Executive Committee (2015-16/17)

<table>
<thead>
<tr>
<th>President</th>
<th>Prof. Bipin V Mehta</th>
</tr>
</thead>
<tbody>
<tr>
<td>VP</td>
<td>Dr. Anirban Basu</td>
</tr>
<tr>
<td>Hon. Secretary</td>
<td>Mr. Sanjay Mohapatra</td>
</tr>
<tr>
<td>Hon. Treasurer</td>
<td>Mr. R K Vyas</td>
</tr>
</tbody>
</table>

Immd. Past President

Mr H R Mohan

important contact details

For queries, correspondence regarding Membership, contact helpdesk@csi-india.org

Regional Vice-Presidents

<table>
<thead>
<tr>
<th>Region - I</th>
<th>Mr. Shiv Kumar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delhi, Punjab,</td>
<td>Haryana, Himachal</td>
</tr>
<tr>
<td>Poona, Jammu &amp;</td>
<td>Pradesh, Uttaranchal</td>
</tr>
<tr>
<td>other areas in</td>
<td>and other areas in</td>
</tr>
<tr>
<td>Northern India.</td>
<td>CSI-India.org</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Region - II</th>
<th>Mr. Devaprasanna Sinha</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assam, Bihar,</td>
<td>West Bengal, North</td>
</tr>
<tr>
<td>Eastern States</td>
<td>and other areas in</td>
</tr>
<tr>
<td>East &amp; North East</td>
<td>India</td>
</tr>
<tr>
<td><a href="mailto:rvp2@csi-india.org">rvp2@csi-india.org</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Region - VI</th>
<th>Dr. Shirish S Sane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maharashtra and</td>
<td>Goa</td>
</tr>
<tr>
<td><a href="mailto:rvp6@csi-india.org">rvp6@csi-india.org</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Region - VII</th>
<th>Mr. K. Govinda</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamil Nadu,</td>
<td>Pondicherry, Andaman</td>
</tr>
<tr>
<td>Nicobar, Kerala,</td>
<td>Lakshadweep</td>
</tr>
<tr>
<td><a href="mailto:rvp7@csi-india.org">rvp7@csi-india.org</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Region - IV</th>
<th>Mr. Hari Shankar Mishra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jharkhand,</td>
<td>Chhattisgarh, Orissa,</td>
</tr>
<tr>
<td>Delhi, NCR</td>
<td>and other areas in</td>
</tr>
<tr>
<td>Central &amp; South</td>
<td>Eastern India</td>
</tr>
<tr>
<td><a href="mailto:rvp4@csi-india.org">rvp4@csi-india.org</a></td>
<td></td>
</tr>
</tbody>
</table>

Publication Committee (2015-16)

<table>
<thead>
<tr>
<th>Dr. A K Nayak</th>
<th>Chairman</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. R Nadarajan</td>
<td>Member</td>
</tr>
<tr>
<td>Mr. Ravikiran Manikar</td>
<td>Member</td>
</tr>
<tr>
<td>Dr. Durgesh Kumar Mishra</td>
<td>Member</td>
</tr>
<tr>
<td>Mr. Suresh Chandra Satapathy</td>
<td>Member</td>
</tr>
<tr>
<td>Dr. Vinip Tyagi</td>
<td>Member</td>
</tr>
<tr>
<td>Dr. R N Satapathy</td>
<td>Member</td>
</tr>
</tbody>
</table>

Important links on CSI website

<table>
<thead>
<tr>
<th>About CSI</th>
<th><a href="http://www.csi-india.org/about-csi">http://www.csi-india.org/about-csi</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Structure and</td>
<td><a href="http://www.csi-india.org/web/guest/structureandorganisation">http://www.csi-india.org/web/guest/structureandorganisation</a></td>
</tr>
<tr>
<td>Organization</td>
<td></td>
</tr>
<tr>
<td>Executive</td>
<td><a href="http://www.csi-india.org/executive-committee">http://www.csi-india.org/executive-committee</a></td>
</tr>
<tr>
<td>Committee</td>
<td></td>
</tr>
<tr>
<td>Nomination</td>
<td><a href="http://www.csi-india.org/web/guest/nominations-committee">http://www.csi-india.org/web/guest/nominations-committee</a></td>
</tr>
<tr>
<td>Committees</td>
<td></td>
</tr>
<tr>
<td>CSF Fellows</td>
<td><a href="http://www.csi-india.org/web/guest/csf-fellows">http://www.csi-india.org/web/guest/csf-fellows</a></td>
</tr>
<tr>
<td>National, Regional &amp; State</td>
<td><a href="http://www.csi-india.org/web/guest/national-regional-state">http://www.csi-india.org/web/guest/national-regional-state</a></td>
</tr>
<tr>
<td>Student Coordinators</td>
<td><a href="http://www.csi-india.org/web/guest/student-coordinators">http://www.csi-india.org/web/guest/student-coordinators</a></td>
</tr>
<tr>
<td>Collaborations</td>
<td><a href="http://www.csi-india.org/web/guest/collaborations">http://www.csi-india.org/web/guest/collaborations</a></td>
</tr>
<tr>
<td>Distinguished Speakers</td>
<td><a href="http://www.csi-india.org/web/guest/distinguished-speakers">http://www.csi-india.org/web/guest/distinguished-speakers</a></td>
</tr>
<tr>
<td>Divisions</td>
<td><a href="http://www.csi-india.org/web/guest/divisions">http://www.csi-india.org/web/guest/divisions</a></td>
</tr>
<tr>
<td>Regions</td>
<td><a href="http://www.csi-india.org/web/guest/regions">http://www.csi-india.org/web/guest/regions</a></td>
</tr>
<tr>
<td>Chapters</td>
<td><a href="http://www.csi-india.org/web/guest/chapters">http://www.csi-india.org/web/guest/chapters</a></td>
</tr>
<tr>
<td>Student Branches</td>
<td><a href="http://www.csi-india.org/web/guest/student-branches">http://www.csi-india.org/web/guest/student-branches</a></td>
</tr>
<tr>
<td>Membership Services</td>
<td><a href="http://www.csi-india.org/web/guest/membership-services">http://www.csi-india.org/web/guest/membership-services</a></td>
</tr>
<tr>
<td>Upcoming Events</td>
<td><a href="http://www.csi-india.org/web/guest/upcoming-events">http://www.csi-india.org/web/guest/upcoming-events</a></td>
</tr>
<tr>
<td>Publications</td>
<td><a href="http://www.csi-india.org/web/guest/publications">http://www.csi-india.org/web/guest/publications</a></td>
</tr>
<tr>
<td>Student’s Corner</td>
<td><a href="http://www.csi-india.org/web/education-directorate/student-s-corner">http://www.csi-india.org/web/education-directorate/student-s-corner</a></td>
</tr>
<tr>
<td>CSI Awards</td>
<td><a href="http://www.csi-india.org/web/guest/csi-awards">http://www.csi-india.org/web/guest/csi-awards</a></td>
</tr>
<tr>
<td>CSI Certification</td>
<td><a href="http://www.csi-india.org/web/guest/csi-certification">http://www.csi-india.org/web/guest/csi-certification</a></td>
</tr>
<tr>
<td>Upcoming Webinars</td>
<td><a href="http://www.csi-india.org/web/guest/upcoming-webinars">http://www.csi-india.org/web/guest/upcoming-webinars</a></td>
</tr>
<tr>
<td>About Membership</td>
<td><a href="http://www.csi-india.org/web/guest/about-membership">http://www.csi-india.org/web/guest/about-membership</a></td>
</tr>
<tr>
<td>Membership Benefits</td>
<td><a href="http://www.csi-india.org/web/guest/membership-benefits">http://www.csi-india.org/web/guest/membership-benefits</a></td>
</tr>
<tr>
<td>BABA Scheme</td>
<td><a href="http://www.csi-india.org/web/guest/baba-scheme">http://www.csi-india.org/web/guest/baba-scheme</a></td>
</tr>
<tr>
<td>Special Interest Groups</td>
<td><a href="http://www.csi-india.org/web/guest/special-interest-groups">http://www.csi-india.org/web/guest/special-interest-groups</a></td>
</tr>
<tr>
<td>Membership Subscription Fees</td>
<td><a href="http://www.csi-india.org/web/guest/membership-subscription-fees">http://www.csi-india.org/web/guest/membership-subscription-fees</a></td>
</tr>
<tr>
<td>Membership and Grades</td>
<td><a href="http://www.csi-india.org/web/guest/membership-and-grades">http://www.csi-india.org/web/guest/membership-and-grades</a></td>
</tr>
<tr>
<td>Institutional Membership</td>
<td><a href="http://www.csi-india.org/web/guest/institutional-membership">http://www.csi-india.org/web/guest/institutional-membership</a></td>
</tr>
<tr>
<td>Become a member</td>
<td><a href="http://www.csi-india.org/web/guest/become-a-member">http://www.csi-india.org/web/guest/become-a-member</a></td>
</tr>
<tr>
<td>Upgrading and Renewing Membership</td>
<td><a href="http://www.csi-india.org/web/guest/upgrading-and-renewing-membership">http://www.csi-india.org/web/guest/upgrading-and-renewing-membership</a></td>
</tr>
<tr>
<td>Download Forms</td>
<td><a href="http://www.csi-india.org/web/guest/download-forms">http://www.csi-india.org/web/guest/download-forms</a></td>
</tr>
<tr>
<td>Membership Eligibility</td>
<td><a href="http://www.csi-india.org/web/guest/membership-eligibility">http://www.csi-india.org/web/guest/membership-eligibility</a></td>
</tr>
<tr>
<td>From the President Desk</td>
<td><a href="http://www.csi-india.org/web/guest/from-the-president-desk">http://www.csi-india.org/web/guest/from-the-president-desk</a></td>
</tr>
<tr>
<td>CSIC Communications (PDF Version)</td>
<td><a href="http://www.csi-india.org/web/guest/csic-communications-pdf-version">http://www.csi-india.org/web/guest/csic-communications-pdf-version</a></td>
</tr>
<tr>
<td>CSIC Communications (HTML Version)</td>
<td><a href="http://www.csi-india.org/web/guest/csic-communications-html-version">http://www.csi-india.org/web/guest/csic-communications-html-version</a></td>
</tr>
<tr>
<td>CSJ Communication</td>
<td><a href="http://www.csi-india.org/web/guest/cs-commencement">http://www.csi-india.org/web/guest/cs-commencement</a></td>
</tr>
<tr>
<td>CSJ eNewsletter</td>
<td><a href="http://www.csi-india.org/web/guest/csj-enewsletter">http://www.csi-india.org/web/guest/csj-enewsletter</a></td>
</tr>
<tr>
<td>CSIC Chapters SBS News</td>
<td><a href="http://www.csi-india.org/web/guest/csic-chapters-sbs-news">http://www.csi-india.org/web/guest/csic-chapters-sbs-news</a></td>
</tr>
<tr>
<td>Education Directorate</td>
<td><a href="http://www.csi-india.org/web/guest/education-directorate">http://www.csi-india.org/web/guest/education-directorate</a></td>
</tr>
<tr>
<td>National Students Coordinator</td>
<td><a href="http://www.csi-india.org/web/guest/national-students-coordinator">http://www.csi-india.org/web/guest/national-students-coordinator</a></td>
</tr>
<tr>
<td>Awards and Honors</td>
<td><a href="http://www.csi-india.org/web/guest/awards-and-honors">http://www.csi-india.org/web/guest/awards-and-honors</a></td>
</tr>
<tr>
<td>eGovernance Awards</td>
<td><a href="http://www.csi-india.org/web/guest/e-governance-awards">http://www.csi-india.org/web/guest/e-governance-awards</a></td>
</tr>
<tr>
<td>IT Excellence Awards</td>
<td><a href="http://www.csi-india.org/web/guest/it-excellence-awards">http://www.csi-india.org/web/guest/it-excellence-awards</a></td>
</tr>
<tr>
<td>YITP Awards</td>
<td><a href="http://www.csi-india.org/web/guest/yitp-awards">http://www.csi-india.org/web/guest/yitp-awards</a></td>
</tr>
<tr>
<td>CSI Service Awards</td>
<td><a href="http://www.csi-india.org/web/guest/csi-service-awards">http://www.csi-india.org/web/guest/csi-service-awards</a></td>
</tr>
<tr>
<td>Academic Excellence Awards</td>
<td><a href="http://www.csi-india.org/web/guest/academic-excellence-awards">http://www.csi-india.org/web/guest/academic-excellence-awards</a></td>
</tr>
<tr>
<td>Contact Us</td>
<td><a href="http://www.csi-india.org/web/guest/contact-us">http://www.csi-india.org/web/guest/contact-us</a></td>
</tr>
</tbody>
</table>

