Cloud Security through Key Agreement

Subramanian Anbazhagan, K.Somasundaram

Abstract— Cloud computing refers to applications and services that run on a distributed network using virtualized and accessed by common internet protocols and networking standards. It is distinguished by the notion that resources are virtual and limitless and that details of the physical systems on which software runs 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. The concept incorporates technologies that have the common theme of reliance on the Internet for satisfying the computing needs of the users. Cloud Computing services usually provide applications online that are accessed from a web browser, while the software and data are stored on the servers. As the users deal their sensitive data to clouds i.e. public domains, the major hurdles for cloud adoption are lack of security and access control. The main setback is that the insecure information flows as service provider can access multiple virtual machines in clouds. So it is necessary to build up proper security for cloud implementation. Therefore the main aim of this paper is to provide cloud computing security through secret key using a public-key scheme. This article proposes a protocol which enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established.

Index Terms— Cloud computing, cloud security, cloud services, domains, public-key scheme secret key ,virtualized resources, virtual machines.

I. 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. A scalable network of such nodes forms a cloud. An application based on these clouds is taken as a cloud application. In recent years, most of the developed software's are based on distributed architecture, such as service-oriented, P2P & cloud computing. Cloud computing represents a real paradigm shift in the way in which systems are deployed. The massive scale of cloud computing systems was enabled by the popularization of the internet and the growth of some large service companies. Cloud computing makes the long-held dream of utility computing possible with a pay-as-you-go, infinitely scalable, universally available system. With cloud computing we can start very small and become big very fast. That's why cloud computing is revolutionary, even if the technology it is built on is evolutionary. In cloud computing, a data center holds information that end-users would more traditionally have stored on their computers.

Manuscript received August, 2013.

Subramanian Anbazhagan, Research Scholar (Karpagam University), Computer Science and Engineering, Karpagam University, Pollachi Main Road, Eachanari Post, Coimbatore 641021, India.

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

This raises concerns regarding user privacy protection because users must outsource their data. Additionally, the move to centralized services could affect the privacy and security of users' interactions. Security threats might happen in resource provisioning and during distributed application execution. Also, new threats are likely to emerge. For instance, hackers can use the virtualized infrastructure as a launching pad for new attacks. Cloud services should preserve data integrity and user privacy. At the same time, they should enhance interoperability across multiple cloud service providers. In this context, we must investigate new data-protection mechanisms to secure data privacy, resource security, and content copyrights.

II. RELATED WORK

A. Cloud Architectures

Cloud computing architecture refers to the components and subcomponents required for cloud computing. These components typically consist of a front end platform (fat client, thin client, mobile device), back end platforms (servers, storage), a cloud based delivery, and a network (Internet, Intranet, Intercloud). Combined, these components make up cloud computing architecture.

Cloud computing architectures consist of front-end platforms called clients or cloud clients. These clients comprise servers, fat (or thick) clients, thin clients, zero clients, tablets and mobile devices. These client platforms interact with the cloud data storage via an application (middleware), via a web browser, or through a virtual session.

The Cloud Computing Architecture of a cloud solution is the structure of the system, which comprise on premise and cloud resources, services, middleware, and software components, geo-location, the externally visible properties of those, and the relationships between them. The term also refers to documentation of a system's cloud computing architecture. 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.

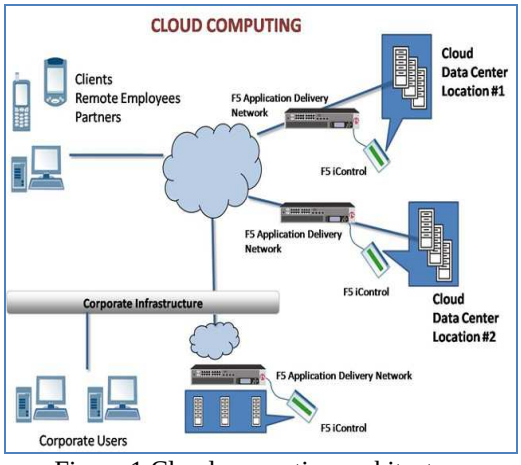

Figure 1 Cloud computing architecture

B. Cloud Computing Services

The architecture of Cloud computing can be categorized according to the three types of service models, namely Infrastructure as a service (IaaS), Software as a service(SaaS) and Platform as a service (PaaS).

