IEI Centenary Publication

M S Ramanujan Memorial Lecture

A Compilation of Memorial Lectures
presented in

National Conventions of Computer Engineers

35th Indian Engineering Congress

December 18-20, 2020

The Institution of Engineers (India)

8 Gokhale Road Kolkata 700020

Background of
M S Ramanujan Memorial Lecture

Born in 1887, Srinivasa Ramanujam was brought up in an orthodox traditional south Indian environment. He was an enigma to his teachers even at school because of his prodigious memory and unusual mathematical talent, which began to show, even before he was ten. That was the age when he topped the whole district at the primary examination and this procured him a half-fee concession at Town High School, Kumbakonam. He passed the Matriculation examination of the University of Madras in December 1903, secured a first class, and earned for himself the Subramaniam Scholarship in the FA (First Examination in Arts) class at Government College, Kumbakonam.

His research marched on undeterred by environmental factors-physical, personal, economic or social; magic squares, continued fractions, hypergeometric series, properties of numbers-prime as well as composite, partition of numbers, elliptic integrals and several other such regions of mathematics engaged his thought. He recorded his results in his notebooks. Exact facsimiles of these notebooks have now, since 1957, been published in two volumes by the cooperative efforts of the University of Madras, the Tata Institute of Fundamental Research and Sir Dorabji Tata Trust.

Though Ramanujam accepted a clerk's appointment in the office of the Madras Port Trust, his mathematical work did not slacken. His first contribution to the Journal of the Indian Mathematical Society appeared in 1911. Ramanujam was brought to the University of Madras as a Research Scholar on May 1, 1913 at the age of 26.

Ramanujam thus became a professional mathematician and remained as such for the rest of his short life. He began a correspondence with Prof G H Hardy, the then Fellow of Trinity College, Cambridge and his first historic letter to Prof Hardy in January 1913 contained an attachment of 120 theism all originally discovered by him. Thereafter, he was invited to England in March 1914.

Ramanujam spent four very fruitful years at Cambridge, fruitful certainly to him, but more so to the world of mathematics, published twenty-seven papers, seven of them jointly with Prof Hardy. In 1918, he was elected Fellow of the Royal Society and in the same year was elected Fellow of Trinity College, both honours coming as the first to any Indian. The University of Madras rose to the occasion and made a permanent provision for Ramanujam by granting him an unconditional allowance of £ 250 a year for five years from April 01, 1919.

Unfortunately, Ramanujam had to spend the fifth year of his stay in England in nursing homes and sanatoria. He returned to India in April 1919 and continued to suffer from his incurable illness. All the time his mind was totally absorbed in mathematics. Thus, arose the so called Lost Notebook of Ramanujam, which contains 100 pages of writing and has in it a treasure house of about 600 fascinating results. Ramanujam's discoveries and flights of intuition were contained in the four notebooks and also his thirty-two published papers as well as in the three Quarterly Reports, which he had submitted to the University of Madras in 1913-14. These had thrilled mathematicians the world over. More than two hundred research papers had been published as a result of his discoveries. Later Ramanujam died at the unexpected age of 32.

In memory of his dedicated service, The Institution of Engineers (India) instituted an Annual Memorial Lecture in his name during the National Convention of Computer Engineers.

M S Ramanujan Memorial Lecture

presented during **National Conventions of Computer**

New Horizons in Computing Encompassing, Mobile Computing, Grid Computing and Automatic Computing

Dr D S Rane

Former Head, Computer & Information Group, VSSC, Trivandrum

Today we are paying a tribute to the great mathematician of India M. S. Ramanujan, the genius who explained the concept of infinity to the world. In the first part of my presentation We will very briefly take a look at the life and work of this genius.

I. Ramanujan and other great mathematicians of India

1. Srinivas Ramanujan was born on December 22, 1887. When he was merely thirteen years of age, he mastered a book on Trigonometry written by Loney. He was so taken by the subject that he launched his own research work. He put forward theorems and formulae that had been discovered earlier by great mathematicians but were not covered in the book and not known to him.

Two years later a friend introduced the book 'Synopsis of Elementary Results in Pure and Applied Mathematics' by George Shoobridge Carr to Ramanujan. A young boy at the age of fifteen may have recoiled from the book, but Ramanujan began solving problems given in the book. With the floodgates now open, ideas began to pour forth. Such was the gush of ideas that Ramanujan found it difficult to write them all down. He scribbled his results in loose sheets and notebooks. In fact, before he went abroad for pursuing his studies at the Cambridge University, he had filled three notebooks with his jottings, which later came to be known as Ramanujan's Frayed Notebooks.

Ramanujan had secured a first class in his matriculation examination and had also been awarded a scholarship but he failed in his first year college examinations, because, being obsessed with mathematics, he had neglected all other subjects. At this stage his father got him married. He thus needed to find money to support self, wife and buy paper for his jottings. Ramanujan approached several offices and applied for a clerical job, displaying his now famous frayed notebooks and papers and claiming that he was good in mathematics. However, nobody could follow his work and he was turned away. Luckily for him, he came across one Francis Spring, who did seem to understand what was in the notebooks and appointed him at the Madras Port Trust, Soon after, some educationists took up the cause of Ramanujan and in May 1913, the University of Madras awarded him a fellowship although he had no formal degree.

In the meantime, Ramanujan had approached the great mathematician G. H. Hardy and presented to him a set of one hundred and twenty theorems and formulae. A part of it was the Reimann series. Ignorant of Reimann's original work, Ramanujan had reproduced the work all over again. Another intriguing portion of the collection sent to Hardy was Ramanujan's interpretation about the equations called "modular". It was later proved that Ramanujan's conjectures were indeed correct. The collection also included a formula in hypergeometric series, which later came to be named after him. Hardy and his colleague, J. E. Littlewood, recognized the genius in Ramanujas and made arrangements for him to travel to Cambridge University to study. Hardy was amused to find that Ramanujan was an unsystematic mathematician, who played with mathematics much as a child played with toys. His mathematical truths were not explained and it was left to other mathematicians to prove them.

