CLOUD COMPUTING SECURITY THROUGH SYMMETRIC CIPHER MODEL

Subramanian Anbazhagan[1], Dr. K.Somasundaram[2]

[1]Research Scholar (Karpagam University), Computer Science and Engineering, Karpagam University,Pollachi Main Road, Eachanari Post, Coimbatore 641021, India.
[2]Research Supervisor, Karpagam University, Professor, Department of Computer Science and Engineering, Jaya Engineering College, CTH Road, Prakash Nagar, Thiruninravur, Thiruvallur - Dist, Tamilnadu.

ABSTRACT

Cloud computing can be defined as an application and services which runs on distributed network using virtualized and it is accessed through internet protocols and networking. Cloud computing resources and virtual and limitless and information's of the physical systems on which software running are abstracted from the user. Cloud Computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. To satisfy the needs of the users the concept is to incorporate technologies which have the common theme of reliance on the internet Software and data are stored on the servers whereas cloud computing services are provided through applications online which can be accessed from web browsers. Lack of security and access control is the major drawback in the cloud computing as the users deal with sensitive data to public clouds .Multiple virtual machine in cloud can access insecure information flows as service provider; therefore to implement the cloud it is necessary to build security. Therefore the main aim of this paper is to provide cloud computing security through symmetric cipher model. This article proposes symmetric cipher model in order to implement cloud computing security so that data can accessed and stored securely.

KEYWORDS

Cloud computing, virtualized resources, virtual machines, symmetric cipher model, cloud security, cloud services.

1. INTRODUCTION

Cloud computing is a paradigm that focuses on sharing data and computations over a scalable network of nodes, spanning across end user computers, data centers, and web services. Nodes from scalable network form a cloud. Applications which are bases on these clouds are considered as a cloud application. Most of the developed software's are based distributed architecture's, such as service-oriented,P2P & cloud computing. The representation of real paradigm shift in which way the systems are deployed is done by the cloud computing. Growth of some large service companies and popularization of the internet enables massive scale of cloud computing systems. The long-held dream of possible computing utility can be implemented with a pay-as-you-go, infinitely scalable and it is universally available system. To start the cloud computing is very small and with this it can become big and very fast. Because of this cloud computing is revolutionary and the technology also builds on evolutionary.

DOI:10.5121/ijcsit.2014.6304

At the end of users, traditionally data's are stored on computers whereas in cloud computing, a data center holds the information. Therefore it requires privacy protection as the users must outsource their data. Moving to centralized services leads to the privacy and security issues in the user's interactions. During the execution of distributed application and provisioning of resource security threats might happen and there is chance of new threats, for example virtualized infrastructure can use as launching padding for creating new attacks. Cloud should preserve user privacy and data integrity. They should also enhance interoperability across multiple cloud service providers. Therefore there is need to investigate new data protection policies to secure the data, resource security and content copyrights.

The main aim is to focus on problems which are associated with security of clouds and to propose security throw symmetric cipher model in cloud computing. The research paper is organized as sections i.e., section 2 provides literature review, section 3 demonstrates proposed work and section 4 represents the conclusion of the paper.

2. Related Work

2.1 Cloud Architectures

To make the cloud architecture mainly refers to the components and subcomponents which are required for cloud computing. The main components are, front end platforms and back end platforms, front end platforms are fat client, thin client, mobile device etc. and back end platforms are servers, storage etc., it also requires cloud based deliver and a network such as internet, intranet, intercloud etc.

Front-end platforms such as clients or cloud clients present in cloud computing architectures. Clients comprise servers, fat, thin and zero clients; they also comprise tablets and mobile devices. The data storage in the cloud interacts through an applications such as web browser, or through a virtual sessions.

The architecture of the cloud computing provides the cloud solutions to various system, and it comprise on various components such as cloud resources, services, middleware and software component, geo-locations and its externally visible properties and relations between them. Documenting facilitates communication between stakeholders, documents early decisions about high-level design, and allows reuse of design components and patterns between projects. Figure 1 shows the cloud computing architecture.