Important Contact Details

For queries, correspondence regarding Membership, contact helpdesk@csi-india.org

CSI Communications | May 2015 | www.csi-india.org
Cover Story
Cloud Security – Challenges at a Glance
R Sridaran, Disha H Parekh Doshi and Sudhir Kumar Suman

Improving Cybersecurity using NIST Framework
Sandeep Godbole

Cyber Security: Issues and Challenges
N J Rao

Security, Privacy and Trust in Social Networking Sites
Richa Garg, Ravi Sankar Veerubhotla and Ashutosh Saxena

Comparative Evidence of Cryptographic Based Algorithms under the Cloud Computing Environment to Ensure Data/System Security
Shruti Chhabra and V S Divit

Privacy Security Settings – Challenges of Social Media
Mini Ulanat and K Poulose Jacob

Importance of Morality, Ethical Practices and Cyber Laws as Prelude to Cybersecurity
D G Jha

Do You Need an Operating System to Run an Application
Biswajit Mohapatra and Debasis Roy Choudhuri

Context Aware Intelligence: Approach for Multi-Dimensional Security
Amit Badheka

e-Learning for Effective Classroom Teaching: A Case Study on Educational Institutes in India
Sarika Sharma

Brain Teaser
Dr. Durgesh Kumar Mishra

A Report from CSI Division IV Communications
Dr. Durgesh Kumar Mishra

CSI News

PLUS
Dear Fellow CSI Members,

The internet has changed the world completely. Now it is available for us for the fast data transmission, for doing all kind business and satisfying needs. But at the same time, data passing from source to destination securely is the important task. One of the necessary requirements to prevent data theft and protect the same is securing the information on the transmission channel and across the network. Further, open access to the Internet has revolutionized the way individuals communicate and collaborate, entrepreneurs and corporations conduct business, and governments and citizens interact. As number of internet users is about to touch three billion, the number of cyber security threats is also increasing. Cyber threats are no longer restricted to fragments of malicious code, aimed to exasperate, incite or stall; now the threats are strategic, targeted, organised and relentless. Such targeted attacks can cause significant financial losses as well as deep-seated damage. In the age on internet, cybercriminality affects everyone individuals, companies, institutions, governments. It has become a curse of society.

As per a study of ASSOCHAM, the cyber crimes in India are likely to cross the 3,00,000 at compounded annual growth rate (CAGR) of about 107 per cent. As per the findings, every month nearly 12,456 cyber crime cases are registered in India. What is causing even more concern is that the origin of these crimes is widely based abroad in countries including China, Pakistan, Bangladesh and Algeria among others. Phishing attacks of online banking accounts or cloning of ATM, Debit cards are common occurrences. The increasing use of smartphones, tablets for online banking, financial transactions has also increased the vulnerabilities to a great extent. With increasing use of information technology enabled services such as e-governance, online business and electronic transactions protection of personal and sensitive data have assumed paramount importance. The economic growth of any nation and its security whether internal or external and competitiveness depends on how well it is its cyberspace secured and protected.

Due to increase in internet penetration and use of online banking India is becoming a favourite among the cybercriminals, who target online financial transactions using malware. India ranks third after Japan and US in the tally of countries most affected by online banking malware during the year of 2014. Indian websites are being hacked by various hacker group spread across worldwide and likely to touch 85,000 by now.

The economic growth of a country depends on how well its physical and cyber space is secured. Today we are living in a world that has virtually no privacy and a big number of cybercrimes. Due to nature of cyberspace cyber security is a very big challenge. None of us is immune from the threat of cyberattacks. So there is an urgent need of developing techniques to secure our cyberspace. Apart from developing techniques awareness related to cyber security is also needed. Computer Society of India selected theme of CSI communications (The Knowledge Digest for IT Community) - May issue as Cyber Security to discuss various techniques and create awareness about cyber security.

This issue has come up with a new column "Message from Vice-President". This issue has a number of good articles related to Cyber Security. In the article by R. Sridaran, D.H.P. Doshi and S. K. Suman, challenges in cloud security are described, while S. Godbole has described the ways to improve cybersecurity using National Institute of Standards and Technology (NIST) framework. We have also provided gist of National Cyber Security Policy – 2013. N. J. Rao has described cyber security issues and challenges in his article. S. Chhabra and V.S. Dixit have done a study on “Comparative Evidence of Cryptographic based Algorithms under the Cloud Computing Environment to ensure Data/System Security” to identify, analyze and report the evidence of different cryptographic security algorithms.

Social networking is very popular these days. M. Ulanat and K. P. Jacob in “Privacy Security Settings – Challenges of Social Media” and R. Garg, R.S. Veerubhotla and A. Saxena in “Security, Privacy and Trust in Social Networking Sites” have described security issues related to social networking sites. In the use of the technology, there is a need of moral values and ethics in every citizen. D. G. Jha in his article has described the importance of morality and ethical practices. In an article, Amit Badhekh has given an approach for multidimensional security called context aware intelligence for enterprise applications.

We have included a case study on e-learning for effective classroom teaching by Sarika Sharma. Hope this study will help in planning of e-learning in schools, colleges and universities. In Research Front category we have selected an article by B. Mohapatra and D.R. Choudhuri that describes allocation containerization in their article “Do you need an OS”. This issue also contains practitioners’ workbench, crosswords, CSI reports, and news from divisions, chapters, student branches, and calendar of events.

I take this opportunity to credit of successfully bringing this issue to guest editor Dr. Vipin Tyagi. I am thankful to Prof. M.N. Hoda and Dr. Durgesh Mishra for their support in bringing out this issue. On behalf of publication committee, I wish to express my sincere gratitude to all authors and reviewers for their contribution to this issue.

I hope this issue will be successful in its aim of creating awareness about Cyber Security, providing information about latest trends in cyber security research and provide new ideas for research in the area.

Finally we look forward to receive the feedback, contribution, criticism, suggestions and reply from our esteemed members and readers at csic@csi-india.org.

Prof. A.K. Nayak
Chief Editor
Dear Members

I am happy to inform you that CSI Communications, April 2015 issue with a theme “Digital India” has been well received by the members at large. The newly formed Publication Committee headed by Dr. A. K. Nayak and the Guest Editor Dr. Durgesh Kumar Mishra has done commendable work in bringing April, 2015 issue of CSI Communications well. You could have observed the changes like more coverage of activities conducted by various chapters and student branches. I request all the Chapters and Student Branches to send their activity reports for timely publications in CSI Communications. CSI is now adopting Green initiative by changing over from print version of CSI Communications to digital version in immediate future. The digital version will be available on CSI website and Mobile App. This is a practice followed by majority of the professional bodies over the globe.

I acknowledge the exemplary work done by the previous Publications Committee chaired by Dr. S. S. Agarwal and the editorial team for bringing various theme based issues of CSI Communications.

As per CSI byelaws, various committees are formed by the Executive Committee. These Committees have started working on the tasks assigned to them. The Membership Committee has prepared a blue print for the growth of the membership and better service to the members. This initiative will attract more IT professionals, academicians and students to get associated with CSI - the largest network of computer professionals in India.

The 50th Annual Convention - CSI – 2015 with the theme DIGITAL LIFE is being held during 3-5December, 2015 at New Delhi. The team of Delhi Chapter has started gearing for the grand success of this Golden Jubilee Convention. The call for papers is announced. I hope you all will participate in large number to deliberate and discuss the emerging trends in ICT Based Innovation, Next Generation Networks, 3-D Silicon Photonics & HPC, Real Time Languages Translation, Sensors, Big Data Analytics, Systems and Architecture and Cyber Security.

We have received very good response towards the Call for Nominations for Regional Student Co-ordinators (RSC) and State Student Co-ordinators (SSC). The region wise committee headed by each RVP will scrutinize nominations and identify RSC and SSC under that region in due course of time.

At present, most of the IT companies want to automate work to improve the efficiency and economize the error free processes like software testing. The processes adopted by BPO and KPO are repetitive in nature and can be automated easily. This will bring major change in the employment opportunity. Many entry level jobs will become redundant affecting the placement opportunity of young IT graduates. However, the acquiring skills required for automation will bring high level quality employment. We need to deliberate on this major paradigm shift in job market and CSI can play a role in

Re-skilling to help employees to survive the automation wave in the IT industry.

The other area of interest for CSI is to discuss the importance of STEM (Sciences, Technology, Engineering and Mathematics) courses which have become increasingly important and prominent in all sectors of economy in which Computing and IT are playing major role. The Indian universities are required to enhance their policies and practices to emphasize the importance of STEM courses. The role of CSI could be promoting innovation and computing tools in the fields other than traditional computing and programming.

These days, debate went on Net Neutrality in India. The majority of the net users have favoured net neutrality and sent petitions in lakhs to TRAI and objected the move of ISP against net neutrality.

I had an opportunity to meet the prominent members of Ahmedabad, Vallabh Vidyanagar, Pune and Udaipur Chapter recently. The Chapters are very active in conducting various activities for the members and IT fraternity in the emerging areas. They are also active in arranging advance level training programs for students, academicians and IT professionals. It is heartening to note that Managing Committee Members of Pune Chapter are visiting student branches and interacts with the student members regularly. Their enthusiasm attracts more students to join CSI. The Ahmedabad Chapter has planned a common placement platform to provide equal opportunities to students and recruiters by arranging a Placement Week in near future. As part of Golden Jubilee Celebrations, this Chapter has planned lecture series during the year, by inviting prominent professionals to share their expertise in different domains in which IT is a major tool. I may I suggest MC members of other Chapters to follow such best practices to reach to a large number of members, students and society at large.

At present, there are many Special Interest Groups (SIGs) under the banner of CSI. Many SIGs are active and others are required to be active. My colleague Dr. Anirban Basu, Vice President and President Elect is working on revamping SIGs to strengthen their presence. I urge Conveners of SIGs to take positive steps to make SIGs, more vibrant.

Recently, I represented CSI at SEARCC (South-East Asian Regional Computer Confederation) Executive Committee Meeting at Singapore. This committee meets twice in a year and deliberates on new initiatives. In this Meeting, the members deliberated on SEARCC Awards and Recognition Program, Virtual Conferences, Draft Strategic Plan 2015 – 2020 and SEARCC Conference at WCC-2015 hosted by Australian Computer Society in South Korea. The other representatives of Computer Societies of Sri Lanka, New Papua Guinea, Australia and Malaysia presented their views on important issues. The ISSC – 2015 is hosted by Sri Lanka Computer Society during 9-11 October, 2015 at Sri Lanka. This will be great opportunity for our schools to participate in this competition. An announcement in this regard will be made by Education Directorate, CSI in due course of time.

I look forward for your valuable suggestions for the better working of CSI.

With best wishes,

Bipin V Mehta
For the last 50 years, the Computer Society of India, the largest and oldest body of IT professionals in India has been working on promoting use of IT among the different segments of the society. CSI was considered to be the prime body of IT professionals few decades back and recognized by the Governments in the states and at the Centre as a prominent group with capability to advise the Governments on framing policy matters. Now it is the high time to take the society to a greater height to contribute significantly for transforming the nation to Digital India.

The new ExecCom which assumed office effective April 1, 2015 is committed to bring more efficiency, transparency and effectiveness in functioning of the society. The team comprises of dynamic members who have been elected this year as Vice President, Treasurer, Chairs of Division I,III and V and as Vice Presidents of Regions I, III, V and VII. They along with the incumbent President, Hony. Secretary, and Chairs of Division II and IV and Vice Presidents of Regions II and VI are determined to change the face of Computer Society of India. In this golden jubilee year, we need to increase our membership substantially both from the corporate world and from the academic community. Although CSI has the biggest following among the student community, we need to have more Student Branches throughout the country. To attract more members we need to organize better quality events and improve the quality of our journals.

