World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 1, No. 7,283-288, 2011

Quantum Attack Resistant Cloud

Asst.Prof .PSV Vachaspati
Dept.of CSE,
Bapatla Engg.college
Bapatla,AP,India
psvvachapati@yahoo.com

Prof.P.S.Avadhani
Dept.of CS&SE,
AU college of Engg.
Vizag,AP,India
psavadhani@yahoo.com

Abstract— The emergence of cloud computing in the computing arena has had a major effect in a way we utilize computing resources. It is being heralded by many as the new computing paradigm, coming with disruptive technologies which are expected to foster all sorts of innovations. However, further investigations suggest that the cloud computing is nothing new, rather an evolution of different existing technologies creatively integrated together. Therefore, it has inherited strengths and weaknesses of existing technologies, but has lowered the entry bar to computing making it an interesting proposition. In this paper we propose quantum attack resistant cloud computing.

Keywords- Cloud Computing; quantum attack; lattice cryptography; Cloud Providers.

I.INTRODUCTION

The cloud computing model is composed of five characteristics, which are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured services. It has three service models; software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Cloud computing can be deployed as a private cloud, community cloud, public cloud or hybrid cloud.

There is no agreement on its definition this has led to all sorts of definitions being proposed. For example, NIST defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [24]. The lack of clear definition is a source of confusion in the design and implementation of cloud computing solutions.

While currently the use of cloud computing for personal use is widespread. Most researchers and practitioners recommend caution before using it for critical applications. Specifically, users or organizations are required to inquire on the following issues from the cloud providers: privileged user access, regulatory compliance – external security audits and security certifications, data location, data segregation and use of data protection routines such as encryption,

Recovery, investigative support and long term viability (hosting, scalability, instant provision and cost saving). Answers from these issues will allow them to make an informed decision on whether to move their sensitive data or critical applications to the cloud.

In the next few years Cloud computing spending worldwide will continue to grow. For example IDC predicts IT cloud service spending to grow from about $6 billion in 2008 to about $42 billion by 2012 accounting for 25 percent annual IT expenditure growth [16]. This growth highlights the potential of cloud computing in the technological development and the realization of the industry of the new kind in the computing arena. Cloud computing has the potential to set a stage for company innovation (through networking, remote access and collaboration) as more resources are devoted to developing solutions rather than the traditional chores of maintenance and upgrades.

The main advantages of cloud computing are cost saving, high availability, and easy scalability [17]. It frees the use the user from the hassle of having to install and maintain the software at the cost of the user security, privacy and loss of control of platforms, data and information. Cloud computing lowers the cost of application development and makes the process to be truly distributed and scalable. This enable startup companies into enter the process at the lowest cost. There are still a number of challenges which cloud computing must address for it to be a success. These include reliability, security, privacy, user loss of control of data and information, the additional cost of the necessary bandwidth, and the dangers of vendor lock-in into specific cloud vendor. Is cloud computing a disruptive scientific innovation we have been waiting, which is going to shake the foundations of computing and provide a paradigm shift? The challenges it faces are many and formidable, the computing industry and the academic community have their work cut out. However, the potential for being successful are huge, therefore it is a matter of time before we know the verdict on the future of cloud computing.

In this paper we analyze and provide solutions to the specific security challenges which must be addressed in the cloud. As there is a lot of progresses in the quantum computing the adversaries are equipped with quantum computing power .we have to resist them.

The rest of the paper is organized as follows. In section two we give background and related information to cloud computing. The data ownership, processing, control, movement and trust issues are discussed in section three Section four looks at the security challenges, possible attacks and proposed solutions in the cloud computing. Summary and conclusions are discussed in section five.

II. BACKGROUND AND RELATED INFORMATION

Conceptually cloud computing is attractive, because it means less management, more scalability, possibly broader access (particularly for companies with multiple locations, teleworkers and flexible working). However, there is a perception among consumers that the company computing infrastructure remains more secure and highly accessible when everything is held internally. This viewpoint is likely to be challenged by the technological trends that suggest cloud computing is the only game in town.