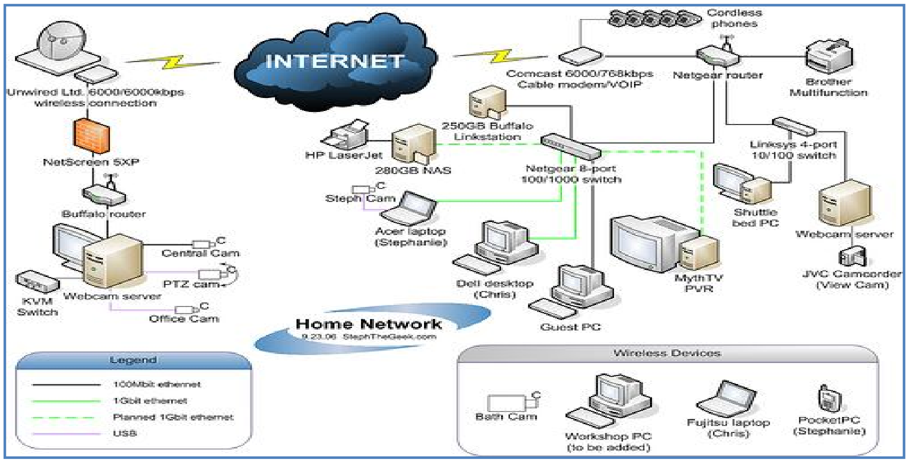

Figure 1 Cloud computing architecture

2.2 Cloud Computing Services

There are three types of architectures for cloud computing to be categorized according to their service models, such as Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS).

2.2.1 Infrastructure as a Service (IaaS)

Cloud computing vendor's dedicated resources are only shared with contracted client at a pay-per-use fee, where Infrastructure is Service to single tenant cloud layer. With this huge initial invest in computing hardware such as servers, networking devices and processing power will be greatly minimized. IaaS allow Varying degrees of financial and functional flexibility is not found in internal data centers or with co-location services, computing resources and can be added or released quickly and it can be cost effectively then in internal data center or with a collocation service[8].

2.2.2 Software as a Service (SaaS)

Through specialized Saas vendor's software applications are leased to contracted organizations where software services are operated on pay-per-use costing mode and virtualized and which can be accessed through web browser via internet. The core pack of the software is limited but its functionality can be expanded and Contracted through easy customization which is billed accordingly. Saas provider can host through own data centers or with co-location providers, or it can be outsourced to other Sass providers. The key enabler of the SaaS model is, availability of IaaS services [9].security is vitally important as software service applications are accessed using web browsers over the Internet. to consider the various methods of securing SaaS applications, the information security officers are responsible. The data protection can be enforced through internet services such as Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL)

2.2.3Platform as a Service (PaaS)

IaaS provides platform as service to cloud as well as it provides additional level of rented functionality. To transfer costs from capital investment to operational expenses clients uses PaaS as service but they must acknowledge the constraints and has to implement some degree of lock-in posed by the additional functionality layers [6] .The use of virtual machines acts as catalyst in cloud computing PaaS layer. Malicious attacks such as cloud malware must be protected in the virtual machines The fundamental need is to enforce accurate authentication over entire networking channels to accurate authentication check during the transfer of data, therefore maintaining of the integrity of applications are also necessary. Figure 2 demonstrates the cloud services.

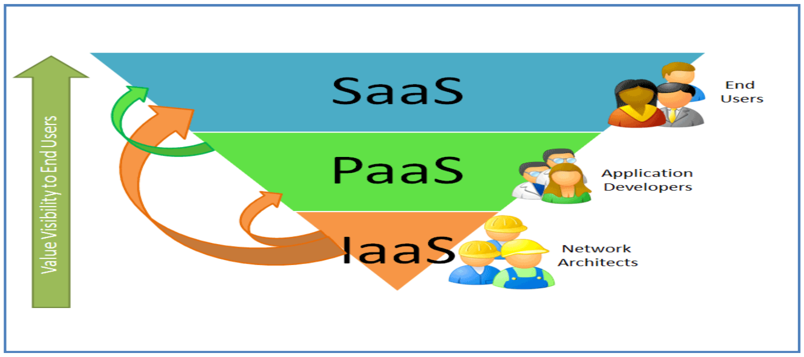

Figure 1.2 shows the Cloud services

2.3 Types of Cloud

While providing secure cloud computing solution, the major decision is to decide which type of cloud is to be implemented. Right now there are three types of cloud deployment models, namely, a public, private and hybrid cloud. The security implications are discussed below.