Ramanujan was elected Fellow of the Royal Society in February 1918. He was the second Indian to be honoured with this fellowship and the first Indian to be elected Fellow of the Trinity College, Cambridge. His contributions to the field of mathematics included the Hardy-Ramanujan —Littlewood circle method in number theory, Roger-Ramanujan's identities in partition of integer s, list of highest composite numbers and some work on the algebra of inequalities and the number theory. Unfortunately, Ramanujan fell victim to tuberculosis and had to be sent home to India. Fighting pain and death, Ramanujan kept himself pre-occupied by playing with numbers. He succumbed to the illness at the tender age of thirty-two on April 26,1920. Within the short life span, Ramanujan had earned repute as an astrologer and an orator too.

Ramanujan left behind a set of scribbled papers wherein he stated 50 analytical series and equations without any proof. By now many of them have been proved, but a few more are still under the investigation of mathematicians. Dr George Andrews of Pennsylvania State University and his research students are still pursuing the proof of these series and Theorems.

2. Prior to Ramanujan, many Mathematicians of repute have made significant contributions. I would like to mention a few of them very briefly

Aryabhata (475 A.D. -550 A.D.) is the first well known Indian mathematician. In his astronomical treatise Aryabhatiya (499 A.D.), he made the fundamental advance in finding the lengths of chords of circles, by using the half chord rather than the full chord method used by the Greeks. He gave the value of π (Pi) as 3.1416, claiming, for the first time, that it was an approximation. He also gave methods for extracting square roots, summing arithmetic series, solving indeterminate equations of the type ax -by = c. He also wrote a textbook for astronomical calculations, *Aryabhatasiddhanta*. In recognition to his contributions to astronomy and mathematics, India's first satellite was named Aryabhata.

Brahmagupta (598 A.D. -665 A.D.) is renowned for introduction of negative numbers anc operations on zero into arithmetic. His main work was *Brahmasphutasiddhanta*. This work was later translated into Arabic as *Sind Hind*. He formulated the rule of three and proposed rules for the solution of quadratic and simultaneous equations. He gave the formula for the area of the cyclic quadrilateral as SQROOT[s(s-a)(s-b)(s-c)(s-d)] where s is the semi perimeter. He was the first mathematician to treat algebra and arithmetic as two different branches of mathematics. He gave the solution of the indeterminate equation $Nx^2+1 = y^2$. He is also the founder of the branch of higher mathematics known as "Numerical Analysis".

Bhaskara (1114 A.D. -1185 A.D.) or Bhaskaracharaya II is the most well known ancient India mathematician. He was the first to declare that any number divided by zero is infinity and that the sum of any number and infinity is also infinity. He is famous for his book *Siddhanta Siromani* (1150 A.D.). It is divided into four sections -Leelavati (a book on arithmetic *Bijaganita* (algebra), *Goladhayaya* (chapter on sphere-celestial globe), and *Grahagani* (mathematics of the planets). Leelavati contains many interesting problems and was a very popular textbook. The second Indian satellite was named as Bhaskara.

3. Well known Indian mathematicians of the 20th century are:

Srinivasa Aaiyangar Ramanujan

P.C. Mahalanobis : He founded the Indian Statistical Research Institute in Calcutta. In 1958, he started the National Sample Surveys which gained international fame.

C.R. Rao: A well known statistician, famous for his “theory of estimation"(1945). His formulae and theory include "Cramer -Rao inequality", "Fischer -Rao theorem" and "Rao — Blackwell Therom".

Narendra Karmarkar : India born and IITB product Narendra Karmarkar, while working at Bell Labs USA, stunned the world in 1984 with his new algorithm to solve linear programming problems. This made the complex calculations much faster, and had immediate applications in optimization of airports, warehouses, communication networks etc.

II. Computing developments in brief.

The first electronic computer was ENIAC, developed at the University of Pennsylvania by Eckert and Mauchly in the early 1940s with Brainard as the Project Director. The top secret ENIAC was disclosed in 1945 after the end of II world war. This was to have been followed by EDVAC based on the stored program concept of John Von Neumann. But it was not taken up for various reasons. However, it was built as ‘The Institute’ at Princeton University. The technology of course was based on Vacuum Tubes. ’The Institute’ was also copied at University of Illinois (Illiac) and several other Universities. With the commercial production of the transistor in 1954, newer hardware designs came up. With the rapid developments in the solid state electronics field (IC, MSI, LSI, VLSI on one hand and magnetic core, solid State memories, optical memories on the other), the computer also became compact, smarter, faster and versatile. Here the miniaturization of electronics hardware played a major role.

The Microprocessor gave a big push to the further size reduction and higher capability/capacity. The microprocessor itself came about in a strange way. A calculator manufacturer (Busicom) from Japan desired to have their calculator on a single chip. After a few design iterations (from late 1969 to February 1971) the microprocessor 4004 was ready at Intel. Soon after other developers also came out with their versions.

The hunger and need for higher and higher computing power kept on growing. In this connection, I would like to refer to 2 projects; namely ILLIAC IV and the so called 'Fifth Generation' project of the Japanese consortium. ILLIAC IV was designed as the first super computer at the University of Illinois. It had many delays but finally when it came out, it was used as an attached Scientific Processor (BSP for example). Fifth Generation Computer project was a very ambitious project. It envisaged an extremely powerful engine (CPU) at the core along with several attached processers to carry out Artificial Intelligence (AI) tasks based on a Knowledge Processing Systen. The project itself could not be completed in its entity, but the components of the Knowledge Processing System have been developed and are in use today.