It is evident that the Cloud computing has the potential to be a game changer in the computing landscape. Research shows that it has attracted vendors, consumers and even governments. Major vendors providing cloud computing are Amazon [3], Google [14], Salesforce [25] and Microsoft [18]. Other players include AppNexus [4], GoGrid [13], GridLayer [15], Mosso [19], and XCalibre Communications [7]. It will become the foundation for a greatly expanded IT industry by lowering cost and technical barriers to developers and users alike. A key will be whether it overcomes the challenges it currently faces.

The use of cloud computing will be enhanced and extended by other seemingly unrelated computing paradigms such as Autonomics computing which is an initiative started by IBM to provide the computing system with the ability to manage itself in computing landscape which is complex. Autonomics computing can help in addressing the following systems behavior in cloud computing [5]:

- Management of unpredictable system behavior and unforeseen user behavior and abuse.
- Better management of quality of service, primarily to gain greater confidence from the user community, thereby adding value to existing deployment.
- Better management of energy consumption.
- More effective resource management to support scalability so that resources behave elastically at higher usage levels.

The role of the traditional Operating Systems (OS) is changing with the advent of new computing approaches such as virtualization, cloud computing and other application development frameworks (ADF) which enable the faster development of applications that work with multiple Oss making traditional OS less important (key players in the ADF market include Django, Ruby on Rails and Microsoft Silverlight) [11]. This change will spur a rush towards new innovations and competition in the quest for producing a dominating Operating System. The obvious victim of this rush is likely to be security and privacy in OS. The usual story then repeats that once the Operating System is insecure the applications running on top will be insecure as well.

Cloud computing have ignited the old war on Operating Systems domination. In the last few years a lot of cloud aware operating systems have been made available. For example, the private cloud – EyeOS [10] and their collaboration with IBM.Google ChromeOS is another cloud OS that is more internet aware than most [20]. Part of the security scheme for Chrome is that it's hard to make any unauthorized changes to the system. The root file system, which stores the core files needed to make software run, is stored in a read-only format. On top of that, every time the user boots the machine, ChromeOS verifies cryptographic signatures that ensure that the operating system software is properly updated, and matches the build Google has approved.

There is a great deal of truth that cloud providers like Google can maintain the security of systems better than individual companies. This specifically involves server security and not data security. The reasons for this are that companies must trust Google, the privacy of their data cannot be guaranteed and Google is much bigger and attractive target for hackers [28]. When you use cloud computing services, you are limiting yourself to the amount of advanced security tools that you can put on the system. Tools such as data leak prevention (DLP), and misuse and abuse detection. Further, you cannot limit the access to only internal staff. There are many other cloud security tools that cannot be put in place in cloud environments, unless the cloud environment is specifically designed for them [9]. You have little control over how much audit information is collected. For example, you likely do not have access to failed log-in attempts, so you cannot proactively look for attack reconnaissance. Likewise, while you may maintain the ownership of your own data, you do not likely own all of the access log data. That potentially creates legal problems. For example, if someone does illicitly access your information, you might need to get a court order to see where they are coming from. If however you maintained your data

internally, you would have instant access to all this information.

A. Cloud Computing Challenges

Cloud computing is still relatively new and has not yet been widely adopted. There are a lot of challenges to be addressed by the computing industry and researchers.

Most of the Cloud computing resources will be based outside of the organization. Therefore its designs and platforms are controlled by the provider. More worrying is that users cannot change the platform's technology when they want, while providers can do so when and how they see fit in most cases without the consent of the users.

Performance concerns may prevent some companies from using cloud computing for transaction oriented and other data intensive applications. Security and privacy are the main concerns when companies think of using cloud computing. This is because their business information and critical IT resources are outside the company firewall. Users worry about the security and privacy of their information should there be a security break. They want to be sure that providers follow standard security practices, which requires disclosure and inspection. For example, users do not want to share the same virtual hardware and network resources with multiple customers. Another concern is that information can be anywhere in the world, making it subjected to national and international data storage laws related to privacy and record keeping. Various governments or regional bodies such as EU, have privacy regulations that prohibit the transmission of some types of personal data outside their jurisdiction. In the last decade there have been significant improvements in the design and rollout of large bandwidth. However, depending on the model of cloud computing usage, the bandwidth cost can turn out being very high. For example, if a company makes a multi-terabyte database available via cloud computing the cost can be prohibitive. There are few open cloud computing standards for elements and processes such as APIs, the storage server images for disaster recovery, and data import and export. This is hampering adoption by limiting portability of data and applications between systems. Portability will become more important as more cloud providers emerge and the market become more competitive. It can be difficult for companies to move from one provider to another or to bring back data into their internal systems. Even when they bring back data the efforts involved in reformatting data and applications is going to be expensive as the company may be required to acquire new skills from outside the company. As a part of the service level agreement (SLA), Cloud providers must demonstrate that their systems will provide the necessary audit and protection of user's information. They must be able to show how they keep unauthorized personnel from accessing user's information. In some cases providers have allowed third parties to conduct security audit and document in order that it can be used by potential customers to show the due diligence paid by the provider in securing its systems. Experience shows that it is not easy for cloud providers to demonstrate all these aspects in order to instill trust on the part of users.

