4
HIGH PERFORMANCE COMPUTING AND CYBER SECURITY

In contemporary research computation is the main pillar of scientific discovery, which provides an in-expensive way to achieve high science, complementing theory, experiment and observation. The capability and credibility of a scientific organization is often judged by the computational facility the researchers have access to. CSIR-4PI provides state-of-the-art High Performance Computing(HPC) facility to the computational scientists and researchers across CSIR to address Grand Challenge problems in their frontier areas of science and engineering. The facility at CSIR-4PI is a centralized HPC facility. It is one of the top supercomputers of the country and provides multiple architectures suitable for domain specific applications. All the CSIR laboratories, through the high speed National Knowledge Network, access this facility. In addition to providing access to HPC, the group is also involved in research on cyber security. Under the 12th five-year plan of CSIR works have been initiated to develop a "Cyber Security Research & Observation" abbreviated as "CySeRO" to carryout research in the field of Cryptography and Cyber Security.

Inside

4.1 Cyber security research and observation platform at CSIR-4PI

It is well known that cyber security research is highly experimental driven. In order to strengthen the ongoing and future research in this area, CSIR Fourth Paradigm Institute (CSIR-4PI) has established a Cyber Security Research and Observation (CySeRO) platform. CySeRO is a sophisticated test-bed for experimental research and data analysis. The test-bed is hosted in a self-contained data center spread across three racks and equipped with inbuilt cooling, UPS, Fire Detection and Suppression, water leakage detection, CCTV, etc. Figure 4.1 shows a picture of the CySeRO test-bed environment.

Figure 4.1 Cyber Security Research and Observation Test-bed at CSIR-4PI

It is a highly reconfigurable and observable environment consisting of 60 nodes. Each node is a rack-mountable server of 1 U size equipped with multiple network interface cards. Each node can be configured as a router or data transmitter or receiver. The test-bed permits emulation of multi-hop network topology and tracking of packet movement across the test-bed. Upcoming Internet protocols like Stream Control Transmission Protocol (SCTP) and Multi Path Transmission Control Protocol (MPTCP) are deployed on the test-bed environment, in addition to standard TCP/IP protocol suite. A wide variety of network tools like tcpdump, pcap library, wireshark, iperf, etc., are also installed on the test-bed.

CySeRO is currently being used for various cyber security and protocol engineering related experimentsin different emulated network conditions like varying packet drop, end-to-end latency, queuing schemes, etc., at packet granularity. Network emulation is performed using ‘tc’ and ‘dummynet’ network emulation tool. The reconfigurable test-bed is also being extensively used for cryptographic research including security analysis of newly designed cryptographic protocols. This enables to test the robustness of these protocols towards countering different forms of attacks. The test-bed is also capable of generating near true random numbers, which are very essential for testing these cryptographic protocols.

Anil Kumar V, Patra G K and Thangavelu R P

4.2 Characterization of internet background radiation

Internet background radiations, also known as unsolicited packets, have become an integral part of the overall Internet traffic. It is reasonably well established that any local network connected to the Internetreceives a sizable amount of unsolicited packets proportionate to the size of the public Internet Protocol (IP) address space allotted to the local network. Unsolicited traffic originates from a wide verity of malicious activities such as Internet wide port scan for identification of vulnerable hosts and services, automated worm propagation, reflections from denial-of-service and distributed denial-of-service attacks due to IP address spoofing, etc.

CSIR-4PI, as part of its Cyber Security Research and Observation (CySeRO) programme, has been collecting and analyzing such unsolicited packets for gaining insight into security dynamics in the cyber space. Considering the fact that source IP address of unsolicited packets could be subjected to spoofing, it is important to validate the source address of these packets before using them for further analysis. An active TCP responder is being developed for responding to these unsolicited packets in a protocol compliant manner to solicit further response for address validation. A preliminary version of the active TCP responder is experimentally deployed at CSIR-4PI. Figure 4.2 shows the data collected in a 240 days period starting from May 2015.