III Current Scenario (New Horizons)

1. Microprocessors:

Pentium IV of Intel currently operates at clock speeds of above 3 GH. The speed keeps going up every few months, thanks to the Moore's Law. Other processors are HP Itarium 2, MIP Technology's R8000 and Apple & IBM's G5 Processor. Another microprocessor is under development by IBM, Sony and Toshiba.

IBM, Sony and Toshiba have announced details of a microprocessor they say has the muscle of a supercomputer and can power everything from video game consoles to business Devices built with the computers, processor, code-named "Cell," will compete directly with the PC chips that have powered most of the world's personal computers for a quarter-century. Cell's designers say their chip, built with the growing world of rich media and broadband networks in mind, can deliver 10 times the performance of current PC processors. It will not carry the same technical baggage that has made most of today's computers compatible with older PCs. That architectural divergence will challenge the dominant paradigm of computing that Microsoft Corp. and Intel Corp. have fostered. The new chip is expected to be used in Sony Corp.'s next-generation PlayStation game console. Toshiba Corp. plans to incorporate it into high-end televisions. And IBM Corp. has said it will sell a workstation with the chip starting later this year.

2. Supercomputer:

Supercomputers are getting faster, at an even faster rate. IBM's Blue Gene, to be delivered this spring to the U.S. Department of Energy's Lawrence Livermore National Laboratory in Livermore, Calif, takes the top spot, with a performance of 70.72 teraflops (trillion floating - point operations per second). Silicon Graphics' Columbia, built for NASA and named after the space shuttle lost in 2003, comes in second, at 51.87 teraflops. The two machines displaced Japan's famed Earth Simulator to third place after that 35.86-teraflop computer had reigned supreme for two and a half years.

Comparison:

Maker/ Name	Processors	Memory	Disk Storage	Speed	Cost
IBM Blue Gene	32 768	8 T Bytes	28 T Bytes	70.72T flops	100M$
SGI Columbia	10 240	20 T Bytes	440 T Bytes	51.87T flops	50 M$
NEC Earth Simulator	5 120	10 T Bytes	700 T Bytes	30.86T flops	350-500

3. Technology Developments

Mobile Computing:

Since mobile computers can change location while connected to the network, the network address will change. The mobile user also needs to receive information relevant to the current position and time. Therefore there are a few issues to be dealt with when it comes to mobility and scalability. Mobility has introduced new problems in data management for wireless computing. We can define two types of data management: global and local data management. Global data management deals with locating the mobile user, addressing, broadcasting and replicating. Local data management deals with energy efficient data access, management of disconnection and query processing.

GRID Computing:

Grid computing is the next wave of the Internet. Think of it like a time machine. Grid computing enables you to effectively compress time by expanding computing space. Today, the first stage of grid computing — the cluster grid — enables organizations to better utilize available compute resources. As grids evolve from cluster to enterprise to global grids — from single departments to multiple departments to outside the firewall — grid computing will provide seamless, transparent, secure access to IT resources such as hardware, software, scientific instruments, and

services. Like electrical power, this access will be dependable, consistent, and pervasive. While the primary adopters of grid technology today are in compute intensive research of various kinds, the benefits of grid computing have broad appeal.

Autonomic Computing:

Autonomic Computing (also called Autonomy Oriented Computing or AOC) is a complementary paradigm for solving hard computational problems and for characterizing the behaviors of a complex system. The first goal of AC is to reproduce life-like behavior in computation. With detailed knowledge of the underlying mechanism, simplified life-like behavior can be used as model for a general-purpose problem solving technique. Replication of behavior is not the end, but rather the means, of these computational algorithms. The second goal is to understand the underlying mechanism of a real-world complex system by hypothesizing and repeated experimentation. The end product of these simulations is a better understanding of or explanations to the real working mechanism of the modeled system. The third goal concerns the emergence of a problem solver in the absence of human intervention. In other words, self-adaptive algorithms are desired.

References:

1. IEEE Spectrum, Vol. 42, no. 2 (INT), February, 2005, p.3 “IBM Reclaims —.”

2. IEEE Spectrum Online, February 8, 2005.

3. Federico Faggin, “The Birth of the Microprocessor”, Byte, March 1992.

4. Ancient India’s Contribution to Mathematics, website www.India,CoolAtlantic.com.

5. Matthew Fordahl, “IBM, Sony, Toshiba unveil microprocessrs” www.cnews.canoe.ca.

6. Autonomic Computing, IBM Research, www.research.ibm.com.

7. What is Grid Computing? website, www.cio.com.

8. IEEE Transactions on Mobile Computing, 2004, Vol. 3, nos. 1 to 4.

Introduction to Soft Computing

Prof (Dr) Prashanta Kumar Patra

HOD, CSE Dept, CET, Bhubaneswar

What is Soft Computing?

• Soft computing differs from conventional (hard) computing in that, unlike hard computing, it is tolerant of imprecision, uncertainty, partial truth, and approximation. In effect, the role model for soft computing is the human mind.

• The principal constituents, i.e., tools, techniques, of Soft Computing (SC) are Fuzzy Logic (FL), Neural Networks (NN), Support Vector Machines (SVM), Evolutionary Computation (EC), Machine Learning (ML) and Probabilistic Reasoning (PR).

Premises of Soft Computing

• The real world problems are pervasively imprecise and uncertain

• Precision and certainty carry a cost

Guiding Principles of Soft Computing

• The guiding principle of soft computing is exploit the tolerance for imprecision, uncertainty, partial truth, and approximation to achieve tractability, robustness and low solution cost.

What is Hard Computing?

• Hard computing, i.e., conventional computing, requires a precisely stated analytical model and often a lot of computation time.

• Many analytical models are valid for ideal cases.

• Real world problems exist in a non-ideal environment

Premises of Hard Computing

• Premises and guiding principles of Hard Computing are Precision, Certainty, and rigor.