To achieve these:

- ExecCom in its first meeting decided to rationalize the Membership fee structure and decided to have an uniform fee structure irrespective of the age. This has become essential to attract young IT professionals to CSI. An appeal is being made to CSI Members to approach their acquaintances in the Industry and in the academic community to make them members of CSI.

- The Publication Committee has started their work in the right earnest. Due to the resignation of the erstwhile Members of Editorial Board of CSI Communications, all efforts have been made to publish CSI Communications in time. A Call for Editors was made which received an overwhelming response. New Editorial team is getting constituted for all the CSI journals. Efforts are on to ensure the timely publication of Journal of Computing.

- Students and members of the Academic Community have been the main strength of CSI. For this the CSI Education Directorate is being revamped, new procedures are being put in place for timely response to queries and for processing membership applications. Attempts are being made to start a Journal solely dedicated to publishing papers by the students.

- A call has been given to enlist a new team of student coordinators both at the Region and at State levels. I am happy that the response to the call has been extremely good and a very large number of our members have shown interest in contributing towards increasing our student activities.

- CSI Web site has not been working satisfactorily and there have been numerous complaints about the difficulties the members have been facing in using the web site. Prospective members have failed to file their membership application and pay their fees by credit cards due to poor operation of CSI web site. Decision has been taken to develop a new web site at the earliest and to integrate all operations of CSI under the same software framework.

- It has been decided that Chapters when organizing any event will keep the relevant RVP in the Advisory Committee. The RVPs are being encouraged to visit the Chapters and to interact with the members. All chapters have been asked to use the official logo of CSI given below and misuse of CSI logo will be taken seriously.

- The procedure for publishing reports of various events organized by different CSI Chapters and Student Branches is being worked upon and the streamlined procedure will be announced soon.

- Over the years, CSI has signed Memorandum of Understanding with different bodies and international societies. These are being looked into so that these MOUs can be used more effectively for the benefit of our Members.

To summarize, in the brief period that the new ExecCom has taken over, a plan of work has been drawn to improve the working of CSI. In this endeavor, we hope to get the cooperation of all sections of CSI Members. For any suggestions or issues, members can always approach the ExecCom members at any point of time.

Let us work together to make a difference.

Best wishes,

Dr Anirban Basu
Members of CSI ExecCom led by the Hony. Secretary Mr. Sanjay Mohapatra and accompanied by DIV V Chair and Vice President cum President (Elect) of CSI for the year 2015-16/17 Prof. Dr. Anirban Basu, DIV III Chair Dr. A K Nayak and DIV I Chair Dr. M N Hoda met the legendary personality Padma Bhusan Faqir Chand Kohli, considered Father of Indian Software Industry on March 27, 2015 at his office in Mumbai.

Sri F C Kohli who turned 90 in February last year shared his views on Computer Society of India, of which he was the President few decades back. He shared his thoughts with the ExecCom members on a variety of subjects including direction CSI should take to bring IT to the masses. He feels that the Indian IT industry should give lot of thrust on computerization in Indian languages. Sri Kohli shared his thoughts on several other topics and discussed his thoughts on priorities for progressing India in the fields of Education, Information Technology, Power and Agriculture. He has been working on improving the condition of India in these areas and shared his personal experiences on these aspects.

The ExecCom members who met him shared their plans about CSI and sought his blessings and good wishes to restore the past glory of CSI.

Meeting with Dr. FC Kohli

Senior ExecCom Members (left to right) : Dr. Anirban Basu, Dr A K Nayak, Sri F C Kohli , Dr. M N Hoda, Mr. Sanjay Mohapatra .

Guest Editor - Dr. Vipin Tyagi

Dr. Vipin Tyagi, Guest editor for May Issue of CSI Communications is working as faculty in Dept. of CSE at Jaypee University of Engg and Technology, Raghogarh, Guna (MP) India. He is Regional Vice President of Computer Society of India of Region 3. He is also associated with CSI Special Interest Group on Cuber Forensics. He has about 20 years of teaching and research experience. He is a senior life member of Computer Society of India. He was President of Engineering Sciences Section of the Indian Science Congress Association for the term 2010-11, and recorder for the term 2008 - 2010. He is a Life Fellow of the Institution of Electronics and Telecommunication Engineers. He is actively associated with professional societies like CSI, IETE, ISCA, Indian Society of Remote Sensing, IEEE etc. He was nominated by Indian National Science Academy (INSA), New Delhi under international collaboration to visit Czech Republic, for two weeks in May 2012. He has published more than 100 papers in various reputed journals, advanced research series and has attended several national and international conferences in India and abroad. He is Principal Investigator of research projects funded by DRDO, MP Council of Science and Technology and CSI.

He is an expert in the area of Cyber Security, Cyber Forensics and Image Processing. He can be reached at dr.vipin.tyagi@gmail.com
Cloud Security - Challenges at a Glance

Introduction

Any organization today requires dynamism, abstraction and resource sharing at a superior level in order to flourish and accomplish maximum success. These three requirements mentioned are satisfied by the one, very genuine computing model - known as Cloud Computing (CC), which is becoming the technology trend of the future. The backbone of CC model is a server which is considered as a very crucial part behind the entire processing environment. Server environment involved in cloud computing need not be a high-end hardware but instead it ties together the power of inexpensive hardware on a larger scale in contrast to using lesser amount of servers, high in quality. It is helpful for an enterprise to use CC capabilities since it allows all of their customers to access the data from any computer when required, which prevents data loss or mismanagement of files. This helps an organization to gain improved data security.

CC has become the most preferred business model of this decade. Since cloud users who are tremendously increased in recent years tend to keep their data and information in the cloud. This raises lot of issues relating to the aspects of safety and security. Amongst the different issues connected with cloud computing, the security is being the most sensitive one. This has been already pointed by the International Data Corporation (IDC)[1] and Aman Bakshi et al.[2].

Since CC incorporates different technologies used with operating system such as resource sharing, transaction management, scheduling, memory management etc., and also some others relating to networks databases and so on. The traditional issues associated with each one of them will automatically become part of cloud computing issues also. Moreover cloud itself consists of many contexts for security issues. There is a special category of threats emerge due to virtualization[3]. This happens due when a virtual machine is to be mapped to several physical machines. The data security consists of methods and policies relating to encryption and data sharing. Security algorithms are also being used widely for resource allocation, memory management, detection of malware in clouds using data mining techniques etc. etc., Any connection regardless of its scale, relies on data and infringement by an unauthorized individual can have large-scale sway on the business[4].

Cloud Security Threats at a Glance:

The threats of CC vary according to the delivery model in used. An ideal way is to categorize them into confidentiality, integrity and availability (CIA)[4]. Some of the most common threats categorized in this way are depicted in Fig. 1.

Threats associated with Confidentiality

Malicious Insiders: CC presents flexibility by outsourcing the services, but it also adds intrinsic risks of malicious insiders and offensive use of login access by an unauthorized person.

External Attackers: CC vendors supply Application Program Interface (API) for clients to merge with and avail services. Customers utilizing these APIs are proposing much more associated services in order to help their own clients. Cloud APIs with frail authentication and access to command can risk the confidentiality of the pertaining customer. When the services are deployed, any vulnerability in the API can endanger the security issues for the users, because of malevolent intents.

Data Loss: Data in the cloud is prone to plentiful risks, for example, deletion of record, loss of encryption key, weak encryption, altered data, etc.

Threats associated with Integrity

Data Segregation: It is generally in practice to keep the data in cloud in the encrypted form. This improves security. The data segregation problem emerges when some clients do not support encryptions due to the fear that encryption may mislead to devastate the data.

User Access: Threats due to user access may happen because of unsafe access control processors which may even enable the outsider to gain an unauthorized access to the cloud services and data sources.

Data Quality: This is a very important factor that avoids happening of crashes by malicious insider or any outsider. This threat is also commonly occurring when multiple customer’s data are being hosted by the cloud providers.[5]

Threats associated with Availability

Change Management: The cloud provider is expected to have proper change management policies across all the cloud delivery models. Sometimes this may lead to some negative effects also that need to be addressed.

![Cloud Security Threats](image_url)
Denial of Service threat: This is caused normally in public cloud services. However, the threat can also have an impact on different cloud service models, even may go to the extent of launching applications or services relating to hardware which in turn may cause a denial of service.

Physical Interruption: This threat is caused due to the interruption to cloud services caused due to dissimilarities in the physical access between cloud service providers and their customers. In case either of the office environments are not protected properly or the remote working is dealt frequently, the physical interruption threats may occur.

Exploiting fragile recovery practices: This threat will be frequently occurring due to insufficient policies pertaining to the recovery procedure whenever the client initiates. This has got an implication on the recovery time also.\(^{[46]}\)

Some Threat Avoidance Practices

Every cloud provider is expected to incorporate the threat management capabilities at a gross level in order to ensure that the shared storage management preserves all its data. A time tested encryption plan should be in place since majority of threats are due to the illegal access to the data, a proper access control mechanism should also be thought of. It is also needed to have the data security features embedded with storage, backup and retrieval procedure. Even though many of the securities features contain the above capabilities, there is a need for better awareness\(^{[7]}\). It is also time to think of a proper security models which promotes CIA.

Conclusion

Even though the CC is very much popular and ever growing, the threats associated with them need to be brought under limelight. This includes the threats across different levels from network to application, threats relating to the data and also issues linked with the confidentiality and integrity and so on. A proper auditing at defined intervals should be performed mandatorily. This would narrow down the security issues connected with the cloud. The Service Level Agreements (SLA) should also aim at capturing the most common errors any human may commit in the CC scenario.

References


About the Authors

Dr. R. Sridaran is a Dean, Faculty of Computer Applications, at Marwadi Education Foundation’s Group of Institutions, Rajkot, Gujarat. He is a life member of CSI and also the Founder Chairman for CSI, Rajkot Chapter. He has 15 years of teaching experience, 7 years of industry experience. His areas of interest are Software Engineering, Cloud Computing and E-Learning.

Mrs. Disha H. Parekh Doshi is an Assistant Professor, Faculty of Computer Applications, at Marwadi Education Foundation’s Group of Institutions, Rajkot, Gujarat and also a research scholar of Bharathiar University. She has 6 years of teaching experience. Her areas of interest are Cloud Computing, Virtualization and Applications of Cloud.

Mr. Sudhir Kumar Suman is an Assistant Professor, Faculty of Computer Applications, at Marwadi Education Foundation’s Group of Institutions, Rajkot, Gujarat. He has having 2 years of teaching experience.

OBITUARY

Mr. V V P Swamy,
Member, Computer Society of India.

Mr. V.V.P. Swamy passed away on 28th March 2015, in Hyderabad at the age of 72.

Mr. V. V. P. Swamy was one of the early members of the Computer Society of India, Ranchi chapter, along with other IT stalwarts in Ranchi, such as Mr. R. K. Sandhir of MECON, Prof. Kanta Rao of BIT Mesra, Mr. Kaushik Roy of HEC. He contributed significantly to the chapter by bringing in on the table, the then fast emerging role of computerization in coal mining, explorations, mine planning and development, MIS and Office Automation. He has given talks in CSI seminars/workshops.

After his retirement from the industry in 2001 till the last days of his life, he kept himself active teaching in several engineering colleges in and around Hyderabad. While in Delhi, he also worked on themes like Modernization, Mechanization, Automation, and Computerization in Asian Coal mines.