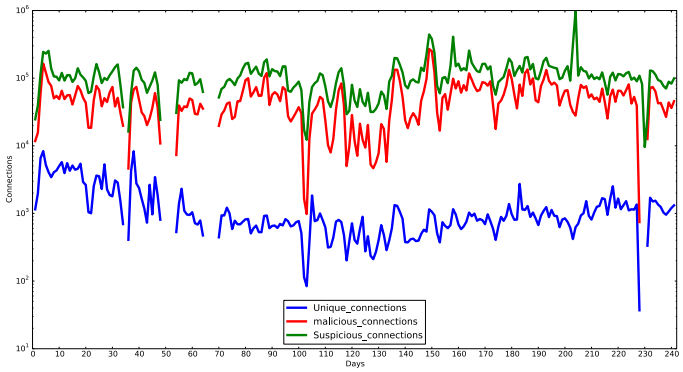

Figure 4.2 Unsolicited TCP connections

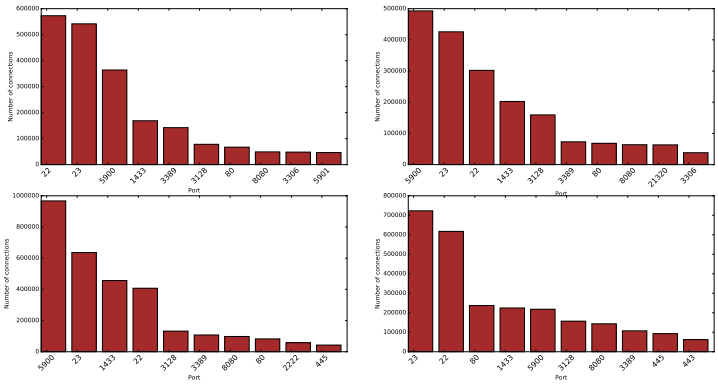

Figure 4.3 TCP port-wise distributions of malicious connection attempts

The data associated with malicious connections are being subjected to further analysis. Towards, this we divided the entire malicious TCP connections into four blocks with each block corresponding to 60 days of data. Figure 4.3 shows one representative result providing additional information about the destination TCP ports with which the malicious hosts are attempting to establish TCP connection.

Each port represents a unique application service. For example, port number 22 (secure shell) and port number 23 (telnet) are two variants of remote login service on Linux and Unix operating systems. Likewise, port number 5900 is the default VNC remote control port. This indicates that majority of the malicious connections are initiated with an intention to gain remote access for possible installation of bots or other malicious programs.

Anil Kumar V, Sujata, Chinmaya Mohini and Jahnavi Meda

4.3 Synchronization of chaos in multiple three-dimensional chaotic maps and its application in cryptography

In recent years, extensive studies have been done in the theory of chaos in different fields of physics, mathematics, engineering, biology, chemistry, economics and atmospheric sciences. Since the beginning of last decade, the use of continuous as well as discrete dynamical systems has been quite popular to develop cryptosystems. Chaoticare the complex mathematical systems that show sensitivity to initial conditions. In such systems, any uncertainty in the beginning (no matter how small) will produce rapidly escalating patterns in the prediction of system's future behavior. These properties are found suitable for cryptosystems.

Here a block cipher is designed to encrypt data using separate chaotic maps for different portions of the plain-text. Sender and receiver systems are synchronized using chaotic synchronization process and are used to generate secret keys. These secret keys can be considered as pseudo-random and applied individually to each block. Such a coupled, chaos-based approach makes the process of key-prediction practically impossible and provides protection against common statistical attacks.