• Many contemporary problems do not lend themselves to precise solutions such as Recognition problems (handwriting, speech, objects, images), Mobile robot coordination, forecasting, combinatorial problems etc.

Implications of Soft Computing

• Soft computing employs NN, SVM, FL etc, in a complementary rather than a competitive way.

• One example of a particularly effective combination is what has come to be known as "neuro-fuzzy systems."

• Such systems are becoming increasingly visible as consumer products ranging from air-conditioners and washing machines to photocopiers, camcorders and many industrial applications.

Unique Property of Soft computing

• Learning from experimental data

• Soft computing techniques derive their power of generalization from approximating or interpolating to produce outputs from previously unseen inputs by using outputs from previous learned inputs.

• Generalization is usually done in a high dimensional space.

Current Applications using Soft Computing

• Application of soft computing to handwriting recognition

• Application of soft computing to automotive systems and manufacturing

• Application of soft computing to image processing and data compression

• Application of soft computing to architecture

• Application of soft computing to decision-support systems

• Application of soft computing to power systems

• Neurofuzzy systems

• Fuzzy logic control

Future of Soft Computing

• Soft computing is likely to play an especially important role in science and engineering, but eventually its influence may extend much farther.

• Soft computing represents a significant paradigm shift in the aims of computing a shift which reflects the fact that the human mind, unlike present day computers, possesses a remarkable ability to store and process information which is pervasively imprecise, uncertain and lacking in categoricity.

Overview of Techniques in Soft Computing

• Neural networks

• Support Vector Machines

• Fuzzy Logic

• Genetic Algorithms in Evolutionary Computation

Neural Networks

• A neural network is a system composed of many simple processing elements operating in parallel whose function is determined by network structure, connection strengths, and the processing performed at computing elements or nodes.

• A neural network is a massively parallel distributed processor that has a natural propensity for storing experiential knowledge and making it available for use. It resembles the brain in two respects: Knowledge is acquired by the network through a learning process. Inter neuron connection strengths known as synaptic weights are used to store the knowledge

• A neuralnetwork is a circuit composed of a very large number of simple processing elements that are neurally based. Each element operates only on local information. Furthermore each element operates asynchronously; thus there is no overall system clock

Where are Neural Networks applicable?

• in signature analysis as a mechanism for comparing signatures made (e.g. in a bank) with those stored. This is one of the first large-scale applications of neural networks in the USA, and is also one of the first to use a neural network chip.

• in process control: there are clearly applications to be made here: most processes cannot be determined as computable algorithms.

• in monitoring: networks have been used to monitor

• the state of aircraft engines. By monitoring vibration levels and sound, early warning of engine problems can be given.

• British Rail have also been testing a similar application monitoring diesel engines.

• Pen PC's where one can write on a tablet, and the writing will be recognized and translated into (ASCII) text.

• Speech and Vision recognition systems Not new, but Neural Networks are becoming increasingly part of such systems. They are used as a system component, in conjunction with traditional computers.

• Support Vector Machines and Neural Networks

• The learning machine that uses data to find the APPROXIMATINGFUNCTION (in regression problems) or the SEPARATION BOUNDARY (in classification, pattern recognition problems), is the same in high dimensional situations. It is either the so-called SVM or the NN.

Some SVM Features

SVMs combine three important ideas:

• Applying optimization algorithms from Operations Research (Linear Programming and Quadratic Programming)

• Implicit feature transformation using kernels

• Control of overriding by maximizing the margin

FUZZY LOGIC (FL)

FL is a problem-solving control system methodology that lends itself to implementation in systems ranging from simple, small, embedded micro-controllers to large, networked, multi-channel PC or workstation based data acquisition and control systems. It can be implemented in hardware, software, or a combination of both. FL provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, imprecise, noisy, or missing input information. FL's approach to control problems mimics how a person would make decisions, only much faster.

WHY USE FL?

FL offers several unique features that make it a particularly good choice for many control problems.

1) It is inherently robust since it does not require precise, noise-free inputs and can be programmed to fail safely if a feedback sensor quits or is destroyed. The output control is a smooth control function despite a wide range of input variations.

2) Since the FL controller processes user-defined rules governing the target control system, it can be modified and tweaked easily to improve or drastically alter system performance. New sensors can easily be incorporated into the system simply by generating appropriate governing rules.

3) FL is not limited to a few feedback inputs and one or two control outputs, nor is it necessary to measure or compute rate-of-change parameters in order for it to be implemented. Any sensor data that provides some indication of a system's actions and reactions is sufficient. This allows the sensors to be inexpensive and imprecise thus keeping the overall system cost and complexity low.

4) Because of the rule-based operation, any reasonable number of inputs can be processed (1-8 or more) and numerous outputs (1-4 or more) generated, although defining the rulebase quickly becomes complex if too many inputs and outputs are chosen for a single implementation since rules defining their interrelations must also be defined. It would be better to break the control system into smaller chunks and use several smaller FL controllers distributed on the system, each with more limited responsibilities.

5) FL can control nonlinear systems that would be difficult or impossible to model mathematically. This opens doors for control systems that would normally be deemed unfeasible for automation.

HOW IS FL USED?

1) Define the control objectives and criteria: What am I trying to control? What do I have to do to control the system? What kind of response do I need? What are the possible (probable) system failure modes?

2) Determine the input and output relationships and thoose a minimum number of variables for input to the FL engine (typically error and rate-of-change-of-error).

3) Using the rule-based structure of FL, break the control problem down into a series of IF XAND YTHEN Z rules that define the desired system output response for given system input conditions. The number and complexity of rules depends on the number of input parameters that are to be processed and the number fuzzy variables associated with each parameter. If possible, use at least one variable and its time derivative. Although it is possible to use a single, instantaneous error parameter without knowing its rate of change, this cripples the system's ability to minimize overshoot for a step inputs.