Mr. V.V.P.Swamy is survived by his wife, Sita Devi and two well-settled daughters, Lakshmipriya and Krishnapriya with their families in Delhi and Hyderabad respectively. CSI deeply mourns his death and conveys condolence to the bereaved members of his family and friends. May God’s grace grants his soul to rest in peace. ***
Vipin Tyagi
Guest Editor, Jaypee University of Engg and Technology, Raghogarh, Guna (MP)

National Cyber Security Policy 2013

http://deity.gov.in/content/national-cyber-security-policy-2013-1

VISION: To build a secure and resilient cyberspace for citizens, businesses and Government

MISSION: To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities, and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation

Objectives:
•to create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy
•to create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people)
•to strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem
•to enhance and create National and Sectoral level 24x7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response resolution and crisis management through effective predictive, preventive, protective, response and recovery actions
•to enhance the protection and resilience of Nation’s critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources
•to develop suitable indigenous security technologies through frontier technology, research, solution oriented research, proof of concept, pilot deployment of secure ICT products/processes in general and specifically for addressing National Security requirements
•to improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products
•to create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training
•to provide fiscal benefits to businesses for adoption of standard security practices and processes
•to enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen’s data and for reducing economic losses due to cyber crime or data theft
•to enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention
•to create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy
•to develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace
•to enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace

Strategies
•Creating a secure cyber ecosystem
•Creating an assurance framework
•Encouraging open standards
•Strengthening the regulatory framework
•Creating mechanisms for security threat early warning, vulnerability management and response to security threats
•Securing E-governance services
•Protection and resilience of critical information infrastructure
•Promotion of Research & Development in cyber security
•Reducing supply chain risks
•Human Resource Development
•Creating cyber security awareness
•Developing effective Public Private partnerships
•Information sharing and cooperation
•Prioritized approach for implementation
•Operationalisation of the policy

Congratulations!!!

Dr. G. Satheesh Reddy, Hon. Fellow - Computer Society of India, Distinguished Scientist & Director, Research Centre Imarat, DRDO has been conferred with the prestigious Fellowship of the Royal Institute of Navigation for his significant contributions in the fields of inertial and satellite-based Navigation and avionics technologies. As on date Dr. Satheesh Reddy is the only one to be elected from India for this award.

CSI.congratulates Dr. Reddy on receiving this honor.
Improving Cybersecurity using NIST Framework

Cybersecurity refers to the tools, practices, approaches and safeguards implemented to protect information and information assets in the interconnected cyber world. The internet and the cyberspace have brought immense benefit to the human society. It has brought the world closer and offered opportunities where none existed earlier. New vistas have opened up in multiple sectors including banking, education, travel, e-commerce, entertainment, governance and many more. Distances and geographical limitations when transacting and obtaining services have become redundant by the pervasive nature of the cyber world. This indeed is good news for bona fide users. It is equally good news for individuals or entities involved in dubious, illegal, criminal, anti-national or unethical activities. Inadequately protected information and information technology infrastructure provides immense opportunities for mischief mongers as well as dedicated and hardened criminals, state actors and terrorists. Corporate espionage, spying, financial crimes, identity theft, privacy compromises have become matters of concern from a national, commercial as well as individuals perspective. Organizations like New York Times, Sony Entertainment, Target, Home Depot, Anthem have experienced of advanced cyber-attacks that have been sophisticated, stealthy and caused significant damage. Cyber-attacks are not limited to commercial organizations and national governments too have borne the brunt. In 2007, Estonia experienced cyber-attacks and the Estonian Foreign Minister accused Russia of direct involvement. The Stuxnet episode that severely damaged Iran’s Nuclear Program was an eye opener for the cyber protection of Critical Infrastructure.

A common feature in all these attacks was the remote nature of the attacks. The attackers were nowhere near the scene of the crime and in many cases located across international borders. Majority of these attacks came through the cyberspace that provided them an attack route to the victim. Serious attacks in the cyber space have moved up from the network layer to the application layer. Unpatched systems, outdated software provide avenues to attackers. Sophisticated attacks are known to exploit vulnerabilities that are not yet known in public domain (zero day). The weapons used in cyber-attacks is code. Unlike physical weapons, once created, multiplication of the attack weapon – the code, is simple and does not consume significant amount of resources. Many such attack tools and attack codes are available over the Internet – some for free and others at a price. The interconnected cyberspace hosts valuable information assets and also attackers who are on the prowl. Protection and security is thus an imperative for private enterprises and governments alike. The diversity and complex nature of cyberspace requires that protection and security be driven by wholesome policies, practices and frameworks that address multiple aspects in a cohesive manner.

The Department of Electronics and Information Technology under the Ministry of Communication and Information Technology, Government of India notified the National Cyber Security Policy in July 2013. The Policy is an important document that lays down the objectives, vision, mission and strategies at a high level. In February 2013, the US President issued a Presidential Order on ‘Improving Critical Infrastructure Cybersecurity’. The order called for the development of a voluntary, risk based Cybersecurity Framework. In response to the order, National Institute of Standards and Technology (NIST) developed the – ‘Framework for Improving Critical Infrastructure Cybersecurity’ (referred to in this article as the Framework) in February 2014. The framework is technology neutral hence can be adopted irrespective of the technology implementation. While India’s National Cyber Security Framework sets the high level context to Cybersecurity and the overall approach, the NIST Framework helps organizations in developing an a method for addressing Cybersecurity risk. It can therefore be viewed as complementary to the India’s National Cybersecurity Policy. The Framework is composed of three parts:

1. Framework Core
2. Framework Implementation Tiers
3. Framework Profiles

The Framework core is composed of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Framework Core has defined five Functions—Identify, Protect, Detect, Respond, Recover. The five when viewed sequentially can be come close to a cybersecurity risk management cycle. Each of these five functions includes categories and sub-categories along with references. E.g. the category Anomalies and Events under Detect function includes subcategories:

- A baseline of network operations and expected data flows for users and systems is established and managed
- Detected events are analyzed to understand attack targets and methods
- Event data are aggregated and correlated from multiple sources and sensors
- Impact of events is determined
- Incident alert thresholds are established

For each of the subcategory references to standards and frameworks like ISO27001, Cobit5, NIST SP 800-53 have been provided. The table below provides list of functions and the corresponding categories. Detailed information on all the sub categories within each category and the references can be found in the document. (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf )

The Framework Implementation Tiers helps an organization to view itself in one of the four tiers from Tier 1 - Partial to Tier 4 - Adaptive. These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. An organization may select a Tier profile for itself that seems appropriate to its activities and risk profile. Framework Profile represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. Profiles are useful to identify opportunities for improving cybersecurity. The gap between the “Current” Profile and the “Target” Profile identifies areas for improvement. This helps in prioritization of efforts that should primarily be driven by the organizational risk assessment with reference to cybersecurity.

Frameworks like these provide a great advantage in meeting the cybersecurity challenges. They are non-prescriptive and provide for flexibility in line with the risk profile of the organizations. Frameworks provide a much needed guidance and reference to ensure that basic processes and the building blocks necessary for resilience and recovery are identified. The Framework has identified categories and

CSI Communications | May 2018 | 11
sub-categories that can map to or spawn specific processes. Eg the sub category Event data are aggregated and correlated from multiple sources and sensors requires that organizations define and implement comprehensive processes and capabilities for log/alert definition, generation, collection and correlation. The Framework provides for informational references that can be useful in this regard.

The framework underscores the point that there is no silver bullet against cyberattacks. The capability comes from implementing preventive (Identify, Protect), detective (Detect) and corrective (Respond, Recover) measures against cyber attacks. Processes, controls and technology that ensure that requirements defined by the categories/sub categories are addressed help to build an organization that is secure and resilient from cyber attacks. NIST has thus provided a reference and framework that organizations can adopt to evaluate themselves and build cyber security capability.

References


---

**About the Author**

Sandeep Godbole works as Dy General Manager, Information Security at Syntel. He is a Past President of ISACA Pune Chapter. Sandeep is a speaker at national and international events and conferences. He can be reached at Sandeep_godbole@yahoo.com. The views expressed in the article are his own and do not necessarily reflect those of his employer or anybody else.
Cyber Security: Issues and Challenges

India is marching towards “Digital India” as the world is about to commemorate “World Telecommunications Day” this month. All the citizens of the country need connectivity through digital means. If this dream has to be realized, we need policies, techniques and procedures which address the issues of “Cyber Risks and Security” to guarantee success to these concepts.

Cyber attacks are global, cyber security risks are universal, and these are not the concerns of India alone. Satellites, power grids, thermalpower plants, websites, banks and almost all systems attempting to be digital, are prone to cyber attacks all over the world. As we march to 2020, we are looking at a world of 7 billion people, 50 billion devices connected to internet or 7 devices per capita. As internet device’ use increases, there is increase of security threat, and the need for R&D activities in these areas. The world will feel the shortage in availability of specialists and experts in Cyber Security.

As ICT dependence is growing, so is the opportunities for attackers, providing them increased surface to operate, providing them greater potential to damage and create havoc. Today’s netizens are under increasing stress due to words like “Disrupt”, “Destroy”, “Damage”, “Down”. People are worried. The core issues is “Cyber Security” and “Dependability”.

Today’s attackers/hackers are ahead of time, proactive while the people responsible for ensuring security and reliability, namely systems and R&D personnel are reactive. They think in general after the event to find solutions. Current practice of cyber security and defence is too late to act. The cyber security researcher is often chasing the attacker, trying to find one more innovative solution to combat the attackers move after the damage. This needs to change. We need researchers ahead of attackers, anticipate the moves, create defence mechanisms fighting the vulnerabilities, working towards systems which the hackers can’t hack.

These are immense challenges.

The motivation for attacking is increasing along with their numbers. In spite of increasing R&D activities in “Cyber Security”, the gap between means to check attacks and actual attacks seems to be increasing. The impact after threat is large. The answer lies in renewing efforts on cyber-security activities to assure netizens that the ICT activities are safe and Indians dream of digitization is based on sound system founded on security and reliability.

With over a billion personnel with cloud storage accounts, organizations are providing cloud space free. This is with a risk. The storage is in a domain where there is no freedom. Our data is not stored with us, it is stored elsewhere. Result is application of rules and laws of that country where it is stored. The protection of personal information is a matter of serious concern. We need advancements in technological solutions and ease of their availability without compromising on “Privacy” and “Security”. Technological solutions need to be developed to empower users with full control on their own data as well as to provide technological support to assist in regulating the protection of data.

There has to be a strong international cooperation to implement this. There has to be understanding on issues and challenges of “Cyber Security, Reliability and Availability with Privacy” along with coordination in approach among world community of nations.

The issues and problems needing attention of global community of researchers are:

- Social networks functioning on issues of “Security and Privacy” with emphasis on “Malware Detection”
- The engineering process design and production methodologies need to focus on the product developments where security, privacy are assured in software designs
- Create mechanisms which will provide a framework for improved methods for cyber attacks detection
- better response and sharing of information on prevention of cyber attack
- Create manpower with better qualification/training and skills on cyber security matters through public-private partnerships
- Create mechanisms for protection of personal data in third party domain namely, social networks, cloud providers, outsources during various phases of its life cycle i.e., transmission, processing or storage
- Create new flexible access control technologies which are ethical, less dependent on dynamic identities, using more reliable way of management in a distributed world
- We need better risk mitigation strategies for the whole system through precise, reliable, realistic measurements to help management at all levels from technical to top level with assured levels of security
- Create mechanisms which ensure trust in dynamic environment where identities are protected, anchors of trust exist and those interacting are trustworthy. This is in a transparent domain
- Develop mechanisms for ensuring digital rights and protecting privacy with assured empowerment of user to manage their data and avoid anonymous usage.
- Create protocols for creating increased awareness on issues of security, risks and cyber incidents to form a healthy base for use.

Human values, morals and ethical behaviour stand far above freedom. There seems to be an erosion in these facets and quantum jump in unethical practices, corruption and loss in concept of fellow feeling. This is a cause of serious concerns and calls for redefining these facts and establish new norms particularly in IT-act with regard to freedom of expression, acceptable code of conduct, cyber security and control. The need of the day to create cyber system which while meeting the basic parameters of utility, cost and ease with security must be sustainable. This stems from the following parameters

- Must ensure continuous service with profit and productivity. The system must use resources which are recoverable and recyclable. The system must ensure efficient energy and environmental management.
- The system must ensure creation of suitable human resources which is dynamic, forward looking and is ahead of its time.
- All this must be capped with adequate address to social security, safety and sustainability ensuring freedom of individual and security to society.
- Issues of ethics must weigh heavily along with rights and freedom.