Table-4.1: Governing equations and system parameter values in chaotic range used in the present cryptosystem

Chaotic Map	*Map Number*	*Governing Equation*	*System parameters*
RA	***0***	$\dot{x} = -y - z$ $\dot{y} = x + ay,$ $\dot{z} = b + z(x - c)$	$a = 0.432$ $b = 2$ $c = 4$
RFE	***1***	$\dot{x} = y(z - 1 + x^2) + \gamma x$ $\dot{y} = x(3z + 1 - x^2) + \gamma y$ $\dot{z} = -2z(\alpha + xy)$	$\alpha = 1.1$ $\gamma = 0.87$
LA	***2***	$\dot{x} = \sigma(y - x),$ $\dot{y} = x(\rho - z) - y,$ $\dot{z} = x y - \beta z.$	$\sigma = 10$ $\beta = 2.67$ $\rho = 28$

Our primary focus is on identical synchronization with drive-response (unidirectional) coupling technique. Two identical chaotic systems (with random initial conditions, but identical system parameters) are synchronized at both the ends that intend to communicate. The values of system states at (and after) synchronization point are used to generate keys and realize a PRNG. Weproposea cryptographic algorithm using multiple three-dimensional chaotic maps. We use 3 three-dimensional chaotic maps – Rössler Attractor (RA), Rabinovich–Fabrikant

Equations (RFE) and Lorenz Attractor (LA) - and for convenience, we identify each chaotic map by an integer index(map number N). The Governing equations are shown in Table 4.1.

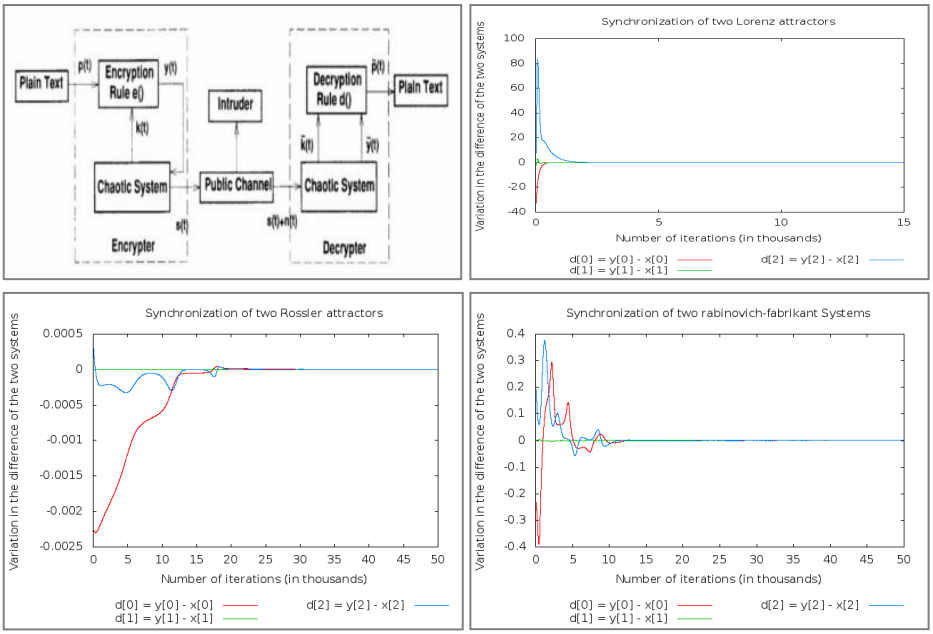

Figure 4.4 Schematic Diagram of a Chaotic Cryptosystem and the synchronization of chaos in a Lorenz, Rössler and RFE Attractor

The convergence in Figure 4.4 indicates the successful synchronization using the three different attractors. The security analysis is as follows:

Cipher text-only attack (COA): In this type of attack, the intruder has access only to the cipher text. For this type of attack, this algorithm depends on the arbitrary system states that drive the evolution of chaotic maps and the order in which they are applied. Initial values for all three system states is chosen randomly between [-1, 1] with decimal precision of up to 6 digits. So, the probability that an intruder can correctly assume the actual message or secret key by intercepting only the encrypted text is ~ 1/(N*3!), where N = 46656 (permutations for 6 decimal places).