4) Create FL membership functions that define the meaning (values) of Input/Output terms used in the rules.

5) Create the necessary pre- and post-processing FL routines if implementing in S/W, otherwise program the rules into the FL HA/V engine.

6) Test the system, evaluate the results, tune the rules and membership functions, and retest until satisfactory results are obtained.

FL does not require precise inputs, is inherently robust, and can process any reasonable number of inputs but system complexity increases rapidly with more inputs and outputs. Distributed processors would probably be easier to implement. Simple, plain-language IF X AND Y THEN Z rules are used to describe the desired system response in terms of linguistic variables rather than mathematical formulas. The number of these is dependent on the number of inputs, outputs, and the designer's control response goals.

Genetic Algorithms

Genetic Algorithms were invented to mimic some of the processes observed in natural evolution. Many people, biologists included, are astonished that life at the level of complexity that we observe could have evolved in the relatively short time suggested by the fossil record. The idea with GA is to use this power of evolution to solve optimization problems. The father of the original Genetic Algorithm was John Holland who invented it in the early 1970's.

Genetic Algorithms (GAs) are adaptive heuristic search algorithm based on the evolutionary ideas of natural selection and genetics. As such they represent an intelligent exploitation of a random search used to solve optimization problems. Although randomized, GAs are by no means random, instead they exploit historical information to direct the search into the region of better performance within the search space. The basic techniques of the GAs are designed to simulate processes in natural systems necessary for evolution, specially those follow the principles first laid down by Charles Darwin of "survival of the fittest". Since in nature, competition among individuals for scanty resources results in the fittest individuals dominating over the

weaker ones.

Why Genetic Algorithms?

It is better than conventional Al in that it is more robust. Unlike older Al systems, they do not break easily even if the inputs changed slightly, or in the presence of reasonable noise. Also, in searching a large statespace, multi-modal state-space, or n-dimensional surface, a genetic algorithm may offer significant benefits over more typical search of optimization techniques, (linear programming, heuristic, depth-first, breathfirst, and praxis.) GAs simulate the survival of the fittest among individuals over consecutive generation for solving a problem. Each generation consists of a population of character strings that are analogous to the chromosome that we see in our DNA. Each individual represents a point in a search space and a possible solution. The individuals in the population are then made to go through a process of evolution. GAs are based on an analogy with the genetic structure and behaviour of chromosomes within a population of individuals using the following foundations:

• Individuals in a population compete for resources and mates.

• Those individuals most successful in each' competition' will produce more offspring than those individuals that perform poorly.

• Genes from 'good' individuals propagate throughout the population so that two good parents will sometimes produce offspring that are better than either parent.

• Thus each successive generation will become more suited to their environment.

Applications

• Artificial Creativity

• Automated design, including research on composite material design and multi-objective design of automotive components for crashworthiness, weight savings, and other characteristics.

• Automated design of mechatronic systems using bond graphs and genetic programming (NSF).

• Automated design of industrial equipment using catalogs of exemplar lever patterns.

• Calculation of Bound states and Local-density approximations.

• Chemical kinetics (gas and solid phases)

• Configuration applications, particularly physics applications of optimal molecule configurations for particular systems like C60 (buckyballs).

• Container loading optimization.

• Design of water distribution systems.

• Distributed computer network topologies.

• Electronic circuit design, known as Evolvable hardware &File allocation for a distributed system.

• JGAP: Java Genetic Algorithms Package, also includes support for Genetic Programming

• Parallelization of GAs/GPs including use of hierarchical decomposition of problem domains and design spaces nesting of irregular shapes using feature matching and GAs.

• Game Theory Equilibrium Resolution.

• Learning Robot behavior using Genetic Algorithms.

• Learning fuzzy rule base using genetic algorithms.

• Linguistic analysis, including Grammar Induction and other aspects of Natural Language Processing (NLP) such as word sense disambiguation.

• Mobile communications infrastructure optimization.

• Molecular Structure Optimization (Chemistry).

• Multiple population topologies and interchange methodologies.

• Optimization of data compression systems, for example using wavelets.

• Protein folding and protein/legend & Plant floor layout.

• Representing rational agents in economic models such as the cobweb model.

• Scheduling applications, including job-shop scheduling. The objective being to schedule jobs in a sequence dependent or non-sequence dependent setup environment in order to maximize the volume of production while minimizing penalties such as tardiness.

• Selection of optimal mathematical model to describe biological systems.

• Software engineering

• Solving the machine-component grouping problem required for cellular manufacturing systems.

• Tactical asset allocation and international equity strategies.

• Timetabling problems, such as designing a non-conflicting class timetable for a large university.

• Training artificial neural networks when pre-classified training examples are not readily obtainable (neuroevolution) & Traveling Salesman Problem.

Information Security - Current Status and Future Trends

Dr P Pal Chaudhuri

Professor Emeritus
Cellular Automata Research Lab (CARL),
Alumnus Software Ltd., Infinity Tower II, Saltlake, Kolkata

The Institution of Engineers is one of the well-respected professional bodies of India that projects national pride and heritage through seminars and conventions. This lecture in memory of M S Ramanujan organized today is one such occasion. Let me join all of you to pay my homage to this legendary mathematician of India who left indelible mark in a short span of his life covering only 32 years. He was born in 1887. He spent the most active period of his life in England around the –period of 1911 to 1916.

British mathematician G H Hardy, his mentor and collaborator, summarized some of his works in the book entitled" Ramanujan : Twelve Lectures on Subjects suggested by His Life and Work"; it was published in 1942. Sir Ramanujan occupies a unique place among the mathematicians who worked in the analytical number theory. His formulas, conjectures, identities and calculations still attract the attention of mathematicians even in this new millennium. He used to say that the goddess of Namakkal (his native place in Tanjore district) inspired him with the formulae in dreams. The number theory he worked on plays an important role to lay the mathematical foundation of modem techniques employed in Information Security.