*1) **Infrastructure as a Service (IaaS)***

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with co-location services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a collocation service [9]. However, corporate decision makers must be aware of the capital outlay shift from a periodic fixed expense payment reflected on the income statement to an **operational expense increase.**

2) Software as a Service (SaaS)

Software as a Service also operates on the virtualized and pay-per-use costing model whereby software applications are leased out to contracted organizations by specialised SaaS vendors. This is traditionally accessed remotely using a web browser via the Internet. The software has limited functionality and its core pack can be expanded and contracted allowing of easy customisation which is billed accordingly. SaaS providers may host the software in their own data centers or with co-location providers, or may themselves be outsourced to IaaS providers. The availability of IaaS services is a key enabler of the SaaS model[10]. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet.

*3) **Platform as a Service (PaaS)***

Platform as a service cloud layer works like IaaS but it provides an additional level of "rented" functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers[6]. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental. Figure 2 demonstrates the cloud services.

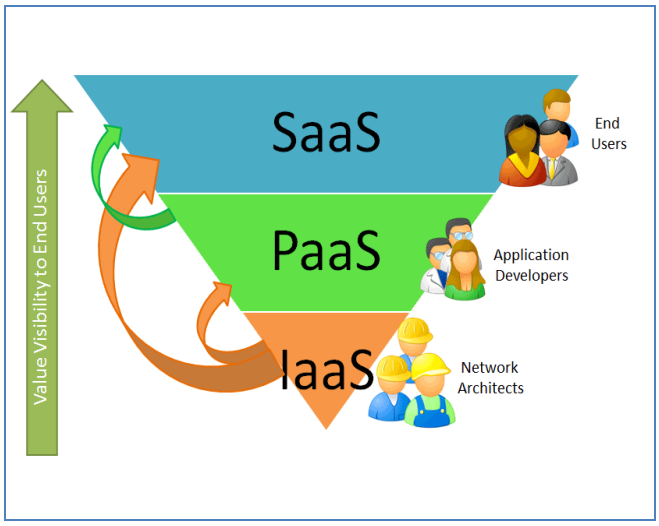

Figure 2 shows the Cloud services

C. Types of Cloud

In providing a secure Cloud computing solution, a major decision is to decide on the type of cloud to be implemented. Currently there are three types of cloud deployment models offered, namely, a public, private and hybrid cloud. These, together with their security implications will be discussed below.

1) Public Cloud

A public cloud is a model which allows users' access to the cloud via interfaces using mainstream web browsers. It's typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. This helps cloud clients to better match their IT expenditure at an operational level by decreasing its capital expenditure on IT infrastructure [4]. 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. Therefore trust and privacy concerns are rife when dealing with Public clouds with the Cloud SLA at its core. A key management consideration, which needs to be answered within the SLA deals with ensuring that ample security controls are put in place. One option is for both the cloud vendor and client mutually agree in sharing joint responsibility in enforcing cloud checks and validation are performed across their own systems. The alternative option will be for each party to set out individual roles and responsibilities in dealing with cloud computing security within their utilization boundaries.

2) Private Cloud

A private cloud is set up within an organization's internal enterprise datacenter. It is easier to align with security, compliance, and regulatory requirements, and provides more enterprise control over deployment and use. 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 [5].

3) Hybrid Cloud

A 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 [6]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Clouds provide more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. To summarize, in the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand. In deciding which type of Cloud to deploy, business managers' needs to holistically assess the security considerations from an enterprise architectural point of view, taking into account the information security differences of each Cloud deployment model mentioned above. Figure 3 shows the models of cloud.

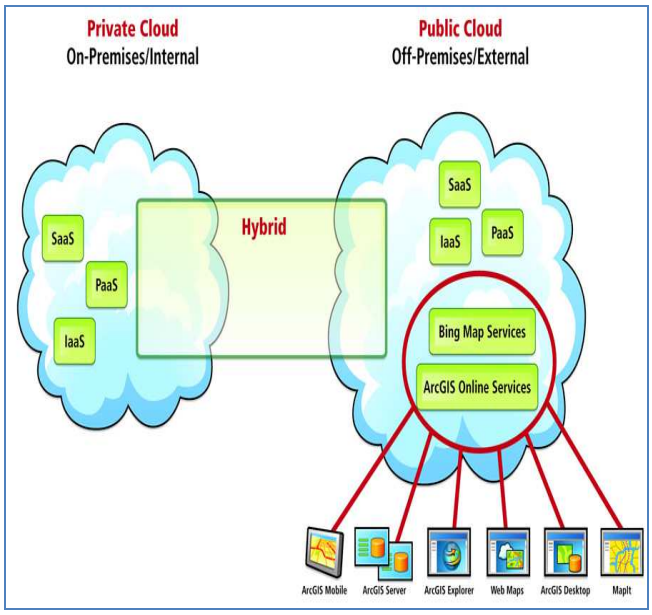

Figure 3 demonstrates Cloud Models

D. Cloud computing security issues

Securing data sent to, received from, and stored in the cloud is the single largest security concern that most organizations should have with cloud computing. 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:

1) Identification & authentication

In Cloud computing, depending on the type of cloud as well as the delivery model, specified users must firstly be established and supplementary access priorities and permissions may be granted accordingly. This process is targeting at verifying and validating individual cloud users by employing usernames and passwords protections to their cloud profiles.