Users should be realistic in their view of loss of control by comparing their ability against that of the third party in terms of supporting high availability, continuity, disaster recovery, power consumption, and the on-going management of technical and physical infrastructure. Therefore, demonstrating cloud computing benefits is going to be a hard task, especially in the light of high user expectations. Cloud computing usage is going to be a business driver and hence any considerable loss of service will have negative repercussions on the business. Internet access is crucial for cloud computing provision .There are a lot of places in the world where the internet availability is still a problem. This issue must be resolved by the governments in order to ensure that there is equity in the availability of the internet. Therefore, technological, sociological and political challenges must be overcome for this to be a reality. Otherwise we are going to have a cloud computing divide which will consignee these communities to the dark ages of computing. The number of cloud providers is still very small to provide enough competition in the market place that will offer better quality of service and increase choice to users. It is also true that some computing problems may not for the time being, be solved in the cloud. Problems such as high-end databases are better hosted within a dedicated environment or applications that process sensitive information.

B. Emerging Cloud Computing Standards and legislations

Benjamin Tom have in his paper "on standards and how dysfunctional they are" makes an observation that, the standards process is littered with vendor self-interest, infighting and politics to such an extent that the merits and the emerging standards are watered down [27].Five cloud computing standards are emerging to provide interoperability and prevent vendor lock-in. The first standard is the Open Cloud Manifesto [22], which is a set of principles defining cloud computing and steps for keeping cloud systems interoperable. The Open Virtualization Format is the specification [1], proposed by the Distributed Management Task Force, which aims to make virtualization simpler by having vendors agree to metadata formats for virtual machines is the second standard. The third standard is being proposed by the Organization for the Advancement of Structured Information Standards [21]. The group that developed XML is working on specification for cloud deployment, management and security. The Open Cloud Computing Interface, proposed by the Open Grid Forum [23] is the standard application programming interface for cloud infrastructure

systems is the fourth standard. The fifth set of standards is the Trusted Cloud, which are security standards for cloud computing, including identity management, under development by the Cloud Security Alliance [2]. There are currently no security standards for cloud computing, until such standards have been developed, and used effectively to measure provider services and enforce accountability, any failures will fall on the customer's in house IT organization. In understanding of this reality, companies should be careful about putting mission-critical and core processes into a public cloud, and private cloud architectures should be designed to minimize any security concerns while realizing the benefits of cloud optimization. Governments and standards bodies should provide a well-coordinated support in the form of necessary standards, guidance, policy decisions, and issue resolution to ensure agencies have the necessary tools to efficiently plan and carry out migrations to cloud environments.

All Cloud providers use APIs that have the structure of Web services standards such as SOAP. The major problem with these APIs is that they are still proprietary because they use the provider's own semantics within the standards structures. This is going to have a major impact on user's ability to move their data from one provider to the next to avail of better services or cost. The threat of vendor lock-in becomes really in this mode of operation. In the long run innovation is going to suffer and cloud computing as a paradigm may not achieve its full potential.

In cloud computing there are a lot of concerns regarding data security, privacy, and legal compliance. Worse, data stored online has less privacy protection both in practice and under the law. It is the responsibility of the company to develop controls that ensures that the vendor chosen will have the appropriate controls in place and are in compliance with laws such as the Sarbanes-Oxley act, the Gramm-Leach-Bliley act, various regional data privacy regulations such as EU Directive 95/46/EC - The Data Protection Directive, and in some cases country specific regulations limitations.