That is the challenge to new age cyber R&D community.
Security, Privacy and Trust in Social Networking Sites

To embrace social networking sites or not, is a dilemma for many online entities today

Today, Social Media\(^8\) is instrumental for rapid communications across the globe. It channels the social interactions using extremely accessible and scalable publishing methods over the Internet. The major objectives of social media include connecting individuals, communities and organizations for exchange of ideas, sharing interests and collaboration. The social media has generated numerous business opportunities\(^2\) for enterprises, aimed at marketing and managing customer relationships. Popular social media tools include social networking sites (e.g., Facebook, LinkedIn, and Twitter), collaborative projects (e.g., Wikipedia), content communities (e.g., YouTube) and blogs (e.g., Blogger). Social media has introduced substantial change in the way people communicate. Further, access to social media is expanding through mobile devices. The blend of location based services, mobile technology and social media facilitates the users to update their current location, share their views on visiting places and use the data to discover a new location or a service.

At the same time, social media has instigated specific concerns related to user’s security and privacy. For example, an ignorant click on a shared link over a social networking site by an employee may prove catastrophic for the entire organization. Similarly, a real time, location update from users on the Social Networking Sites (SNS) may turn out to be a serious threat for their privacy. For these reasons, many individuals as well as organizations are skeptic to endorse them. However, few enterprises chose to design their own social networking sites\(^3\) limited to their employees.

This article aims to discuss various aspects related to social media in general, with an emphasis on Social Networking Sites (also known as Online Social Networks) that are predominant on the Internet. In specific, we identify several advantages of adopting social networking sites and also determine the associated risks; primarily related to security, privacy and trust. We also present various parameters based on which these social networking sites can be evaluated. We conclude this article by suggesting a trade-off between usability, security and privacy aspects of the SNS to reap the best out of them for the individuals, relying parties and the enterprises.

Background

With the proliferation of Web 2.0, SNS has become an integral part of our life. The reason behind the fitment of Web 2.0 for SNS is that many components of Web 2.0 are suitable for the evolution and sustenance of SNS. People use the social networking platform to share their personal and professional data, thereby expediting the flow of information. A prevalent social networking site Facebook has reached one billion active users in October 2012\(^4\). The reason for the skyrocketing popularity of SNS is that they provide a platform for users to share the information, organize events and distribute their photos or videos in a friendly manner.

Today, many enterprises are stepping out of their corporate walls and embracing the social networks\(^6\). In the changing scenario, SNS are not only beneficial for the individuals but also useful for the enterprises. Some employers chose SNS as a first hand tool to vouch for the professional details of an individual during the recruitment phase. Different enterprises recognized this platform as a potential business opportunity since it connects them to their existing customers as well as a large number of new users, for expanding their customer base. SNS offer open communication thereby enhancing information discovery and delivery. Nowadays, individuals prefer to read product reviews of existing customers on the Internet blogs rather than looking at the company’s brochures or advertisements. If a company can quickly resolve a complaint raised by its customer on a social networking site, it can bring customer satisfaction as well as avoid negative publicity from unhappy customers.

Overall, SNS found its application in many areas as shown in Fig. 1. Few of them are listed here –

- **Branding** – Branding refers to the steps taken up by individuals or enterprises to highlight their presence and generate public trust.

- **Digital Marketing** – Enterprises use different marketing techniques to sell their offerings. However, digital marketing through SNS has gained popularity these days. SNS channel opens up new business opportunities, helps in customer identification, acquisition, retention and also simplifies the communication process.

- **Social E-commerce** – SNS aid in the promotion of e-commerce websites. The e-commerce portal owners utilize banners over SNS (as a means of advertisement) which are not limited to one geographical region and reach out to a large number of customers, across the globe.

- **Location Based Social Networking (LBSN)** – The integration of SNS and location-based services, altogether adds a new dimension to the usage of SNS. It creates a unique domain of enquiry to cater user’s needs.
at a new location. Popular LBSN applications such as Foursquare\(^6\) and Gowalla\(^7\) allow users to reveal their whereabouts and find about their friends with the help of their handheld devices. Besides, LBSN is also used for promoting advertisements, tradeshows and offering rewards.

• **Social Gaming** - Few individuals perceive social networking platform as a source of entertainment as well, since it supports sharing anecdotes, jokes and online gaming, facilitating global participation. SNS also empower the people with common interests to connect, share and learn from each other.

**Risks and Challenges**
The massive growth of SNS has brought numerous benefits to online communities, but also generated a large number of security concerns. The SNS operate in public domain. Hence, they also provide a vulnerable platform to be exploited by the attackers. Some of the risks and challenges associated with adoption of SNS are as follows.

**Security Concerns**

- **Identity Misuse** - The impersonation of a legitimate user by an attacker can result in identity misuse. The attacker may capture users’ information and harm them subsequently. Consider an attacker who creates a fake HR representative profile on a social networking site. The attacker posts an attractive job opening and legitimate users may become the victims by sharing their resumes. The attacker may use these resumes to gather victims’ personal information, share it with the third parties or sell to an advertising agency.

  Moreover, adding plenty of personal information in public profiles may also cause significant damage to individuals on SNS. The information revealed on the SNS such as full date of birth, mother’s maiden name and e-mail can allure the attackers since many financial institutes also use this information as a part of user identification. The probability of such attacks can increase further, if the user accepts requests from strangers. There can be potential data leaks through these unknown friends and entities.

- **Malwares, Viruses and Phishing Attacks**
  - Malware and Virus attacks\(^8, 9\) may happen via user posts, tweets and email communications. These attacks are also used by intruders to obtain the user’s credentials and gain access to the network. After gaining access to the network, the attacker may spread spam mails and steal proprietary or confidential data. The attacker may cache or modify the victim’s profile leaving it vulnerable to new attacks.

- **Threats from 3rd party applications**
  - SNS offer the integration with third-party applications. These applications initially seek permission from the user to access personal information present in the user profile. The user clicks on ‘Allow’ button, potentially losing control over the shared data. Some of these applications, serving the intended purpose in the foreground may also download a malware on the user’s machine without their knowledge.

- **Legal Aspects** - The legal risks associated with the use of SNS for an organization can be broadly summarized as follows.
  - Liability due to the breach of organization’s security as an outcome of the attack originated from the SNS.
  - Legal implications as a result of the leakage of third party confidential information due to the use of SNS.
  - Risks associated with attacks against the employees through social networking sites or associated applications.
  - Implications due to posts from employees or outsiders that spread rumours, cause hatred or communal violence.
  - Defamation suits due to posts from employees on SNS that caused reputation loss to third parties.
  - Similarly, SNS may also implicate the individuals. Individuals may face legal charges in the following scenarios.
  - Posting offensive content against a particular entity, community or country.
  - Anti-legal or anti-national activities of individuals using SNS.
  - Leaking confidential information on SNS
  - Invading on someone’s privacy.

**Privacy Concerns**

Privacy, in social networking sites remained a complex problem as the concept of social networking and user privacy are quite opposite to each other. The fact that most of the current SNS do not respect the privacy of the user data, is not because of the technical difficulties but rather a design choice made by the providers of SNS. A list of privacy concerns common among SNS users is as follows.

- **Data Privacy** - Users share their personal and sometimes sensitive information on SNS. This may lead to privacy breaches\(^10\) unless appropriate privacy settings are applied for the user’s profile. Though SNS provide a range of profile privacy settings, most of the users are either unaware of them or find the mechanism as complex. If the user’s profile has the default setting as ‘public’, then all the information in the profile is visible to everyone. This way, everyone can view the personal information, associations, activities, interests and alumni information which may lead to undesirable consequences. Accepting requests from unknown people may also adversely affect user’s privacy. The ‘unknown friend’ may abuse the user’s trust and may try to capture the sensitive information. Besides, users can’t control what others can post about them. This way, privacy of both the user and the associated friends is at stake.

- **Tracking Users** - A recent surge of LBSN has invited serious concerns on users’ privacy. A real time update on users’ location may prove intrusive to the users since the third parties may collect personal information of the roaming users. This way, outsiders probing into the users’ personal information can cause them physical security concerns. Likewise, employers may also use SNS as a tool to keep a check on their employees. For example, the HR agency may attach itself to the employees to keep a track on them and monitor their posts.

- **Identity Federation Challenges** - Identity Federation is the technique used to share identity across multiple domains. Nowadays, many online websites offer users to login using their Facebook account. The primary purpose here is to add convenience to the users so that they need not to create multiple accounts. But this ability presents tough privacy challenges because users do not
have the visibility on how and to what extent their personal information could be shared among third party applications.

**Trust Concerns**

Trust, in social networks, plays a vital role for their adoption and is an active area of research. Due to the high susceptibility of Internet, it is necessary to identify with whom we are communicating or dealing online. However, it is very difficult to identify and establish trust for an individual on SNS as there is hardly any direct contact. Considering two entities A and B, entity A is said to trust entity B when entity B behaves exactly in the same way as entity A expects. This ‘expected’ behavior is often refuted by attackers to exploit the individuals on SNS. Different trust related concerns in SNS are as follows.

- **Online Trust and Reputation Management** - Trust provides a decision support system in SNS. Users often trust their friends, connections and even friend-of-a-friend (FOAF). But attackers use different techniques to abuse user’s trust. For example, the attacker creates fake identity of the legitimate user and exploits the user’s connections. Similarly, a group of individuals may establish certain behavior among each other and provide unfair ratings such as exaggerated recommendations to each other. In some cases, a disgruntled employee may post some adverse comments which could damage the reputation of the employer.

- **Trusting SNS Operators** - Whatever users post or upload content in their profile on SNS, the information is usually available with SNS operators. Therefore, users can’t trust SNS operators in the first place. SNS operators can retain a copy of the account data even if the original account is deleted by the user. Also, if the data available with SNS operators is in an unencrypted form, it means a direct threat to the user.

- **Social Engineering** - The technique to persuade the users to disclose their personal and confidential information such as passwords and employment details is known as Social Engineering. Attackers use such a non-technical means to exploit the user’s trust on SNS. Moreover, Social media platform can be used for Internet bullying which may cause physical and emotional distress to the users.

**Impact on Human Relationships**

With the proliferation of SNS, human communication and relationships have picked up a new facet. Although SNS offer an effective way of socialization, its intensifying addiction is making people not-so-social. People tend to spend their time on these SNS rather than directly interacting with family and friends. Instead of sharing their travel plans with relevant people, individuals tend to post a message on Twitter or on Facebook. Moreover, SNS platform (being an electronic medium) is a poor means for conveying the emotions. This emotional invisibility can further affect the human relationships.

**Evaluation Parameters**

Due to the known risks associated with the use of SNS, it is important to assess SNS before adopting them. The analysis can help in identifying suitable social networking channel for a specific context. Few parameters which can help in this evaluation are as follows -

- Level of Customization of access controls
- Active protection of information related to user
- Controlling Customized search options
- User-friendliness in configuring privacy settings
- Explicit privacy policy statement from SNS
- Data retention policy for SNS
- Privacy policy for applications on SNS
- Privacy Monitoring for SNS users
- Ownership of the User data
- Tracking options on how user’s information is disseminated
- Reporting mechanisms for spam/abuse
- Trust and Reputation management on SNS.

**Improving Privacy, Security and Trust Management**

SNS operators are custodians for the large volumes of user data available with them. They are responsible for storing, disseminating and processing user data. They should also restrict the use of personal data through transparent methods governed by the security policies and statutory laws. Two popular privacy management principles that can be used to enhance privacy aspects in SNS are data minimization and the data protection. Data minimization principle restricts the data collection to what is directly relevant and necessary to accomplish a specified purpose. The data should be used for purpose it was collected and preserved for a specified period only. Data protection principle aims to protect the rights and choices of individuals with respect to the processing of personal data by providing guidelines to process the data. SNS should consider personal data protection as significant and allow users to choose or device appropriate privacy settings. In fact, the default settings of SNS should provide adequate security and privacy for user data. SNS shall provide an interface for users to correct errors in data or posts relevant to them. FaceCloak is an architecture proposed to protect user privacy on a social networking site by shielding a user’s personal information from the SNS and unauthorized users. FaceCloak achieved the goal by providing fake data to the social networking site and by storing the sensitive data in encrypted form on a separate server. Safeguards also attempted to provide a secure architecture for privacy preserving and a trusted online social network using de-centralized approach based on P2P architecture.