Known-plaintext attack (KPA): In this type of attack, intruder has samples of both the plaintext and its encrypted version. However, since the proposed algorithm is based on stream cipher protocol, and each individual character has been encrypted with different key generated from a chaotic system with randomly chosen initial system states, so the probability for an intruder in this attack to correctly identify the secret key is nearly same as cipher text-only attack.

Hence, even for moderate values of system parameters, the probability to break the system tends to zero. So, the proposed approach is fairly unbreakable against above attack models for cryptanalysis.

4.4 A secure key exchange protocol using link weights and dynamic TPM

Artificial Intelligence (AI) concepts have been inherited in cryptography for secure key exchange named as Neural Cryptography. Tree Parity Machine (TPM) which is the main building block of neural key exchange is developed and used for secure communication. In this approach, the participants only need to perform basic arithmetic operations instead of complex number theory approach. The two participants who share their output and input bits in public domain can securely synchronize each other by TPM architecture. However the process can be mimicked by an attacker with the powerful Majority Flipping Attack (MFA) on TPM. The proposed work mainly focuses on overcoming Flipping Attack and Majority Flipping Attack.

The TPM is a feed forward three layer artificial neural network consisting of N input units, K hidden units and an output unit. In order to improve the security of key exchange, a tricky synchronization has been applied on TPM. The number of hidden units K is selected at random at each time step, it is selected among four values 3, 4, 5, and 6 and the size of input vector is determined using constant multiple of LCM of four values. In addition to that, a link weight is connected to a TPM weight, which learns whenever its corresponding weight undergoes learning methods. Synaptic depth (L) of weights signifies security of TPM. Increasing the value of synaptic depth decreases the probability of success for an attacker. Synaptic depth is increased without affecting the performance of TPM significantly by connecting the link weight with the TPM weight. Interestingly, the link weights converge to the link weights of participant's TPM. Convergence of link weights happens faster than convergence of TPM weights. Hence, the mutual information gained with the help of link weights is used in deciding the value of K, which is the number of hidden units at the particular iteration of TPM synchronization. Once the link weights are activated, the TPM no longer has the constant K, instead it obtains the dynamic K at every time steps; it is termed as Dynamic TPM and it is shown in the figure 4.5.

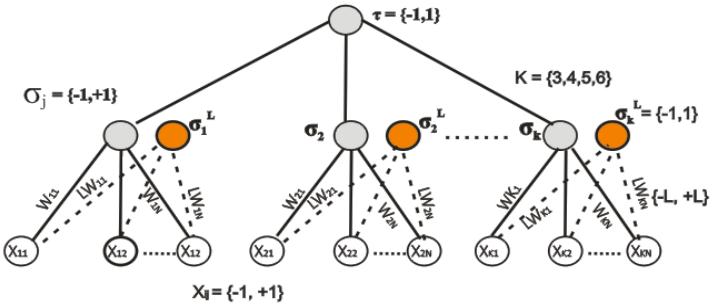

Figure 4.5: A Dynamic TPM with link weights

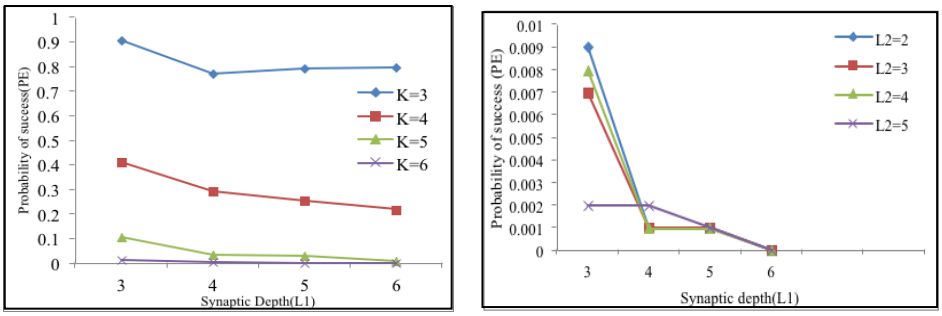

Figure 4.6: (a) Probability of attacker's success as a function of synaptic depth L in TPM averaged over 1000 runs (b) Probability of attacker's success as a function of synaptic depth L in Dynamic TPM averaged over1000 runs.