III. DATA PROCESSING IN THE CLOUD AND SERVICE LEVEL AGREEMENT

There are several criteria used to charge user's such as time spend on the cloud system, level of consumption of resources such as bandwidth, data transferred, or storage space used. These charging mechanisms will improve and very likely become affordable as the cloud matures. Other forms of charging will be possible, such as security and privacy levels afforded to the data and the level of control to data by using audit or forensics tools.

A. Data ownership, control and trust

The question of data ownership is becoming more difficult and confusing by the day. For example in US once you submit data online you cannot claim ownership of it. Furthermore, the data can be sold modified without your consent. Users of cloud computing are worried and likely so that they loose control of their data and information. Closer analysis shows that data is given much better protection when in the hands of cloud service providers. The regulatory compliance requires that there is transparency in data and information processing. However, for the cloud computing to be successful then credibility and trust of the provider will be critical. We trust different providers with our data, but some of the data processed in cloud computing is sensitive and hence the reluctance of users. The problem is further compounded because along the information value chain, everyone "owns" either the tangible or intangible value of data depending on their role within or across elements of the value chain. These roles can be data creators, data providers, data enrichers, data buyers, data consumers, data sponsors, and data regulators. It is therefore reasonable to assume that an individual or a group takes on one or more roles at any given point in time. [32]

IV.POSSIBLE ATTACKS TO THE CLOUD COMPUTING

Cloud computing uses the Web as a means to access the infinite resources it aims to provide. Using the Web leaves the data and information being processed vulnerable to Web information disclosure.

Public key cryptography, a central concept in cryptography, is used to protect web transactions, and its security relies on the hardness of certain number theoretic problems. As it turns out, number theoretic problems are also the main place where quantum computers have been shown to have exponential speedups. Examples of such problems include factoring and discrete log [38A], Pell's equation [18A], and computing the unit group and class group of a number field [17A, 37A]. The existence of these algorithms implies that a quantum computer could break RSA, Diffie-Hellman and elliptic curve cryptography, which are currently used, as well as potentially more secure systems such as the Buchmann-Williams key-exchange protocol Understanding which cryptosystems are secure against quantum computers is one of the fundamental questions in the field.

V. PROPOSED SOLUTION

The GGH public key cryptosystem The GGH cryptosystem, proposed by Goldreich, Goldwasser, and Halevi in [19A], is essentially a lattice analogue of the McEliece cryptosystem [46A] proposed 20 years earlier based on the hardness of decoding linear codes over finite fields. The basic idea is very simple and appealing. The motivation for the introduction of these cryptosystems was twofold. First, it is certainly of interest to have cryptosystems based on a variety of hard mathematical problems, since then a breakthrough in solving one

mathematical problem does not compromise the security of all systems. Second, lattice-based cryptosystems are frequently much faster than factorization or discrete logarithm-based systems such as ElGamal, RSA, and ECC. Roughly speaking, in order to achieve k bits of security, encryption and decryption for ElGamal, RSA, and ECC require O(k3) operations, while encryption and decryption for lattice-based systems require only O(k2) operations. Further, the simple linear algebra operations used by lattice-based systems are very easy to implement in hardware and software.

Definition 1. Let $v_1, v_2, \ldots, v_n$ $v_1, v_2, \ldots, v_n \in R$ be a set of linearly independent vectors. The lattice L generated by $v_1, \ldots, v_n$ is the set of linear combinations of $v_1, \ldots, v_n$ with coefficients in Z, $L = \{ a_1 v_1 + a_2 v_2 + \cdots + a_n v_n : a_1, a_2, a_3, \ldots, a_n \in Z\}$. A basis for L is any set of independent vectors that generates L. Any two such sets have the same number of elements. The dimension of L is the number of vectors in a basis for L.

Proposition1: Any two bases for a lattice L are related by a matrix having integer coefficients and determinant equal to ±1. For computational purposes, it is often convenient to work with lattices whose vectors have integer coordinates. For example, $Z_n = (x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in Z$ is the lattice consisting of all vectors with integer coordinates.

Definition 2. An *integral* (or *integer*) *lattice* is a lattice all of whose vectors have integer coordinates. Equivalently, an integral lattice is an additive subgroup of Zm for some $m \geq 1$.