Cryptography based techniques can be used to enhance the security of SNS. These techniques include Broadcast encryption, Group key exchange communication protocols like zero knowledge. Broadcast encryption is a technique to deliver the content to a large group of people in encrypted form. It is useful to share updates on SNS with a large number of relevant users or friends in a secure manner. EASIER in presented architecture to support broadcast encryption over the SNS. It offers fine-grained access control on the user’s data by using attribute-based encryption, where user attributes are used as encryption key. In this scheme, it is also possible to remove access from an existing user without issuing new keys to other users or re-encrypting existing cipher texts. This is achieved by creating a proxy that participates in the decryption process and enforces revocation constraints. The SNS itself can act as the proxy, who is minimally trusted and cannot decrypt ciphertexts or provide access to previously revoked users. The
steps used in this scheme are:

- Owner encrypts the data with set of attributes and shares the attribute keys with its contacts.
- To share the data with selective contacts, the owner first sends the encrypted content to the proxy.
- Proxy (using its own key) will convert the encrypted content in such a way that only authorized users will be able to decrypt the content with their set of attributes.
- When revocation happens on a contact or attributes are changed, only proxy has to be updated with the new key. Rest users need not to update their key and also content need not to be re-encrypted.
- At the same time, proxy itself does not have enough attributes to decrypt the content itself.

Group key exchange is particularly useful to establish a session key among the group. Ideally, the key is generated by the entire group and everybody arrives at the same key at the end of the protocol. This removes the problem of sharing the secret key with large number of users. In fact, Broadcast encryption methods can be combined with Group key exchange methods\(^{[20]}\) as well. Further, Privacy preserving data mining techniques\(^{[23]}\) allow computations or processing of data in encrypted form without decrypting it. These techniques allow SNS operators or third parties to run queries and establish relationships for user data, preserving privacy of user data on SNS. Zero knowledge protocol\(^{[18]}\) based methods permit SNS users to prove a statement or confirm the position of confidential data to third parties without revealing the actual information.

The increase in distrust over SNS is primarily due to the presence of multiple avatars of some online users on SNS and sophisticated attacks \(^{[22]}\) happening on SNS to steal personal data. An Identity and Trust management system is crucial for the adoption of SNS. It provides a decision support system for online users who can't check the authenticity physically. Users rely on this system to reinforce their trust in an online entity and transact.

Trust management schemes in SNS are responsible for building and propagating trust. They use Trust Modeling and Trust Metrics to establish trust in online user’s identity. Trust Metric \(^{[22]}\) is a measure to depict how much a particular individual can be trusted by the relying parties in a social network. Trust Modeling is mainly qualitative approach based on certain parameters such as user’s association, activities, social status and popularity. One such case is OST \(^{[23]}\) which tries to address the problems of social trust with a trust model based on social activity and transactions. Digital signatures \(^{[18]}\) using x509 certificates can further enhance trust in online transactions. Code signing of SNS applications can verify the authenticity and integrity of these applications.

Online auction and shopping platform, eBay\(^{[24]}\) Trust and reputation management system is a good example to describe trust building and propagation. It collects a set of facts about the service providers on their portal. In this system, customer provides feedback about the service provider. The collected information about the service provider is aggregated and notified to relying parties as the reputation level of the service provider. Similarly, sellers can also rate the buyers. Few social networking sites use similar system and allow endorsement for a user (or skillset) from the rest of the SNS users.

**Role of Stakeholders**

A realistic approach for adopting SNS shall maximize the benefits of SNS while keeping risks at a possible minimum. This needs a combined effort from Users, Organizations and SNS operators as well.

- **Users** should protect their accounts by strong passwords, using appropriate privacy settings and secure connection (HTTPS) to log-on to the SNS. They should be aware of the security implications of their actions on SNS while sharing their information prudently.

- **Organizations** may implement a multi-layered approach to tackle the security threats such as using firewalls and monitoring user activity. The security policies and user guidelines should be in place to mitigate the threats from SNS for their organization. The employees should also be educated to avoid social engineering attacks. Additional security measures include the deployment of anti-virus software and intrusion prevention systems to counter the threats originated from SNS.

- **SNS Operators** should apply security patches as soon as a threat is reported and also take preventive measures to avert them. They should tailor their product to meet the competitive online environment and minimize security risks. SNS shall allow users to choose their security settings, respect confidentiality and privacy of user data. They also should respect the legal framework of the countries they operate and cooperate with law enforcement agencies.

**Future Directions**

SNS is a rapidly expanding segment in Information Technology. W3C organized a workshop\(^{[25]}\) to discuss the current challenges in SNS to allow a healthy expansion of it in future. The key listing is as follows.

- Distributed social networking, to maximize the benefits for the users by using interoperable formats and protocols.
- Preservation of privacy by following the best practices, both for the user and the provider.
- Exploring context in the social networking industry.
- Address the disparity between current implementations of SNS and the devices or capabilities of all users of the Web.

The outcome of W3 workshop combined with efforts from governments, global researchers, International organizations and SNS operators can make SNS a better and safer medium to interact.

**Conclusion**

In this work, we illustrated the potential of social networking sites and determined the associated risks. We also presented various parameters based on which social networking sites can be evaluated. However, combating the security challenges posed by social networking sites need a united effort from the Users, Organizations and the SNS operators. Users should protect their personal information prudently to avoid any identity misuse or theft. Organizations and SNS operators should create a balance by enforcing adequate security measures to reap the best results. Despite of the inherent risks, social media possibly will remain as a powerful communications channel, acting as a dynamic source for information, talent and customers.

**Disclaimer**

All the logos, product names and trademarks are owned by the respective owners and the authors have no intention to use them...
in anybody’s favor. Without any prejudice, the authors presented their views and understanding of various technologies. The views presented in this paper are authors’ personal and need not represent the opinion of their parent organization.

References
Comparative Evidence of Cryptographic Based Algorithms under the Cloud Computing Environment to Ensure Data/System Security

Abstract - Cryptography is considered as the strongest tool for controlling against multiple security threats. Information and data security is the primary concern for Cloud computing users. The data of all the customers are stored on the cloud. Therefore, CSP is responsible for providing security measures to secure data by including use of cryptography and encryption algorithms to achieve data/system goals like Confidentiality, Integrity, Availability, Authenticity, Accountability and Non Repudiation. This paper aims to identify, analyze and report the evidence published in the literature (In major journals and conference proceedings) of different cryptographic security algorithms.

Introduction
Cloud Computing is an emerging technology which provides on-demand resources over the Network. Cloud users can access resources and services anytime and anywhere as per requirement. The resources can be in the form of storage, software applications, servers, network, etc. The customers have to pay just for the services availed by them i.e. according to pay-per-use utility model. An Organization providing Cloud Computing services is known as Cloud Service Provider (CSP). Cloud services have to be reliable and scalable to provide ubiquitous network access and dynamic resource allocation to the clients.

The nature and Quality of Service (QoS) expected by the customer and other details are specified in a negotiation agreement known as Service Level Agreement (SLA). CSP is responsible for meeting various QoS parameters of clients as per agreed and mentioned in their respective SLAs.

Benefits of Cloud Computing
As per NIST, Cloud Computing provides several benefits to the organizations. They are:

- On-demand resources: A customer can avail resources from the cloud as per requirement.
- Ubiquitous network: Resources can be accessed via a network using any device (mobile, laptop, tablet, PC) having Internet connection on it.
- Multi-tenancy: Cloud Computing allows several users to share resources from the resource pool provided by the CSP.
- Elasticity: This provides flexibility of allocation and de-allocation of resources as the requirements expand and shrink of the organization.
- Measured Services: Cloud Computing applies pay-per-use model. This requires keeping track of usage of services or resources by the user and thus maintaining transparency between both the CSP and the cloud user.

Cloud Business Models
Cloud computing also offers various business models for the customer to choose from:

- Software as a Service (SaaS): Allows access to an application and its data center without the need to install it. The application can be accessed via a network.
- Platform as a Service (PaaS): Provides the platform to the software developers of the organization to build their own software applications. The platform includes operating system, database server, and programming language execution environment.
- Infrastructure as a Service (IaaS): Provides the complete infrastructural resources such as Servers, network, software applications and virtual networks.

Cloud Deployment Models
Cloud Computing gives the users capability to choose amongst various deployment models:

- Public Cloud: The resources are provided by the CSP publicly on the Internet. This raises concerns for data security as the malicious users can try to access it.
- Private Cloud: The enterprises can have their dedicated cloud infrastructure. This provides data security to the cloud users.
- Hybrid Cloud: Such clouds are a combination of the private and public cloud. Sensitive information is placed on the private cloud and rest on public cloud.
- Community Cloud: Organizations with common interest or motive like policy considerations or security requirements forms the community cloud.

Cloud Security Issues
Despite of various benefits and services provided by Cloud Computing, there are several security issues related to it:

- Data security: CSP are responsible for securing data of the customers. The security threats can be due to data leakage, attacks by customers, lack of CSP security, etc.
- Physical security: Physical data centers can be attacked by intruders (malicious internal employees and external people). Natural disasters like floods, fire and theft can also damage data centers.
- Malicious Insider: Data can be misused by the employees of the organization who have authorized access to the data.
- Account Hijack: By stealing the username and password of the account, the intruders can misuse the sensitive data of the cloud user.
- Denial of service: The resources can be used by the attacker such that only few are left for the cloud user, making the system slow. Such kind of attack is termed...
Cloud Security Measures

Cloud Computing is widely accepted by several organizations all over the world. Thus, there is a need to take various security measures to maintain data security in the cloud. Few of them are listed here [5, 3, 7]:

• Choose the best CSP after the careful due-diligence.
• Transmission of data should be from a secure channel.
• Regular auditing of the security policies should be done.
• Data privacy should be maintained by authorizing access.
• Regular training programs should be developed to keep the skills of the CSP security team updated.
• CSP must follow the updated policies, standards and guidelines. Also, they should be regularly reviewed.
• Data encryption techniques should be used before data enters into the cloud.
• Trust should be maintained between CSP and the cloud user by applying several security policies and process control techniques.
• CSP should make provisions for the regular back-up of data and recovery in case of server/system failure.

Cryptography

Information and data security is the primary concern for Cloud computing users. The data of all the customers are stored on the cloud. Therefore, CSP is responsible for providing security measures to secure data including use of cryptography and encryption algorithms [3].

Security Goals

There are some specific security goals that must be achieved to ensure secrecy of the data/system [24]. These goals are:

Confidentiality: It states that the data must be accessible to authorized persons only, thus, maintaining the privacy and secrecy of the data.

Integrity: It ensures that the data must be transmitted over the secure channel without unauthorized modification or the loss/destruction of data/information.

Availability: It assures that the data and information is timely available for use. The services are not denied to the authorized users.

Some additional goals are:

• Authenticity: Authentication means verifying that the user accessing the data is genuine. The identity of the sender and receiver of the information must be verified.
• Accountability: It helps to trace the responsible party/entity in case of any security breach. The actions of all the entities must be maintained for security purposes.
• Non-Repudiation: This prevents denial by one of the entities (sender or receiver) in the communication of having less or no participation.

Cryptography means secret or hidden writing. It is considered as the strongest tool for controlling against multiple security threats. For example, Sender, S, wants to send a message, M, to a recipient, R, through a transmission medium. Thus, S will encode/encipher or encrypt the message and transmit it to R. At the receiving end, the encrypted message will be decoded/deciphered or decrypted to obtain the original message [23].

The process of encrypting the message is known as Encryption. The process of decrypting the encrypted message is known as Decryption. The original message is termed as plain text, P. And the encrypted message is known as Cipher text, C.