Since the pre-historic days, human society has passed through the Agricultural and Industrial Age, and finally arrived at the Information Age. Generation of economic surplus and accumulation of wealth are the guiding factors to push the society from one to the next milestone. While the society of a developed nation moves ahead with higher speed in this journey, the speed for a developing nation is comparatively lesser. The human society of a developing nation, however, starts moving with higher velocity as it moves forward down the road.

In the current Information Age, the economic activity of the humansociety shifts its focus from the production of physical goods to manipulation and processing of Information. To remain competitive and maintain economic profitability, each stage of economic growth had to adopt techniques from the later stage. During the transition from Agricultural to Industrial Age, the agricultural products used to be viewed as commodity to be produced through mechanized farming .and production tools. Consequently, the economic value moved to manufacturing. During the transition to Information Age, production of both agriculture and industrial products will have to adopt to information rich practices. Information, in the current age, can be viewed as " Cyber Gold" for a government body, social organizations, commercial organizations and industrial establishments, and even for an individual member of the society.

The field of Information Technology (IT) has evolved to meet this demand of adopting information rich practices to ensure higher productivity at lesser cost. It achieves this goal through the use of computer based information systems to convert, process, transmit, retrieve, and Protect information that may be derived or stored in any corner of the so called global village. The demand from industry has fuelled the phenomenal growth of IT, which in turn has brought in remarkable changes in the manufacture/production of goods and services in this internet-worked world. Information, in the current Information Age, can be viewed as "Cyber Gold".

The technological advances of IT, notably PC and Internet, have changed the life styles around the globe. Such developments in turn have triggered the growth of new industries for controlling and providing Information. One of the most important activities of these upcoming technologies is - INFORMATION SECURITY, the theme of this convention. Irrespective of the hard or soft copy or the media used, the sole objective of Information Security is to ensure CCI (Confidentiality, Integrity, and Availability). This demands protection of Information Systems from unauthorized access and abuse through three D's - Disclosure, Disruption, Destruction of information.

It is often opined in recent times that the current human society has been transformed beyond recognition, specifically for the generation of pre-IT era. In this changed circumstances, the general viewpoint is - the age-old practices of protecting Information have to be abandoned while inventing new innovative schemes. True, the information storage methodology and its access have undergone radical changes in the context of the society that is

fast becoming paper-less. However, the basic framework of protecting our valued possession, the "Cyber Gold", remains the same.

The earlier practice of storing valuable documents under lock and key continues with multiple and combination locks and associated keys. The earlier storage media and its access methodology have been replaced with new one. So it is natural that the physical lock and key we are accustomed to got replaced with various encryption schemes along with different key management systems. The age old practice of storing the key set in a safe place avoiding unauthorized access got embedded within the "private key" and "key rounds" of a typical Encryption system.

In the event of transfer of information from one place to other and avoid unauthorized access, the practice of using permutation and substitution of characters in the text were in operation from the early days of human civilization. Subsequently, kings and warlords used this practice for communication with their friends while deceiving their enemies. These basic operations of Permutation and Substitution still form the core of modern encryption systems.

The mathematical formalism of the encryption schemes of earlier days first appeared around 1850's through the introduction of Permutation and Substitution Groups. No wonder, IBM introduced DES (Data Encryption System) scheme in 1970's based on this basic principle of Permutation and Substitution of plain text to generate the cipher text. Availability of higher computing power made DES vulnerable to attack, and consequently AES (Advanced Encryption Scheme) was introduced. The Substitution Box (S- Box) of AES can be found to contain a highly complex non-linear function. The non-linearity got further embedded in AES through multiple key rounds and row/column operations. The above scenario points to the fact that - with the passage of time, the age old ad-hoc practice of employing Permutation and Substitution got refined with mathematical formulation to arrive at the present day encryption schemes. Further, the public key encryption scheme of RSA (Rivest Shamir Aldlrman) is again based on mathematical foundation of Primality test to determine whether a number is a prime or not. Although not directly related to prime number detection, as early as 1916, Ramanujan did lay his hand to determine what is referred to as Prime Counting Function f(x) that specifies the number of primes less than or equal to x.

Notwithstanding all the mathematical formalism and innovative approaches, it would be impossible to design cost effective measures to stop unauthorized access with hundred percent certainties. In order to search for the available options to fight such a situation, let us review the practices prevailing in human society.

To enhance the security of our valuable possession we hire a bank locker that is supposed to provide better security. In a similar way to protect the information systems, the practice of building multiple levels of Firewalls are in use from 1990's and the scheme got matured over the last decade. This practice is going to stay with us for coming decades.

However, the major sources of security problem lie in the evolution of networked society with phenomenal growth of Internet linking the computer systems around the globe. Against the enormous benefits of the democratic set up Internet with minimal control, the society has to face the music due its abuse and misuse.

We all have to live with the threats of virus, mail bombs, on line scam, cyber crime, Denial of Service (DoS) etc. Many more new and innovative threats and new class of Virus are bound to appear in the coming decades. Internet and higher computing power available today are being used by on-line criminals as tools for fraud, cyber crime, and internet scam. Whatever may be the level of security, highly intelligent computer experts turned to criminals wil! always work out some loopholes to break the security cordon. Let us review the practices prevailing in another discipline for assistance. Let us learn from the discipline of medical science to understand the protection mechanism we need to adopt for such a situation. Vaccination, immunization, medication and enhancing in-built immunity of the human body are the standard solutions for different types of attacks against human system. Add to this the continuous fight of drug researchers to design new drugs to protect from known virus or potential hazards.