GGH Crypto system:. Let us consider the standard parties in cryptography Alice and Bob. Alice's private key is a good basis B*good* (Typically, a good basis is a basis consisting of short, almost orthogonal vectors.) for a lattice *L* and her public key is a bad basis B*bad* for *L*. Bob's message is a binary vector **m**, which he uses to form a linear combination $\sum m_i v_{i\ bad}$ of the vectors in B*bad*. He then perturbs the sum by adding a small random vector **r**. The resulting vector **w** differs from a lattice vector **v** by the vector **r**. Since Alice knows a good basis for *L*, she can use Babai's algorithm[8A] to find **v**, and then she expresses **v** in terms of the bad basis to recover **m**. Eve, on the other hand, knows only the bad basis B*bad*., so she is unable to solve Closest Vector Problem in *L*. The correctness of the GGH cryptosystem rests on the fact that the error vector r is short enough so that the lattice point v can be recovered from the cipher text **v + r** using the private basis B, e.g., by using Babai's rounding procedure [8A],. On the other hand, the security relies on the assumption that without knowledge of a special basis, solving these instances of the closest vector problem in L(B) = L(H) is computationally hard. We remark that no asymptotically good attack to GGH is known: known attacks break the cryptosystem in practice for moderately small values of the security parameter, and can be avoided by making the security parameter even bigger.

VI CONCLUSION

Cloud computing will lead to a paradigm shift in computing, which will shake the foundation of computing. For cloud computing to be successful the issue of users control must be resolved technically, politically and socially. Users must be given assurances that their data and information is well protected, its integrity is maintained and is available when required. The security of the cloud can be assured even after the advent of quantum computers with our proposed crypto system.

The system we proposed in this paper efforts protection of the classified data in motion and at rest. The system is going to serve the basis for cloud computing.

References

[1] Open Virtualization Format Specifications. 2009. p. 1-41.

[2] Alliance, C.S. Trusted Cloud. 2010 [cited 2010 December 18]; Available from: http://www.trusted-cloud.com/.

[3] Amazon. Amazon Elastic Compute Cloud (Amazon EC2). 2010 [cited 2010 December 18]; Available from:

http://aws.amazon.com/ec2/.

[4] Appnexus. AppNexus: Home. 2010 [cited 2010 December 18];Available from: http://www.appnexus.com/.

[5] Cécile Germain-Renaud and O.F. Rana, "The Convergence of Clouds, Grids, and Autonomics," IEEE Internet Computing, 2009. 13(6): p. 9.

[6] Cerf, V.G., "Future Imperfect," IEEE Internet Computing, 2010. January/February: p. 30-34.

[7] Communications, X. XCalibre Communications. 2010 [cited 2010 December 18]; Available from: http://xcalibre.co.uk/new-page.htm.

[8] Conti, G., Googling Security How much does Google know about you? 2009: Addison-Wesley.

[8A]. Babai, L.: On Lovász lattice reduction and the nearest lattice point problem.Combinatorica, 6:1–13 (1986).

[9] Erdogmus, H., "Cloud Computing: Does Nirvana Hide behind the Nebula?" IEEE Software, 2009. 26(2): p. 4-6.

[10] EyeOS. eyeOS - Web Desktop, Cloud Computing Operating System and Web Office. 2010 [cited 2010 December 18]; Available from:http://www.eyeos.org/.

[11] Geer, D., "The OS Faces a Brave New World," IEEE Computer, 2009. 42(10): p. 15-17.

[12] Gilder, G. The Information Factories. 2006 [cited 2010 December 18]; Available from:http://www.wired.com/wired/archive/14.10/cloudware.html.

[13] GoGrid. Cloud Hosting, Cloud Servers, Hybrid Hosting, Cloud Infrastructure from GoGrid. 2010 [cited 2010 December 18]; Available from: http://www.gogrid.com/.

[14] Google. Google Mail. 2010 [cited 2010 December 18]; Available from: mail.google.com/mail/.

[15] Gridlayer. Enterprise Hosting, Cloud Computing, Dedicated Hosting.2010 [cited 2010 December 18]; Available from: http://thegridlayer.com/.

[16] Leavitt, N., "Is Cloud Computing Really Ready for Prime Time?" IEEE Computer, 2009. 42(1): p. 15-20.