2.3.1 Public Cloud

The cloud which allows the users to access interfaces using mainstream web browsers are called public cloud models. Pay-per-use model is similar to prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. The Cloud clients can compare their IT expenditure to an operational level through decreasing its capital expenditure on IT infrastructure. [4]. Public clouds are less secure than various other cloud models as it places an additional burden of ensuring all applications and data accessed on the public cloud which are not subjected to malicious attacks. When dealing with Public clouds trust and privacy concerns are rife, with the cloud SLA at its core. Key management can be answered through SLA dealing by ensuring that ample security controls are put in place. In enforcing cloud check and validation across their own systems, both the cloud vendor and client mutually agree to share joint responsibility. Within the utilization boundaries, each party can set out individual roles and responsibility in order to deal with cloud computing security.

2.3.2 Private Cloud

A private cloud is set up within an organization’s internal enterprise datacenter. To provide more enterprise control over deployment and use, it is easier to align with security, compliance, and regulatory requirements. 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. To operate the specific Private cloud only the organization and designated stakeholders may have access. [5].

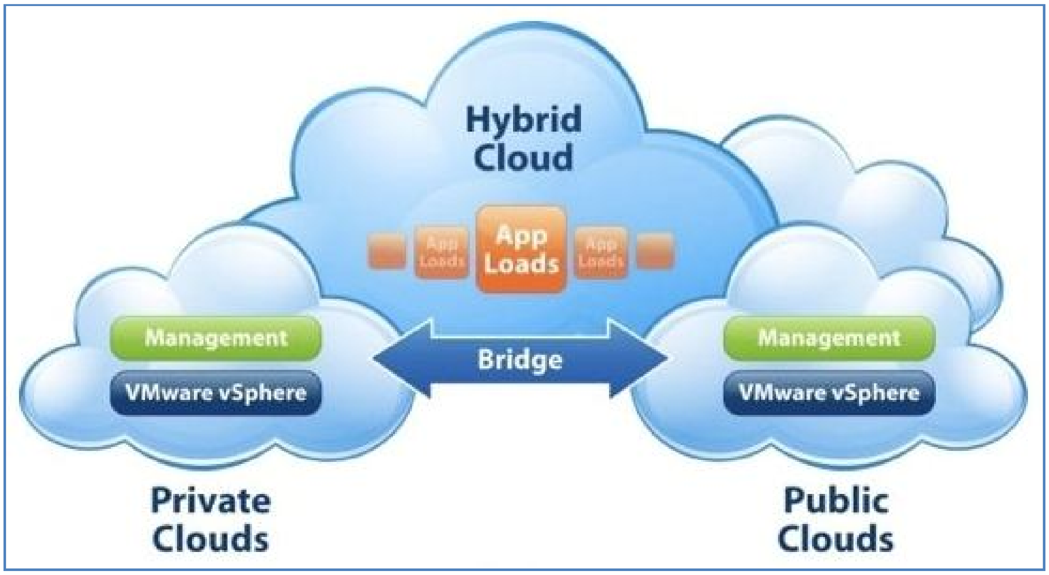

Figure 3 demonstrates Cloud Models

2.3.3 Hybrid Cloud

A cloud which are linked to one or more external cloud services are called a hybrid cloud and they are centrally managed, provisioned as a single unit, and circumscribed by a secure network [6]. Hybrid cloud is a mix of both public and private clouds which provides virtual IT solutions. Hybrid clouds allow various parties to access information over the Internet with a secure control of the data and applications. It has open architecture which allows interfaces to manage the systems. In the cloud deployment model services are provided as Networking, platform, storage, and software infrastructure which scale up or down depending on the demand. The business managers decide which type of cloud to deploy depending upon holistically assess the security consideration from an enterprise architectural point of view, taking information security as key point of each cloud deployment model which are mentioned above. Figure 3 shows the models of cloud.