An Eavesdropper, who listen this network having similar architecture and accessing every public parameter, has disadvantages in synchronizing to genuine participant. Probability of success of an attacker is high when it synchronizes to legitimate TPMs, which is depicted in figure 4.6 (a). In case of Dynamic TPM with link weights, the probability of success of an attacker is exponentially reduced, which is illustrated in the figure 4.6 (b).

Patra G K, Ganesan P

4.5 High performance computing

CSIR-4PI has been providing centralized High Performance Computing facility for the 200 and odd computational scientists across CSIR. It hosts the largest supercomputer, Ananta, of CSIR in additions to few small size clusters as well as storage and network infrastructure.

Ananta (Figure 4.7) has a peak computing power of 360TF and a sustained computing capability of 334TF on the High Performance LINPACK (HPL) and is currently listed as the 7th fastest system in the country and 300th (as of March 2016) fastest in the world. The supercomputer has the distinction of having high average utilization of more than 95% during 2015-16 and an uptime of more than 99%.

Figure 4.7 CSIR centralized 360TF High Performance Computing Facility.

Ananta is a Cluster Platform 3000 with 1088 computing nodes, each of which is a single HP Blade server, with two Intel Xeon E-5 2670 (8 cores, Sandy bridge) processors. The computing nodes are distributed over 17 numbers of 42U 600 mm width racks, resulting in 2176 physical processors and 17408 processing cores. The inter-node communication, which is of high importance in HPC are based on high speed FDR infiniband (providing a dedicated 56 Gbps interconnect bandwidth) in a FAT tree topology in a high availability mode. This is achieved by connecting the nodes using two numbers of centralized Mellanox 648-port core switch through a large number of 16 port leaf switches located in each computing as well as storage rack in a complete redundant mode. The system is equipped with 4GB memory per core, which amounts to about 68 TB of distributed memory in the total system. However, the 48 GB memory located inside a single node can be used for shared memory parallel applications.

An online storage using LUSTRE parallel file system plays an important role in achieving faster data access to individual nodes for carrying out computation in an efficient and fast manner. The high performance parallel file system has a usable capacity of about 2.1 Peta Bytes (3 Peta Bytesraw) and is capable of providing a minimum of 20 Gbps simultaneous read and write. The storage is optimized for performance and data availability using hardware RAID in a RAID6 configuration, parallel I/O through 8 numbers of object servers and two numbers of redundant metadata servers.

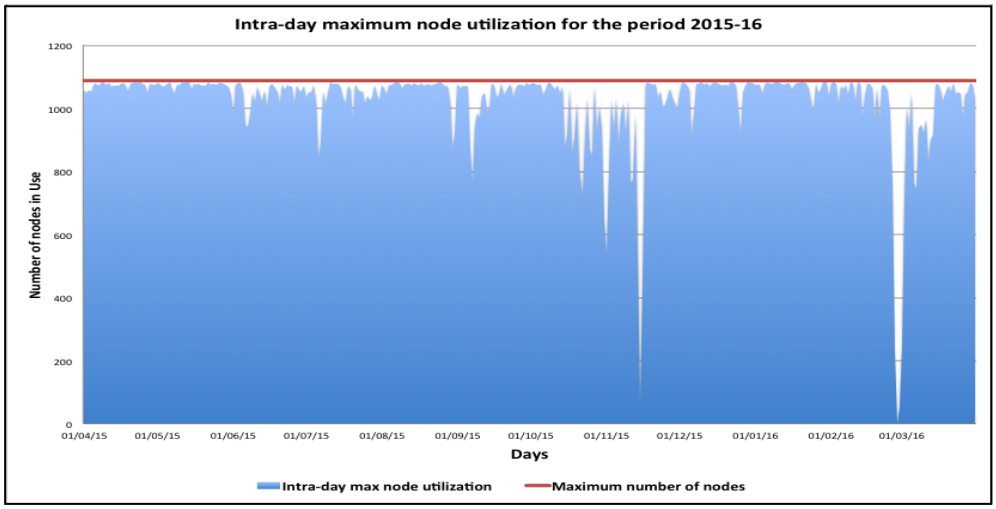

Figure 4.8 Intra-day maximum node used since the 1st April 2015 till 31st March 2016