A variant of similar approach is a necessity to protect information systems. Each of the known and potential attacks against a network or a Information System should be analyzed to evolve adequate protection mechanism. Since mid 1990's a large number of start-up companies have concentrated on this area to provide the service - such as designing mechanisms for Firewalls, anti virus protection, spam detection etc. However, hiring the services of such security companies will not suffice unless proper protection is not practiced by an organization or even an individual to protect the environment. For example, a medical doctor prescribes "does" and "don'ts" to keep our body fit. Such prescribed norms from medical experts got to be followed to keep us fit and active. Similarly, security expert does prescribe specific steps to protect the system. For example, the precaution - not to open an email from an unknown source - is often prescribed. Because virus, malicious software etc. quite often get implanted through emails. Such prescribed protection mechanism got to be followed in practice to get the desired results.

In general, all the organizations, government bodies, and even an individual member of the internetworked society have to hire the services of security agencies to install the well tested protective measures. However, this will not suffice. In addition, it is essential to employ healthy security practices. For example, files with critical information should not be left unsecured at any time, or not to accept a program from uncertified source. The underlying reason being - an apparently harmless program once executed might release virus or even a worm. Such a list of recommended norms is quite long and can never be comprehensive. It will depend on the working environment, IT applications, nature of information transactions/exchange etc.

We shall have to reconcile to the fact that as the human civilization proceeds further in the Information Age, attacks are getting more organized and sophisticated. The list of published successful cyber crimes presents a serious point of concern. To mention a few, in 1990's the files from big organizations like Motorola and Sun were stolen, Russian hacker Vladimir Levin broke into Citibank's cash management system siphoning 10 million dollar. In last one decade a large number of cases of cyber theft of confidential data have been reported, a number of cases of hacking of apparently highly secured sites were noticed.

While big corporations and government bodies are trying their best to install and practice security measures, the on-line experts with distorted mentality are not sitting idle. They are evolving new methodology to break the security cordons. For example, hackers usually use password sniffers or IP snooping to obtain entry into network or view sensitive information. These techniques along with their further sophistication will be a source of major threat in the coming decades.

The above scenario has forced the software developer community to employ improved Security Engineering practices in building and applying software development methodology. In the recent past, user community was happy if a software code enhances productivity and efficiency in executing targeted functionality. In the current Information Age, a piece of software has to ensure its resilience to attack along with desired performance during normal operation and also during crisis. Secured software demands incorporation of measures like - robust access controls, authentication, denial of unauthorized data deletion and modification, data recoverability with back up and restoration, resilience against attacks like Denial of Service etc.

Considering all the above issues, it is essential to employ internal staffs to ensure security within the organization in addition to taking support from Information Security vendors and experts. This security group for each organization and government body will be entrusted with the responsibility of analyzing the total system including the associated networks while identifying weak links and how best to plug the associated loopholes. There will be still lot many security hazards that are not yet fully understood. So embedding security function is a continuous process for any organization because of new dimensions of external threats and also threats from within due to a disgruntled and rogue employees who have access to sensitive information.

The security group should be also trained as Computer Detectives and also on Computer Forensics - the art and science of systematic inspection of Information System environment to identify direct or supportive evidence of security breach. In the process, the group will be able to detect whether an attack has been made or attempted before too much damage is done for the organization. The inherent consideration being - since hundred percent security can never be ensured, an early detection system, equivalent to Bugler Alarm, can be installed on the weak segments of the Information System. Further, the Security Group should be- also trained for disaster management in the event of a successful attack to the system.

Like any other upcoming areas of interest, new technological innovations are being researched continuously for Information Security. For example, the concept of detection of the fact that the message being transmitted has been intercepted is incorporated in Quantum Cryptography. It employs the basic principle of quantum phenomenon th-at is being seriously investigated for various industrial applications.

The discussions so far have provided an overview of current status of Information Security. The following scenario emerges so far as near-future trends are concerned.

Even though the real life application of Quantum Cryptography is a long way to go, it has an inherent appeal so far as secured transmission of data is concerned. It will enable the sender to get the indication that there are some adversaries on the network who have observed the data stream. Hence as the society moves along the Information Age, one of major research focus is bound to be Quantum Cryptography.

Another issue that is being seriously looked into is - Secured Software. In order to avoid massive fall out of security failure, organizations will look for incorporation of security engineering practices m the life cycle of a software code since its planning stage.

One of the most significant developments of the last decade is the Wireless Technology. Very soon the acronym WWW will be expanded as Wirelessly Wired World - "wired" in the present context means "connected". Wireless technology has been making steady inroads in the workplace - both for small and big organizations and also for personal computing environment. Demand for Wireless Local Area Network (WLAN) has gone up dramatically because of its inherent advantages. It allows access to the network and also to Internet from anywhere in the workplace through a set of Access Points (APs). Easy flexible installation of network without any rewiring and plug-in provides the inherent advantages with long-term savings. However, security of wireless LAN poses a significant challenge.

Even though WLAN provides significant advantages, migration to this technology will be slow because of security concerns. The community of hackers is ready to break its security cordons. The security measures for a typical WLAN have not yet matured to the desired level. It is worth noting the fact that physical wires of conventional wired LAN poses one of the primary obstacles to attackers trying to hack their way onto a LAN.

The password-based authentication currently in use for wireless LAN does not provide desired protection. During authentication negotiation between a client and an AP (Access Point), it is not very difficult for a hacker to access user credentials through dictionary attack against password protocols. Further, during data transfer session, one has to compromise security with cost and delay in transmission. Finally, the concern of Rogue Access Point created by hackers. Such an' AP will confuse the user -in respect of the network she/he is connected to. All these security concerns are being addressed in order to proceed to the Wireless Age of the Internet-worked Society of the Information Age.

One of the major emphasis of the earlier discussions is the fact that - considerable benefits can be derived if we try to learn from History. Since Information is viewed as the "Cyber Gold", the age-old conventions of protecting this precious material are worth reviewing and adoption for new environment. Specific environment that exists in nature or those have evolved in the society through refinement in different generations, can provide us the core concepts to address many problems we face in modern society. For example, the basic principle of human Immunology can be studied in details and the relevant features can adopt for protection of Information Systems. The approach being proposed is - let us learn from nature, because Mother Nature provides us with the handbook from which we learn something or other everyday.