2.4 Cloud Computing Security Issues

The largest security concern in most organization in cloud computing is securing data sent to, received from. As with any WAN traffic, we must assume that any data can be intercepted and modified. That’s why, as a matter of course, traffic to a cloud service provider and stored off-premises are encrypted. This is as true for general data as it is for any passwords or account IDs. These are the key mechanisms for protecting data mechanisms.

2.4.1 Identification & authentication

Depending upon the type of cloud as well as the delivery model in cloud computing, the specified users must be granted supplementary access priorities and permissions. This process targets at verifying and validating cloud users through usernames and passwords protections in the cloud profiles.

2.4.2 Authorization

In cloud computing to maintain referential integrity, authorization is an important information security requirement. It controls and privileges over process flow within cloud computing. The authorization is maintained by the system administrator in the private cloud.

2.4.3 Confidentiality

Confidentiality play an major role in cloud computing to maintain and control over organizations data which are situated across multiple distributed databases. It is must to employee a public cloud due to public clouds accessibility nature. There is a necessary to enforce security protocols at various different layers of cloud application to assert confidentiality of user's profiles and protecting their data.

2.4.4 Integrity

While accessing data, integrity requirement lies in applying the due diligence within the cloud domain. Therefore ACID (atomicity, consistency, isolation and durability) properties of the clouds' data should be robustly imposed across all deliver models of cloud computing.

2.4.5 Non-repudiation

Non-repudiation in Cloud computing can be obtained by applying the traditional e-commerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services (digital receipting of messages confirming data sent/received).

2.4.6 Availability

In the cloud computing the key decision factor is availability of most critical information security when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document to highlight the trepidation of availability in cloud services and resources between the cloud provider and client.

3. Proposed Approach

To manage effectively and to control the users of cloud technology in organization, business and strategic decision makers, they need to begin with assessing the potential impact of cloud computing. Therefore there is a need to build up proper security for cloud implementation. Therefore the main aim of this paper is to provide cloud computing security through symmetric cipher model. This article proposes symmetric cipher model in order to implement cloud computing security so that data can accessed and stored securely.

3.1 Symmetric Cipher Model

Symmetric encryption also referred as conventional encryption or single-key encryption, was the only type of encryption in use prior to the development of public key encryption in the 1970's. Symmetric Encryption model has 5 components like

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
Encryption Algorithm: In order to perform transformations and substitutions on the plain text.
Secret Key (Input): The secret key is also input to the encryption algorithm, the key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

Cipher Text: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. Ciphertext text consists of random stream of data and it is unintelligible.

Decryption Algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

The main requirements for conventional encryption to make secure to use are following:

- We need a strong encryption algorithm. We will make the algorithm in such a way that an opponent who knows the algorithm can access one or more ciphertexts and unable to decipher the ciphertext or figure out the key. It is generally stated as stronger form of requirement. The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover they key and knows the algorithm, all communication using this key is readable. All communication using the key is readable if anyone who discovers the key and knows the algorithm.

Selecting and implementing the suitable cloud security architecture is not simple therefore in this paper we propose symmetric cipher model in the cloud computing to provide security for the cloud services. The following figure 4 shows the implementation of symmetric cipher model in the cloud computing.