Therefore, \( C = E(P) \), \( E \) is the encryption rule.
\[ P = D(C), \] \( D \) is the decryption rule. Cryptosystem states \( P = D(E(P)) \).

Processing of plain text: Processing of

Fig. 1: Cryptography Algorithm

Fig. 2: Classification of Cryptographic Algorithms
plain text is done in one of the following ways:

a. **Block Cipher**: Processes n-bit block at a time and produces n-bit output block.

b. **Stream Cipher**: Each bit is processed at a time to produce single output bit.

### Encryption Algorithms

Based on number of keys used in an algorithm, the encryption algorithms are classified as Symmetric encryption algorithms and Asymmetric encryption algorithms.

#### Asymmetric Encryption

When separate keys are used for encryption (KE) and decryption (KD), it is known as Asymmetric Encryption Algorithm. These keys often come in pairs and called as public key and private key \(^{[22, 10]}\).

\[ P = D (K_D, E (K_E, P)) \]

![Fig. 3: Asymmetric Encryption](image)

#### Symmetric Encryption

If only one key, K, is used in algorithm for encryption and decryption, it is termed as Symmetric Encryption Algorithm. The key is also called as private key or single key.

\[ P = D (K, E (K, P)) \]

![Fig. 4: Symmetric Encryption](image)

### Block Cipher Modes of Operations

Block cipher provides various modes of operation \(^{[17, 22]}\):  

- **Electronic Codebook (ECB) mode**: It is the simplest mode where b-bits of plain text is handled at a time and each block is encrypted using the same key. For every b-bit block, there will be a unique cipher text for a given key.

- **Cipher Block Chaining (CBC) mode**: Encryption is done using the XOR of the current plain text block and the previous cipher text block with the same key. Thus, the blocks are chained together, forming dependency on the previous blocks.

- **Cipher Feedback (CFB) mode**: Helps in converting block cipher into a stream cipher. Here, transmission and transformation of s-bits is done at a time. Initially, a b-bit shift register is taken and set to some initialization vector. This shift register is encrypted with a key and a cipher text of b-bits is produced. The leftmost (most significant) s-bits of plain text are XORed with the s-bits of the current cipher text to produce new s-bits of cipher text.

  The shift register is left shifted s-times and rightmost (least significant) bits are replaced with s-bits of cipher text. This process also forms the chain, making

### Table 1: Comparison of Block Cipher and Stream Cipher

<table>
<thead>
<tr>
<th>Factor</th>
<th>Block Cipher</th>
<th>Stream Cipher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformation Size</td>
<td>Transforms one b-bits block at a time.</td>
<td>Transforms one bit at a time.</td>
</tr>
<tr>
<td>Diffusion</td>
<td>High: Information of cipher text depends on various plain text letters</td>
<td>Low: As each symbol is transformed at a time, information of cipher text symbol depends only on one plain text symbol only.</td>
</tr>
<tr>
<td>Transformation Speed</td>
<td>Low: Block of several bits have to transform at a time, therefore, all bits of the block must be received before the encryption begins.</td>
<td>High: Only one character is transformed at a time; therefore, encryption begins as a single character is read.</td>
</tr>
<tr>
<td>Error propagation</td>
<td>High: An error will affect the entire block during transformation.</td>
<td>Low: An error during transformation will affect only that symbol.</td>
</tr>
<tr>
<td>Malicious insertions</td>
<td>Less susceptible: Full block is transformed, so any insertion makes the block size incorrect and reveals the error.</td>
<td>More Susceptible: As only one symbol is transformed, malicious intruder can insert other characters that may look authentic.</td>
</tr>
</tbody>
</table>

![Fig. 5: Block cipher](image)

![Fig. 6: Stream cipher](image)
each cipher text block dependant on the plain text and previous cipher text.

Counter (CTR) mode: The interest in the counter mode has increased recently. A counter with b-bits is initialized to some value and encrypted using a key to produce cipher text. This cipher text is XORed with the plain text to produce to final cipher text. The counter is incremented by 1 for the next block. There is no dependency and chaining among various cipher text.

Output Feedback (OFB) mode: This is quite similar to CFB mode, except that the encryption algorithm accepts the cipher text of the previous encryption, instead of the final cipher text. After the initial encryption of the shift register, the cipher text produced is again transferred to the shift register for next block and the same is also used in XOR with the s-bit plain text to produce the final cipher text.

Comparison of Various Encryption Algorithms
Encryption algorithms are classified under numerous categories described above. Comparisons of cryptographic algorithms based on that classification is given below.

Block Cipher Algorithms
A comparative study of the several block

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Designers</th>
<th>Founded Year</th>
<th>Key Size</th>
<th>Data Size</th>
<th>Transformation Rounds</th>
<th>Keys Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES (Data Encryption Standard)</td>
<td>IBM and submitted to NIST</td>
<td>Jan 1977</td>
<td>56 bits</td>
<td>Block of 64 bits</td>
<td>16 rounds</td>
<td>Single key</td>
</tr>
<tr>
<td>TDES (Triple Data Encryption Standard)</td>
<td>NIST</td>
<td>1998</td>
<td>3 keys of 56 bits each</td>
<td>Block of 64 bits</td>
<td>16 * 3 = 48 rounds</td>
<td>Three Keys</td>
</tr>
<tr>
<td>Blowfish</td>
<td>Bruce Schneier</td>
<td>1993</td>
<td>Vary from 32 to 448 bits</td>
<td>Block of 64 bits</td>
<td>16</td>
<td>Single key</td>
</tr>
<tr>
<td>Camellia</td>
<td>Mitsubishi, NTT</td>
<td>2000</td>
<td>128/192/256 bits</td>
<td>128 bits</td>
<td>18/24</td>
<td>Single key</td>
</tr>
<tr>
<td>Clefish</td>
<td>Sony</td>
<td>2007</td>
<td>128/192/256 bits</td>
<td>128 bits</td>
<td>18/22/26</td>
<td>Single key</td>
</tr>
<tr>
<td>Threefish</td>
<td>Bruce Schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihr Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker</td>
<td>2008</td>
<td>256/512/1024 bits</td>
<td>256/512/1024 bits</td>
<td>72/80 (for 1024 bits)</td>
<td>Single key</td>
</tr>
</tbody>
</table>

Table 2: Comparison of Block Cipher Algorithms
cipher encryption algorithms AES, DES, TDES, Blowfish, etc. is given in the table. The factors presented are designers, founded year, key size, data size, transformation rounds and key used [8, 9, 10, 11, 12, 16, 18].

Stream Cipher Algorithms
Comparison between various stream ciphers algorithms like RC4 and Rabbit is as follows [18, 19]:

Asymmetric Encryption Algorithms
Public key Algorithms such as RSA, Rabbit, etc. are compared in the following table [18, 20]:

Key Management
Cryptography is considered as the key technology to make data secure in the cloud. This requires continuous efforts to

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Designer(s)</th>
<th>Founded Year</th>
<th>Key Size</th>
<th>Initial Vector</th>
<th>Block Size</th>
<th>Transformation Rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>RC4 (Rivest Cipher 4)</td>
<td>Ronal L. Rivest</td>
<td>1987</td>
<td>Vary from 40 to 2048 bits</td>
<td>-</td>
<td>256 bits</td>
<td>1</td>
</tr>
<tr>
<td>Rabbit</td>
<td>Martin Boesgaard, Mette Vesterager, Thomas Pedersen, Jesper Christiansen and Ove Scavenius</td>
<td>Feb 2003</td>
<td>128 bits</td>
<td>64 bits</td>
<td>512 bits</td>
<td>-</td>
</tr>
<tr>
<td>VEST (Very Efficient Substitution Transformation)</td>
<td>Sean O’Neil, Benjamin Gittinsand Howard Landman</td>
<td>June 2005</td>
<td>80–256 bits</td>
<td>80–256 bits</td>
<td>256 - 800</td>
<td>-</td>
</tr>
<tr>
<td>Spritz</td>
<td>Ronald L. Rivest, Jacob C. N. Schuld</td>
<td>2014</td>
<td>256</td>
<td>-</td>
<td>896</td>
<td>1</td>
</tr>
<tr>
<td>Salsa 20</td>
<td>Daniel J. Bernstein</td>
<td>Mar 2005</td>
<td>256</td>
<td>64-bit Nonce and 64-bit stream position</td>
<td>512</td>
<td>20</td>
</tr>
<tr>
<td>Achterbahn</td>
<td>Berndt Gammel, Rainer Götffert and Oliver Kniffler</td>
<td>2006</td>
<td>80/128</td>
<td>80/128</td>
<td>297/351</td>
<td>-</td>
</tr>
<tr>
<td>Chacha</td>
<td>D. J. Bernstein</td>
<td>2008</td>
<td>256</td>
<td>64-bit Nonce and 64-bit stream position</td>
<td>8/12/20</td>
<td>8/12/20</td>
</tr>
</tbody>
</table>

Table 3: Comparison of Stream Cipher Algorithms

<table>
<thead>
<tr>
<th>Factor</th>
<th>Designer(s)</th>
<th>Founded Year</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Factoring large numbers</td>
</tr>
<tr>
<td>Diffie-Hellman Key Exchange</td>
<td>Whitfield Diffie and Martin Hellman</td>
<td>1976</td>
<td>• Discrete logarithm problems</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Provides perfect security in Transport Layer</td>
</tr>
<tr>
<td>Ceilidh</td>
<td>Alice Silverberg and Karl Rubin</td>
<td>2003</td>
<td>• Discrete logarithm problem in algebraic torus</td>
</tr>
<tr>
<td>ElGamal Encryption System</td>
<td>Taher Elgamal</td>
<td>1985</td>
<td>• Discrete logarithm problem in cyclic groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Hybrid cryptosystems</td>
</tr>
<tr>
<td>DSA (Digital Signature Algorithm)</td>
<td>David W. Kravitz</td>
<td>1991</td>
<td>• Digital Signature Standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Uses two hash functions</td>
</tr>
</tbody>
</table>

Table 4: Comparison of Asymmetric Encryption Algorithms
generate keys, encrypt data and transmit over the network. This also involves overheads associated with it\textsuperscript{[3, 13]}:

a. **Transformation Speed:** Encryption involves converting plain text to cipher text which causes delay in time.

b. **Power Consumption:** Processors consume more power in generating keys and encrypting the plain text.

c. **Less Bandwidth:** Limited bandwidth is used by the clients as additional bits of the keys are also present.

Cloud Computing services are used by several organizations and users all over the world. Data security is the primary goal of CSP and the user. Keys used in the cryptography needs to be secret for each and every user. Therefore, number of keys, their length, generation and transportation are to be considered for the data security.

Longer key length and data size requires more power consumption, generating more heat. Also more computation time is required to encrypt and decrypt the data. Whereas, short key length and short data sizes are insecure and can be attacked by the intruder.

Therefore, CSP should make provisions to provide security in generation, assignment, storage, replacement and use of keys.

### Hash Functions

Hash function helps to maintain integrity of the data. It provides a seal/shield to the data before transmission. If the seal is found to be broken at the receiving end, it will state that something has been changed in the file. Hash function can be a checksum, index data in hash table, etc. They are used in Message Authentication Codes (MAC), Digital Signatures and many information security applications\textsuperscript{[22]}.