The highlight of the system is the availability and the average usage of the system. Figure 4.8 shows the intra-day maximum usage in terms of number of nodes for the period 1st April 2015 till 31st March 2016. The size of the problems run by the CSIR computational scientists range from a single node (16 cores) to about 250 nodes (4000 cores). It is interesting to note that the nodes used in a day for most of the days have reached almost the full capacity. This indicates the heavy requirement of computational powers for carrying high science by the scientists and researchers in various fields of computational sciences, such as Biological, Chemical, Engineering, Earth and Atmosphere, Physical and Information Sciences, who use the system in both capacity and capability mode for solving scientific problems. Figure 4.9 shows the distribution of usage by different CSIR laboratories.

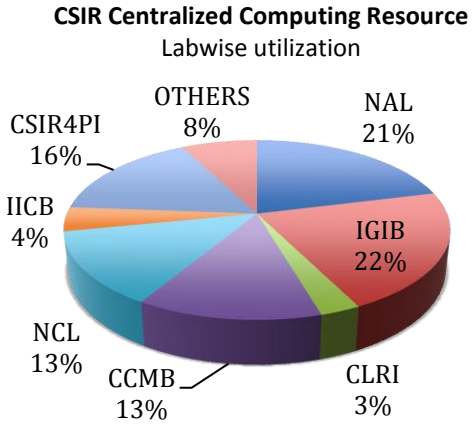

Figure 4.9 Distribution of usage of 360TF system in percentage by Major CSIR labs from 1st April 2015 till 31st March 2016.

In addition to the 360TF super computing system, the Altix ICE cluster has been of great demand (utilization by different CSIR laboratories in Figure 4.10) for solving smaller size problems. This system (Figure 4.11) has 2304 processing cores distributed over 192 nodes interconnected with enhanced hypercube topology using the QDR (32Gbps) infini band interconnect. The system is powered by Intel Westmere-EP Hex core processors running at 2.93/3.06 GHz frequencies, wherein each node has 12 processing cores with 24 GB of memory in a shared memory configurations, while the system as a whole has 4608 GB of memory across the 192 nodes in a distributed architecture. The peak performance the system is 27 TF. This system also uses a LUSTER parallel file system of 30TB for high performance storage access during computation.

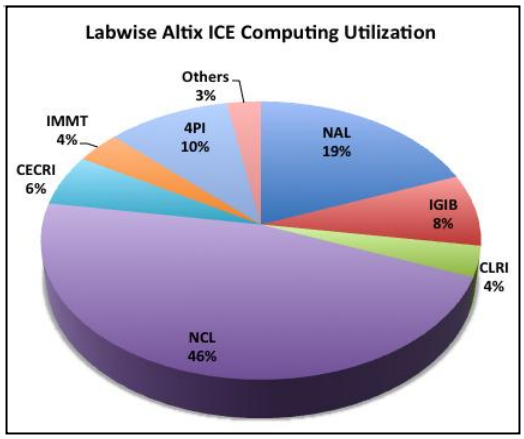

Figure 4.10 Percentage utilization of Altix ICE systems by users from different laboratories of CSIR.

Figure 4.11 Altix ICE systems with 2304 processing cores distributed over 192 nodes and 30 TB of parallel file system along with all associated hardware and software.