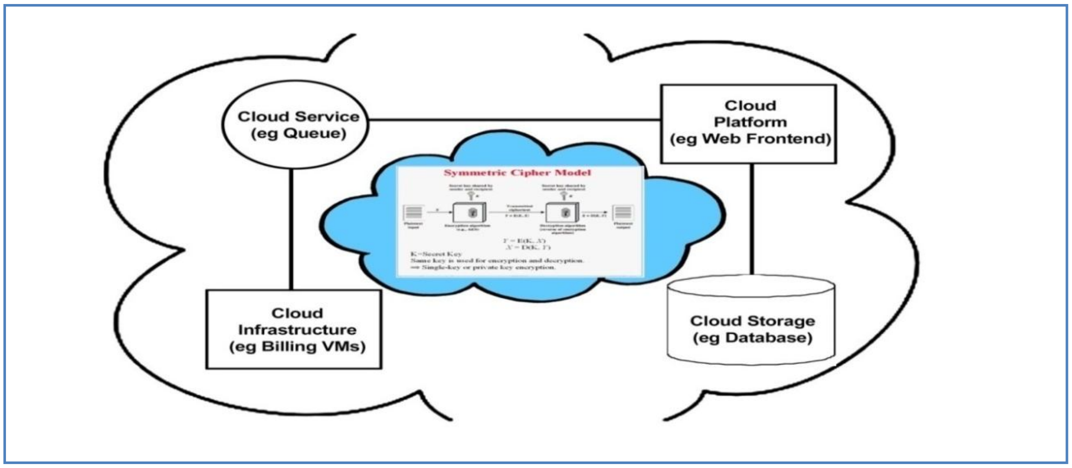
Cloud Service (eg Queue)
Cloud Platform (eg Web Frontend)
Symmetric Cipher Model
Y = E(K, X)
X = D(K, Y)
K=Secret Key
Same key is used for encryption and decryption.
⇒ Single-key or private key encryption.
Cloud Infrastructure (eg Billing VMs)
Cloud Storage (eg Database)

Figure 4 Symmetric cipher Model in cloud architecture

4. Case study and Experimental Results

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing. Figure 5 and 6 shows the secret key cryptography and public key cryptography.

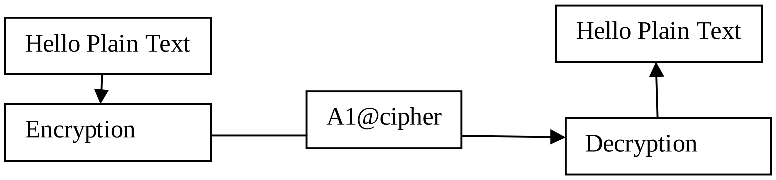

Figure 5 Secret Key Cryptography

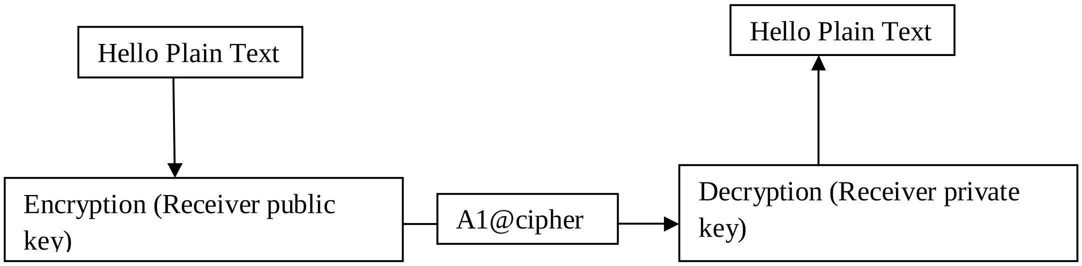
Hello Plain Text
Encryption (Receiver public key)
A1@cipher
Hello Plain Text
Decryption (Receiver private key)