Design Intent Verification of Automotive Architectures and Applications

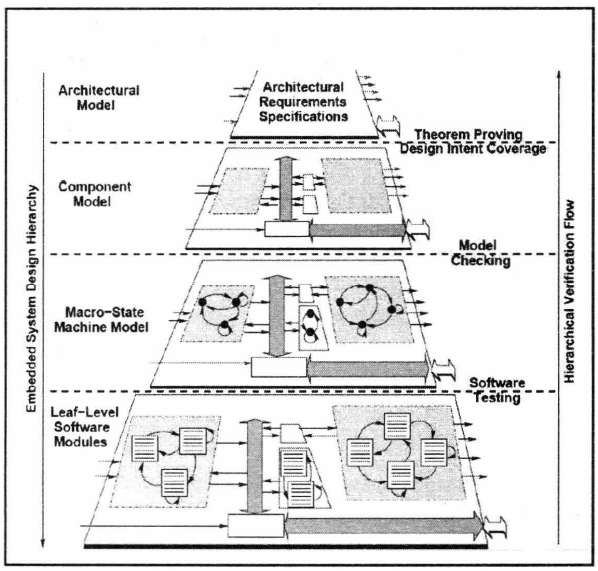
Prof Partha P Chakrabarti

Indian Institute of Technology Kharagpur

Abstract

Modern Automotive Architectures are complex computing systems having a large number of electronic control units (ECU) connected over a multilayered network. The ECD's maintain a synchronized control of a large number of complex automotive functions covering engine control, braking, steering, stability, lights, body and telematics. The software based controllers have unique computational requirements ranging from reactive, real-rime response at various granularities, non-determinism, contain both discrete and continuous variables and require a high degree of reliability and have some critical safety features that must be adhered to. Specification and Verification of Design Intent is key for 'correct by construction' design of embedded automotive controllers. Have I specified what I want to design? Is it correct and complete? Does it meet the functional and safety critical timing features? These are the questions that must be handled in the earliest design phase.

Intent Specification and Verification of such embedded systems requires a layered discipline and can be structured in four major layers as shown in the figure shown alongside. Both top-down and bottom-up design-verification paradigms require validation and verification schemes at each level and between levels. The emerging complexity of embedded automotive tasks requires developing a powerful, scalable, automated methodology that can perform deep analysis at the level of logical and abstract specifications. At the architecture level design intent verification problems include consistency (satifiability), realizability (implementability) and completeness (coverage). At the Block competent level, the problem of design intent coverage to determine how much of the architectural properties is met. Model checking is applied at the state level to determine the correctness of block properties and code level testing of software blocks at leaf level check correctness of the macro states. The intent verification requirement has transcended functional verification and is now addressing key design issues like timing, end-to-end latency, power and reliability. Through vigorous research in recent years, smart methodologies combining formal methods, artificial intelligence and optimization have evolved that are able to critically analyze specifications and early implementations for their functional, timing, fault tolerance, ete., leading to high quality implementations with significantly reduced development cycle time. A number of such methods developed through our research are now implemented in state-of-the-art automotive design processes of leading companies. Some of these will be highlighted in the presentation.



About Computer Engineering Division Board

The Institution of Engineers (India) has established Computer Engineering Division in the year 1984. This Division consists of quite a large number of corporate members from Government, Public, Private sectors, Academia and R&D Organizations.

Various types of technical activities organized by the Computer Engineering Division include All India Seminars, All India Workshops, Lectures, Panel Discussions etc., which are held at various State/Local Centres of the Institution. Apart from these, National Convention of Computer Engineers, an Apex activity of this Division is also organized each year on a particular theme approved by the Council of the Institution. In the National Convention, several technical sessions are arranged on the basis of different sub-themes along with a Memorial Lecture in the memory of '**M S Ramanujam**', the eminent Mathematician of the country, which is delivered by the experts in this field.

In order to promote the research and developmental work in the field of Computer Engineering, the Institution also publishes Journal of The Institution of Engineers (India): Series B in collaboration with M/S Springer which is an internationally peer reviewed journal. The journal is published six times in a year and serves the national and international engineering community through dissemination of scientific knowledge on practical engineering and design methodologies pertaining to Electrical, Electronics & Telecommunication and Computer Engineering. Publishing Annual Technical Volume of Computer Engineering Division Board with ISBN is another initiative taken by IEI to encourage the students, researchers and professionals attached to this engineering discipline, who can contribute papers on contemporary topics in the related fields.

Due to multi-level activities related to this engineering discipline, this division covers different sub-areas such as:

- Social Networking through IT
- Cyber Security/ Privacy
- Cloud Computing
- Network on Chip
- Software Quality Advance and testing
- Participatory Governance through IT
- Big Data Analytics
- Soft Computing and Rough Computing
- Machine Learning
- e-Learning on web and mobile platform
- Nano-computing
- Mobile IPv6 network
- Information forensics and security
- Surveillance System and Application: Hardware and Software architecture, Transportation (road, rail, air)
- e-Healthcare
- The challenges of wireless and mobile Technologies
- e-Governance and M-Governance
- Social and web multimedia
- Wireless multimedia communication
- Multimedia streaming and transport
- 5 G wireless communication systems: prospect and challenges
- Natural Language Processing
- Internet of Things (IoT)
- Enterprise Architecture

The Institution of Engineers (India)
8 Gokhale Road, Kolkata 700020
Phone : +91 (033) 2223-8311/14/15/16, 2223-8333/34
Fax : +91 (033) 2223-8345
e-mail : technical@ieindia.org; iei.technical@gmail.com
Website : http://www.ieindia.org