2) Authorization

Authorization is an important information security requirement in Cloud computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within Cloud computing. Authorization is maintained by the system administrator in a Private cloud.

3) Confidentiality

In Cloud computing, confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed databases. It is a must when employing a Public cloud due to public clouds accessibility nature. Asserting confidentiality of users' profiles and protecting their data, that is virtually accessed, allows for information security protocols to be enforced at various different layers of cloud applications.

4) Integrity

The integrity requirement lies in applying the due diligence within the cloud domain mainly when accessing data. Therefore ACID (atomicity, consistency, isolation and durability) properties of the cloud's data should without a doubt be robustly imposed across all Cloud computing deliver models

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).

6) Availability

Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor 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 which highlights the trepidation of availability in cloud services and resources between the cloud provider and client.

III. PROPOSED APPROACH

In order to effectively manage and control the use of cloud technology in an organization, business and strategic decision makers need to begin with assessing the potential impact of Cloud computing on their competitive edge. So it is necessary to build up proper security for cloud implementation. Therefore the main aim of this paper is to provide cloud computing security through secret key using a public-key scheme. This article proposes a protocol which enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established.

A. Diffie Hellman Key Exchange

Asymmetric Encryption of data requires transfer of cryptographic private key. The most challenging part in this type of encryption is the transfer of the encryption key from sender to receiver without anyone intercepting this key in between. This transfer or rather generation on same cryptographic keys at both sides secretively was made possible by the Diffie-Hellman algorithm.

The Diffie-Hellman algorithm was developed by Whitfield Diffie and Martin Hellman in 1976. This algorithm was devices not to encrypt the data but to generate same private cryptographic key at both ends so that there is no need to transfer this key from one communication end to another. Though this algorithm is a bit slow but it is the sheer power of

this algorithm that makes it so popular in encryption key generation.

The beauty of this scheme is that the two parties, who want to communicate securely, can agree on a symmetric key using this technique. This key can be used for encryption/decryption.

However, we must note that Diffie-Hellman key exchange algorithm can be used only for key agreement, but not for encryption or decryption of the message. Once both the parties agree on the key to be used, they need to use other symmetric key encryption algorithm.

B. The Algorithm

This is a 7 step algorithm. Let us understand it with the help of a simple example. Suppose Puli and Snehal want to agree upon a key to be used for encrypting/decrypting message that would be exchanged between them.

Diffie-Hellman Key Exchange Algorithm:

Step 1:Firstly, Puli and Snehal agree upon two large prime numbers, ***n*** *and* ***g****. These two numbers need not be kept secret.*

Step 2:Puli chooses another large number ***x****, and calculate* ***A*** *such that:*

$A=g^x \bmod n$

Step 3:Puli sends the number A to Snehal.

Step 4:Snehal independently chooses another large random integer ***y*** *and calculates* ***B*** *such that:*

$B=g^y \bmod n$

Step 4:Snehal sends the number B to Puli.

Step 5:Puli now computes the secret key ***K1*** *as follows :*

$K1=B^x \bmod n$

Step 6:Snehal now computes the secret key ***K2*** *as follows :*

$K2=A^y \bmod n$

Result:

K1=K2=K =The symmetric key K now becomes the shared symmetric key between Puli and Snehal.

C. Example of Diffie-Hellman Algorithm

Let us take an example:

1. let n=11, g=7

2. let x=3, then we have, $A=g^x \bmod n$

$=7^3 \bmod 11 \quad =343 \bmod 11$

$=2$

3. Puli sends 2 to Snehal.

4. let y=6, then we have, $B=g^y \bmod n$

$=7^6 \bmod 11 \quad =117649 \bmod 11$

$=4$

5. Snehal sends 4 to Puli.

6. Now, we have $K1=B^x \bmod n$

$=4^3 \bmod 11$

$=64 \bmod 11$

$=9$

7. Now, we have $K2=A^y \bmod n$

$=2^6 \bmod 11$

$=64 \bmod 11$

$=9$

As we have seen this algorithm under a very small prime numbers, but in real life these values are very large.

D. Problems with the algorithm Man-in-the-middle attack

A man, say Golani, is an attacker. Lets see how he come to know the key to be shared between Puli and Snehal.