Figure 6 Public Key Cryptography

Block cipher scheme encrypts one block of data at single time using same key on each block, since it works on block of data it is so called as Block cipher. Generally same plaintext block will encrypt same ciphertext always. While using the same key in a block cipher, the same plaintext will encrypt to different ciphertext in a stream cipher [19].There are different types of stream ciphers but we are discussing two important which are worth full. Each bit in the key stream as a function of the previous n bits in the key stream, which is calculated through Self-synchronizing stream ciphers. It is called self-synchronizing because the decryption process can be synchronized with encryption process knowing the n-bit key stream. Generating key stream independent of the message stream is done by synchronous stream ciphers but it uses same key stream to generate function at sender and receiver side. Stream ciphers do not generate any transmission errors but periodically it repeats key stream. Block ciphers can be operated on four most important modes: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) mode and Output Feedback (OFB). commonly used cryptography secret-key scheme is (DES)Data Encryption Standard, which is developed by IBM in 1970's and again it is adopted by National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for the usages of commercial and unclassified government applications. For the federal information processing DES has been adopted. Standard 46 (FIPS 46- 3) and by the American National Standards Institute as X3.92).DES is a block-cipher which implements 56-bit key to operates on 64-bit blocks [20]. the various secret-key cryptography algorithms which are used today are CAST-128 (block cipher), RC2 (block cipher) RC4 (stream cipher), RC5 (block cipher), Blowfish (block cipher), Two fish (block cipher).NIST developed a secure cryptosystem for U.S. government applications in the year 1997, which has resulted to Advanced Encryption Standard (AES), and it became the official successor to DES in December 2001.

4.1 New Symmetric Key Algorithm

4.1.1 Encryption algorithm

Step 1: First develop an ASCII value for a letter.
Step 2: Generate the corresponding binary value of it.
[Make the binary value to 8 digits for example for decimal value for 32 binary numbers is 00100000]
Step 3: The 8 digit's binary number should be reversed.
Step 4: The key can be taken as 4 digits divisor (>=1000).
Step 5: The divisor should be divided with reversed number.
Step 6: remainder and quotient should be stored in first 3 and 5 digits.(quotient and remainder should be more than 3 and 5 digits long, if they are less than 3 and 5 digits we have to add required number of 0s(Zero's) to its left hand side and now it would be a the ciphertext or encrypted text.)

Now we can store the quotient in next 5 digits and remainder in first 3 digits.

4.1.2 Decryption algorithm

Step 1: The key is multiplies by the last 5 digits of the ciphertext.
Step 2: The result which is produced in the previous step is added with first 3 digits of the ciphertext
Step 3: if step2 does not produce 8-bit number we need to make to 8-bit number.
Step 4: To get the original or the plain text reverse the number

4.2 Example

Let, the character is “T”. As per the give steps we will get following result:
Step 1: ASCII of “T” is 84 in decimal.
Step 2: The Binary value of 84 is 1010100. As per the encryption algorithm, as it is not 8 bit binary number we have to make it 8 bit binary number. Therefore it would be 01010100.

0	1	0	1	0	1	0	0

Step 3: 00101010 is the reverse of binary number.

0	0	1	0	1	0	1	0

Step 4: Let 1000 as divisor i.e. Key
Step 5: Divide the dividend by divisor i.e. 00101010 by 1000.
Step 6: The remainder is 10 and quotient is 101. therefore according to the algorithm the ciphertext is 01000101 and its ASCII is 69 in decimal i.e. "E".

0	1	0	0	0	1	0	1

4.3 Advantages of the New Algorithm

1. Simple algorithm in nature.
2. The two reverse operations makes algorithms more secured.
3. Receiving ends is easier as CRC checking present.
4. For less amount of data this algorithm works well.

5. Conclusion

There is much to be cautious to use cloud, even though cloud computing can be a new phenomenon which is set as revolutionize. Many new technologies emerging rapid rate, each with the improvement of technological and making human's lives potential simple and easier. However we must be careful towards the security risks while using these technologies. There is no exception for the cloud computing. In this paper we highlighted security considerations and challenges which are currently faced by the cloud industry. The main aim of this paper is to provide cloud computing security through symmetric cipher model. This article proposes symmetric cipher model with case studies and with experimental analysis in order to implement cloud computing security so that data can be accessed and stored securely.

References

[1] Leavitt N, 2009, 'Is Cloud Computing Really Ready for Prime Time?', *Computer*, Vol. 42, pp. 15-20, 2009.

