication ACM, vol. 49, pp. 51-55, 2006.