Step1:

Puli	*Golani*	*Snehal*
n=11, g=7	*n=11, g=7*	*n=11, g=7*

Step2:

Puli	*Golani*	*Snehal*
x=3	*x=8, y=6*	*y=9*

step 3:

Puli	*Golani*	*Snehal*
$A=g^x \bmod n$	$A=g^x \bmod n$	$B=g^y \bmod n$
$=7^3 \bmod 11$	$=7^8 \bmod 11$	$=7^9 \bmod 11$
$=343 \bmod 11$	$=5764801 \bmod 11$	$=40353607 \bmod 11$
$=2$	$=9$	$=8$

$B=g^y \bmod n$

$=7^6 \bmod 11$

$=117649 \bmod 11$

$=4$

step 4:	*Puli*	*Golani*	*Snehal*
	*A=2, B=4**	*A=2, B=8*	*A=9*, B=8*

step 5:	*Puli*	*Golani*	*Snehal*
	$K1=B^x \bmod n$	$K1=B^x \bmod n$	$K2=A^y \bmod n$
	$=4^3 \bmod 11$	$=8^8 \bmod 11$	$=9^9 \bmod 11$
	$=64 \bmod 11$	$=16777216 \bmod 11$	$=387420489 \bmod 11$
	$=9$	$=5$	$=5$

$k2=A^y \bmod n$

$=2^6 \bmod 11$

$=64 \bmod 11$

$=9$

At step IV, the real attack happens, Golani intercepts the value of A sent by the Puli to Snehal his own A instead. Moreover, Golani intercepts the value of B sent by Snehal to Puli and sends Puli his own B, instead.

From this we can conclude that man-in-the-middle attack can work against the Diffie-Hellman key exchange algorithm, causing it to fail.

This is plainly because the man-in-the-middle makes the actual communicators believe that they are talking to each other, whereas they are actually talking to man-in-the-middle, who is talking to each of them!

The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates. This could be our future research work in the cloud computing.

IV. CONCLUSION

Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However one must be very careful to understand the limitations and security risks posed in utilizing these technologies, Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing industry are highlighted. The main aim of this paper is to provide cloud computing security through secret key using a public-key scheme. This article proposes a protocol which enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established.

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] Goia M, 'Cloud computing, grid computing, utility computing – list of top providers', http://www.123people.com/ext/frm?ti=personensuche%20telefonbuch& search_term=infosolve%20technologies&search_country=US&st=suche %20nach%20personen&target_url=http%3A%2F%2Flrd.yahooapis.com%2F_ylc%3DX3oDMTVnc2pvM2dpBF9TAzIwMjMxNTI3MDIEYXBwaWQDc1k3Wlo2clYzNEhSZm5ZdGVmcmkzRUx4VG5makpERG5QOWVKV1NGSkJHcTJ1V1dFa0xVdm5IYnNBeUNyVkd5Y2REVElUX2tlBGNsaWVudANib3NzBHNlcnZpY2UDQk9TUwRzbGsDdGl0bGUEc3JjcHZpZANPUHZlVzJLSWNycVFrRjFySGpwMDRDVzZXODV4Wmt2bHMxTUFESnRt%2FSIG%3D13g7vo71f%2F**http%253A%2F%2Fwww.mytestbox.com%2Fmiscellaneous%2Fcloud-computing-gridcomputing-utility-computing-list-topproviders%2F&section=biography&wrt_id=110, viewed 22 Feb 2010.
[9] 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>
[10] ISO. ISO 7498-2:1989. Information processing systems- Open Systems Interconnection. ISO 7498-2
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] Soghoian C, 2009 'Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era', The Berkman Cente for Internet & Society Research Publication Series: http://cyber.law.harvard.edu/publications, viewed 22 August 2009.
[16] Gruschka N, Iancono LL, Jensen M and Schwenk J, '09 IEEE International Conference on Cloud Computing, pp 110-112, 2009.
[17] 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 Berkeley EECS, Feb 2010
[18] Goldstein, P (2009), The Tower, the Cloud, and the IT leader andorkforce, in Katz, R (ed) (2009), The Tower and the Cloud: Higher Education in the Age of Cloud Computing, Educause http://www.educause.edu/thetowerandthecloud
[19] Cloud Security Alliance Web site, http://www.cloudsecurityalliance.org/, viewed 19 March 2010
[20] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc.,1999 pp 23-50
[21] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html

Subramanian Anbazhagan, Research Scholar (Karpagam University), Computer Science and Engineering, Karpagam University, Pollachi Main Road, Eachanari Post, Coimbatore 641021, India.

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.