[2] Weinhardt C, Anandasivam A, Blau B, and Stosser J, 'Business Models in the Service World', *IT Professional*, vol. 11, pp. 28-33, 2009.

[3] Gens F, 2009,' New IDC IT Cloud Services Survey: Top Benefits and Challenges',*IDC eXchange*, viewed 18 February 2010, from <http://blogs.idc.com/ie/?p=730>.

[4] A Platform Computing Whitepaper, 'Enterprise Cloud Computing:Transforming IT', *Platform Computing*, pp6, viewed 13 March 2010.

[5] Dooley B, 2010, 'Architectural Requirements Of The Hybrid Cloud', *Information Management Online*, viewed 10 February 2010, from <http://www.information management.com/news/hybrid-cloudarchitectural- requirements-10017152-1.html>

[6] Global Netoptex Incorporated , 2009, Demystifying the cloud. Important opportunities, crucial choices, http://www.gni.com, pp 4-14, viewed 13 December 2009.

[7] Lofstrand M, 'The VeriScale Architecture: Elasticity and Efficiency for Private Clouds", *Sun Microsystems*, Sun BluePrint, Online, Part No 821-0248-11, Revision 1.1, 09/22/09

[8] Brodkin J, 2008, 'Gartner: Seven cloud-computing security risks',*Infoworld*, viewed 13 March 2009, from http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853?page=0,1

[9] ISO. ISO 7498-2:1989. *Information processing systems- Open Systems Interconnection*. ISO 7498-2

[10] Klems, M, Lenk, A, Nimis, J, Sandholm T and Tai S 2009, 'What's Inside the Cloud? An Architectural Map of the Cloud Landscape', *IEEEXplore*, pp 23-31, viewed 21 June 2009.

[11] Dlamini M T, Eloff M M and Eloff J H P, 'Internet of People, Things and Services – The Convergence of Security, Trust and Privacy', 2009.

[12] Balachandra R K, Ramakrishna P V, Dr. Rakshit A, 'Cloud Security Issues', *2009 IEEE International Conference on Services Computing*, viewed 26 October 2009, pp 517-520.

[13] S. Arnold, 2009,' Cloud computing and the issue of privacy', *KM World*, vol July/August 2008, *www.kmworld.com*, viewed 19 August 2009, pp 14-22.

[14] Soghoian C, 2009 'Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era', *The Berkman Center forInternet & Society Research Publication Series: http://cyber.law.harvard.edu/publications*, viewed 22 August 2009.

[15] Gruschka N, Iancono LL, Jensen M and Schwenk J, 'On Technical Security Issues in Cloud Computing', *'09 IEEE International Conference on Cloud Computing*, pp 110-112, 2009.

[16] Armbrust M, Fox A, Griffith R, Joseph D A, Katz H R, Konwinski A, Lee Gunho, Patterson A D, Rabkin A, Stoica A, Zaharia M, (2009),Above the clouds: A Berkeley view of Cloud Computing, *UC BerkeleyEECS*, Feb 2010

[17] Goldstein, P (2009), The Tower, the Cloud, and the IT leader and workforce, in Katz, R (ed) (2009), *The Tower and the Cloud: Higher Education in the Age of Cloud Computing*, Educause http://www.educause.edu/thetowerandthecloud

[18] Cloud Security Alliance Web site,http://www.cloudsecurityalliance.org/, viewed 19 March 2010

[19] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc.,1999 pp 23-50

[20] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html

Authors

Subramanian Anbazhagan has about twenty years of professional experience in the software industry. He started his career as a Systems Analyst for M/S. SPIC Ltd, Chennai immediately after graduating as a Computer Science Engineer from College of Engineering, Guindy, Anna University, India. He did his Masters in Software Engineering from National University of Singapore. As a senior IT consultant, he had advised various clients in the manufacturing, health care and cosmetics, government services, private and public sector industries. He had successfully implemented various systems using state of the art software technologies and tools.

Dr.K.Somasundaram, Research Guide(Karpagam University), Professor, Department of Computer Science and Engineering, Jaya Engineering College,Thiruvallur,Tamilnadu.