[17] Leavitt, N., Is "Cloud Computing Really Ready for Prime Time?" IEEE Computer, 2009: p. 15-17.

[17A]. Gentry, C. and Szydlo,M.: Cryptanalysis of the revised NTRU signature scheme.In Proc. of Eurocrypt '02, volume 2332 of LNCS. Springer-Verlag (2002).

[18] Microsoft. Windows Azure Platform. 2010 [cited 2010 December 18];Available from: http://www.microsoft.com/windowsazure/.

[18A]. Gentry, C., Peikert, C., and Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In Proc. 40th ACM Symp. on Theory of Computing (STOC), pages 197–206 (2008).

[19] Mosso. Mosso CrunchBase. 2010 [cited 2010 December 18]; Available from: http://www.crunchbase.com/company/mosso.

[19A]. Goldreich, O., Goldwasser, S., and Halevi, S.: Public-key cryptosystems from lattice reduction problems. In Advances in cryptology, volume 1294 of Lecture Notes in Comput. Sci., pages 112–131. Springer (1997).

[20] Naone, E. Google Gives a First Look at the Chrome OS. TechnologyReview 2009 [cited 2010 December 18]; Available from:http://www.technologyreview.com/web/23987/.

[21] Oasis. Organization for the Advancement of Structured Information Standards. 2010 [cited 2010 December 2010]; Available from: http://www.oasis-open.org/who/.

[22] OpenCloudManifesto. Open Cloud Supporters. 2010 [cited 2010 December 2010]; Available from: http://www.opencloudmanifesto.org/supporters.htm.

[23] OpenGridForum. Open Cloud Computing Interface Working Group. 2010 [cited 2010 December 18]; Available from: http://www.ggf.org/gf/group_info/view.php?group=occi-wg.

[24] Peter Mell and T. Grance, "The NIST Defition of Cloud Computing," 2009, National Institute of Technology and Standards. p. 1-2. [25] Salesforce. CRM - salesforce.com Europe. 2010 [cited 2010

December 18]; Available from: www.salesforce.com.

[26] Thomas Ristenpart, et al. Hey, "You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds," in ACM Conference on Computer and Communications Security (CCS). 2009:ACM.

[27] Tomhave, B., "Dysfunction Junction: Do Standards Function?," ISSA Journal, 2010. February: p. 12-16, 42.

[28] Winkler, I. The Real Problems With Cloud Computing. 2009 [cited 2010 December 18];Available from: http://www.csoonline.com/article/500344/winkler-the-real-problemswith- cloud-computing.

[29] Fredrick Mtenzi, Kevin Street, Dublin 8, Dublin, IrelandIs Cloud Computing Ready for Critical Applications?

[30]. Lenstra, A.K. and Lenstra, Jr., H.W., editors: The development of the number field sieve, volume 1554 of Lecture Notes in Mathematics. Springer- Verlag, Berlin (1993). ISBN 3-540-57013-6.

[31]. McEliece, R.: A public-key cryptosystem based on algebraic number theory. Technical report, Jet Propulsion Laboratory (1978). DSN Progress Report 42-44.

[32]ICIT 2011 The 5th International Conference on Information Technology Is Cloud Computing Ready for Critical Applications?

Fredrick Mtenzi School of Computing, Dublin Institute of Technology, Kevin Street, Dublin 8, Dublin, Ireland Fredrick.Mtenzi@dit.ie

AUTHORS PROFILE

PSV Vachaspati is life member of IETE (India), ISTE .He is teaching Computer science to students for 10 years at Graduate level and post Graduate level at Bapatla Engg. College. and produced several research publications.

Dr. P. S. Avadhani is a professor in the department of Computer Science and Systems Engineering of Andhra University. His research areas are Algorithms, Nework Security

and Data Privacy.He is an Expert Cryptalagist. He has guided several Ph. D .scholars. He has guided more than 93 M.Tech. Projects. He received many honors and he has been the member or many expert committees, member of Board of Studies for various universities, Resource person etc. for various organizations. He has co-authored 4 books. He is a Life Member in CSI, AMTI, ISIAM, ISTE, YHAI and in the International Society on Education Technology. He is also a Member of IEEE, and a Member in AICTE.