The secret of the efficient utilization of a system is the intelligent way of job management. PBS Prowork load manager does this on all the high performance computing system at CSIR-4PI and provides uniform user experience across all systems. The workload manager not only ensures efficient usage of the system but also provides an easy user interaction and submission process. Also the system is equipped with highly optimized Intel compilers and application software both commercial and open source.

High performance archival storage

The parallel file systems are typically used as scratch, to achieve performance, during job computation. However, they are quite expensive. Hence, to store and archive the results, which needs to be preserved for longer period, an archival system based on a high performance SAN(Storage Area Network) is made available to the users. As the data generated grows, the archival system is also upgraded regularly to support the growing needs of storage. The SAN archival system has four LTO Gen 5 drives. Currently the virtualized 3-tired storage solution has 6 TB online (FC), 20TB of near-line (SATA) and scalable offline storage, which can be scaled up to multiple petabytes. The home areas of all the users are centralized on a Network Attached Storage (NAS) of 200TB except the 360TF centralized supercomputing system.

Data center

The 360 TF centralized HPC system, Ananta, is located in a Tier-3 equivalent state-of-the-art data center supported byan energy farm. The highlight of the datacenter is the water based cooling system, viz., Rear Door Heat Exchangers (RDHX), which makes the datacenter as one of the high density and highly power efficient datacenter in the country.

The datacenter has achieved a Power Usage Efficiency (PUE) of less than 1.5, and is one of the best-achieved PUEs in a country like India. The energy farm consists of two redundant compact substations of 1.25 MVA each and for ensuring 24X7 power supply to the datacenter

three numbers of diesel generators, an underground diesel yard of more than 15000 liters capacity, three numbers of UPSes with battery backup is available.

The datacenter as well as the energy farm is monitored 24X7 using a Building Management Service (BMS). The system, the electrical infrastructure, fire detection and suppression system, very early smoke detection system, water leakage system, CCTV, rodent repellant system are monitored continuously to ensure that the system is available to users.

Network facilities

Thanks to National Knowledge Network (NKN), CSIR computational scientists across the country are in a position to connect to the centralized HPC as well as other systems through a high speed and reliable access. The NKN connectivity to CSIR 4PI is currently at 1 Gbps, established through a redundant path. In addition, CSIR-4PI have a backup connectivity of 8 Mbps through ERNET mainly used for mail communication. The Scientists and researchers of CSIR 4PI and NAL (all the three campuses) use the facility from their desktops through a 10Gbpshigh-speedbackbone. All network services namely DNS (Domain Name Server), NIS (Network Information Services), WWW (World Wide Web),institutional repository, webmail, mail services, Intranet and Internet gateways(both for ERNET and NKN connections) have been provided for efficient communication and data dissemination. Unified Threat Management (UTM) system ensures protection of the CSIR 4PI networks as well HPC system from multiple security threats through both the NKN and ERNET links.

Software enhancements

Software enhancements are a continuous process wherein the application software are procured, maintained and upgraded. Some of the heavily used software are ABAQUS, IDL, GAMIT/GLOBK, Tecplot, S-Plus, Hyperworks, Fluent, ANSYS, OpenFOAM etc. CSIR 4PI encourages use of open source software and most software required for modelling and simulations are made available on the HPC systems for users. The systems are used extensively for running complex models in the field of ocean, atmosphere, earth and engineering.

Other technical services

Technical support services were provided to a large number of users across CSIR. The team also has provided technical support for establishing HPC facilities at other CSIR laboratories. This includes the HPC system at CSIR CIMFR, Dhanbad under the collaborative research project DeepCoal. The team also has audited the OneCSIR portal and have provided recommendation to improve the security. In addition, several students from academic institutions across the country have availed the computing services as part of their academic work at CSIR 4PI under the SPARK program. Technical advices and consultancies were provided to various institutions within and outside CSIR.

Thangavelu R P, Patra G K, Anilkumar V, Ashapurna Marndi, Prabhu N Mudkavi V Y, Premalatha, National Aerospace Laboratories