There are many hash functions available such as Message Digest (MD) and Secure Hash Algorithms (SHA). Various versions of hash functions have been published like MD-2, MD-4, MD-5, SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. Comparison between the hash functions are summarized in the table\textsuperscript{[18, 21]}.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Founded Year</th>
<th>Designer(s)</th>
<th>Message Digest Size</th>
<th>Block Size</th>
<th>Word Size</th>
<th>Transformation Rounds</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD-2</td>
<td>1989</td>
<td>Ronal Rivest</td>
<td>128</td>
<td>128</td>
<td>32</td>
<td>864</td>
<td>64</td>
</tr>
<tr>
<td>MD-4</td>
<td>1990</td>
<td></td>
<td>128</td>
<td>512</td>
<td>32</td>
<td>48</td>
<td>64</td>
</tr>
<tr>
<td>MD-5</td>
<td>1992</td>
<td></td>
<td>128</td>
<td>512</td>
<td>32</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>MD-6</td>
<td>2008</td>
<td></td>
<td>160/224/256/384/512</td>
<td>512</td>
<td>64/32/8</td>
<td>80/96/104/136/168</td>
<td>80/112/128/192/256</td>
</tr>
<tr>
<td>SHA-1</td>
<td>1995</td>
<td>National Institute of Standards and Technology</td>
<td>160</td>
<td>512</td>
<td>32</td>
<td>80</td>
<td>80</td>
</tr>
<tr>
<td>SHA-224</td>
<td>2004</td>
<td></td>
<td>224</td>
<td>512</td>
<td>32</td>
<td>64</td>
<td>112</td>
</tr>
<tr>
<td>SHA-256</td>
<td>2002</td>
<td></td>
<td>256</td>
<td>512</td>
<td>32</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td>SHA-384</td>
<td>2002</td>
<td></td>
<td>384</td>
<td>512</td>
<td>80</td>
<td>80</td>
<td>192</td>
</tr>
<tr>
<td>SHA-512</td>
<td>2002</td>
<td></td>
<td>512</td>
<td>512</td>
<td>80</td>
<td>80</td>
<td>256</td>
</tr>
<tr>
<td>SHA-3</td>
<td>2008</td>
<td>Vincent Rijmen, Paulo Barreto</td>
<td>224/256/384/512</td>
<td>1152/1088/832/576</td>
<td>64</td>
<td>24</td>
<td>112/128/192/256</td>
</tr>
<tr>
<td>Whirlpool</td>
<td>2000</td>
<td></td>
<td>512</td>
<td>512</td>
<td>8</td>
<td>10</td>
<td>256</td>
</tr>
<tr>
<td>Tiger</td>
<td>1996</td>
<td>Ross Anderson, Eli Biham</td>
<td>128/192/160</td>
<td>512</td>
<td>64</td>
<td>24</td>
<td>192</td>
</tr>
</tbody>
</table>

Table 5: Comparison of Various Hash Functions

Insipite of several benefits, major concern faced by the users is of security. To provide adequate data security, cryptography can be implemented. Cryptography is a technology having different encryption algorithms under different categories. User can choose the best one according to their requirements. We have studied and compared several cryptographic based security algorithms on certain characteristics. Though only few characteristics were examined, there are significant other characteristics which can help us in understanding the true potential, strengths and limitations of the cryptographic security algorithms from the perspective of the cloud computing technology.

### References


as the 5th utility” (2009).


Privacy Security Settings – Challenges of Social Media

Abstract: With social media proliferated affecting our day to day life, our digital dependency level is increasing at a fast pace. In the rush to be live in the connected world, users forget the control over the privacy of the information published. This article hints at some of the Facebook threats and precautions that would help to avoid becoming victim of cyber crime.

Can we think of a day without checking our messages on Whatsapp? Updating our status or reading what is new happening in the life of our family and friends through this medium? Social media today has integrated technology, content, social interaction and revolutionised the way humans communicate. This participatory medium has found a new way of sharing and extracting information. This has become a new community space to interact with friends and relatives. Social life has migrated to online communities. This platform has got into the social space helping people to get connected, stay in touch, reconnect with old friends and also it has permitted creation of new friendships. With more and more people joining the bandwagon, the strong presence of social media has created a new community culture. Social media has also democratized the tools of self expression. These technologies have grown in leaps and bounds during the last few years. Twitter, Facebook and other social networks are used to share information, but the smartphone has become responsible for revolutionising how the information is collected and distributed to the masses. Smartphone penetration which made devices affordable and the wireless networks more ubiquitous and faster can be attributed as the most influential factor for this change.

Facebook has become part of life, influencing our day to day activities and decision making. The size and reach of Facebook speaks about the acceptability and adoption rate. The Facebook Newsroom confirms that there are 1.44 billion monthly active users as of March 31, 2015 and 936 million daily active users of which 798 million are mobile daily active users. The value of Facebook lies in these numbers and database of information they hold. The social media technologies like blogs, wikis, twitter, Facebook are increasingly used by different organisations to improve visibility and knowledge sharing with customers and public. Messages on social media can reach massive audience organically without any financial commitments for organisation. Social networking sites facilitate collaborating, sharing that allow individuals to construct a public or profile. The type of social media that is the most used in India are sites like Facebook, Twitter and Whatsapp. Being top in user base, this article primarily focus on Facebook.

Though they have become a part of the rhythm of our daily life, have we stopped and wondered about the privacy issues therein? When posting information to a social network, a user probably expects authorized contacts to be able to view it. Little are the users aware of the potential risks of wilfully disclosing their own information to public domain. This is relevant market information gathered for organizations who are seeking to secure a place in both the traditional and digital marketplace. European Commission’s project on Privacy Challenges in Social Media is an ongoing project exploring privacy issues associated with social media at the level of the individual, the enterprise and society. It aims at generating effective solutions, from providing users with technical safeguards and informed consent, to establishing corporate guidelines for protecting privacy, to developing and testing recommendations for public policy.

The reach and impact of this digital media is visible in India also. Social media is promoting a lot of discussions on critical or sensitive issues like politics, corruption, poverty and economy including the latest debate on “Net neutrality”. India which is conventionally an orthodox society, has utilised the advantage of social media in 2014 elections. We saw candidates and parties increasingly engaging over Facebook, twitter and similar like forums like never before. Political parties started understanding the new way of reaching out to people without any geographical differentiation of urban and rural. This trend is only expected to increase over the coming years.

This volume of users and the information that gets posted on social media sites has opened a new avenue for people with wrong intentions to use social engineering methods to gain access to the accounts of individuals. The more the information is posted, the more the security and privacy of the individual is at risk. Criminals are increasingly using this platform to get connected to potential victims. The networked nature of social media makes available a substantial amount of information about any single individual. This indiscriminately posted information gets collected and analysed by marketers, identity thieves, and state actors. Security professionals have to look beyond defending its network and infrastructure. Social media is a growing challenge posing new risks for organisations in the new ecosystem of interconnected world.

Facebook acquired and created various new apps over the past years. Facebook with acquisition of popular Whatsapp and Instagram became a multidisciplinary online conglomerate built on the massive success of Facebook.com. WhatsApp focused on instant communication without any frills became hit among common masses. The combination of WhatsApp and Facebook will allow us to connect many more people round the world,” according to Marc Zuckerberg, CEO. WhatsApp is actually the world’s most popular messaging with 27 billion messages sent each day.

Though Facebook has active security monitoring with the site actively scanning for malware and offering security options, there has been increased reports of malware attacks through this site. Just like spams affecting email, on social media, scammers and spammers always find a place to creep in. Many third party applications, which interact with users, becomes a breeding ground for these kind of unexpected behaviours. With
such a large userbase, Facebook is a target for scams; it can also expose your personal information far beyond your group of friends, if the user is not careful.

It would be instructive to look at some of the examples of attacks[4],[5] on the social media sites we usually use-

1. **LikeJacking Attacks**: This is a click jacking attack, where the Trojan in web pages forces users to “like,” “share” or “comment” on pages in Facebook without their knowledge. Users are tricked and driven into clicking a link which does something totally different from user’s expectations. When the user clicks a malicious link, a malware is planted onto the system. This drive includes some key words like “Breaking News”, Latest news, Exclusive content etc. which attract the user attention. The attack is planned as the Facebook user is tagged in a post made by a friend. Clicking the link leads to an external webpage that appears to offer the said video, which is in fact a malware-ridden website. The tagging property of Facebook users in the spammy links helps the scam to propagate further and more quickly.

2. **Phishing attacks**: This is the most popular technique for accessing sensitive information. Fake web pages masquerading as legitimate ones force users to key in their credentials. Without realising that, users key in the credentials and is into serious trouble. Kaspersky Lab’s statistics reveal that fake sites imitating Facebook accounted for nearly 22% of phishing attacks in 2014. A typical example of this attack was an app that boasted it could enable users to ‘guess who viewed your profile’. This app promised Facebook users the ability to see who viewed their profile, which installed malware to spy on their web browsing. When clicked, the site spoofed the appearance of Facebook’s login page and offered two options to activate the fake app. The first option asked users to enter their credentials into the fake website while the second option asked users to download and install software in order to receive notifications when someone viewed their profile. A malware that set up a keylogger on the victim’s computer is installed and sends the logged data to phishers as soon as an Internet connection was detected.

Another badly affected one was a link promising naked videos of their friends. Mostly these phishing messages are sent within the social network from compromised accounts registered by the friends of the potential victim. A short personal message containing a question like “Is that you in this photo?” and a link to the “photo”. Users are prompted to click the link which points to a fake Facebook login page that contains the standard message “Log in to continue”. If users are not careful and enter their credentials, guess the aftermath!

3. **Malwares**: Malware describes a wide range of malicious programs installed on a user’s computer without their explicit consent. This spread quickly on a social network, infecting the computer of a user and then spreading to his or her contacts. Since it appears to come from a trusted contact, users are more likely to fall prey to it. In some cases, these malwares can impersonate users and misuse their account. Also the attackers install some form of adware on your computer which bombards the machine with endless pop-up ads.

    a. Zeus – a Trojan that was spread by clicking the links. This malware scanned all personal files, stole personal information. It was able to collect login details through key logins. This Trojan was specialised in stealing bank credentials of the user.

    b. Koobface –In 2009, it exclusively struck social networking sites. A message from friend with a sentence “you look funny in this video” with a link to watch, is the start. If opened, the link would take you to YouTube or another trustworthy website which seemed to have a legitimate video hosted as the name of your Facebook friend as stated in the website. Once in the video site, a message says an update of flash is needed for video display. If you click “install”, the system was compromised. This bot could install malicious apps at a later stage too.

    c. “LOL” Virus – The “Lol” virus spreads through Facebook’s chat function. Users receive a message from one of their friends, simply stating “lol” and with an attachment. Curious, they click the attachment which triggers the download of a Java file containing malware from Dropbox. The virus infects the computer and hijacks your Facebook account and spreads itself to your network of friends.

Facebook in its Facebook Privacy Basics[6], discusses a set of tools available to secure their account, to keep your information secure, and the ways to recognize and avoid attempts to compromise the account. This helps the user to control the information the user wishes to share, the persons whom the user wants to share with and also who can share with you. They have divided the privacy basics into four subdivisions:

    a. **What-others-see-about-you/posts?** : This is a priority setting for Facebook users. This helps you to choose who sees your post, who sees the tags or delete the posts you have made. You may hide your friends list from general public also. With the limitation that some of your activity will still be visible, you can deactivate or delete the account. There is also a provision for reactivating a dormant account.

    b. **How Others Interact With You?** : This helps user to manage how other people’s activity affect the user and content. This includes untagging as well as unfriending or blocking someone.

    c. **What-you-see?:** This section is on why user sees the ads popping up. The user has minimal control over this setting. This helps the user to control whose post appears on their newsfeeds.

    d. **How-to-keep-your-account-secure?** This covers the most important aspects a user
should know regarding secure passwords, alerts of logins, any changes made and to make it really secure. A login approval with a code sent to the registered mobile number would appear, when a login is attempted from a computer, phone or browser, the user has not used before. Facebook notifies and asks user approval with a security code. Users should not click or share but report if anything that looks suspicious or sounds too good to be true is found. Phishing attempts should be spotted and alerted.

Attracted by the volumes that Facebook has engendered, there is an increasing number of scams and malicious software spreading through it. The attackers have used social engineering to get people to click on infected links spreading through friends’ news feeds with click-bait headlines. Facebook has been trying its best through the feedback options to blocking and remove links which are found malicious. With the new antivirus service and more user awareness, the social network hopes to reduce the spread of malware. A high level of carelessness on the part of users attracts most of the attacks. Hence, it is the responsibility of the users of Facebook and other social media sites to be vigilant and situationally aware at all times. The official Facebook security team is constantly on the lookout for new exploits and immediately notifies users through the security pages. Millions of people have fallen for Facebook scams. The virus affecting pattern is highly polymorphic. To curb and bring down the attacks to a minimum level, many of the organisations has a security bug bounty program which encourages the user to report any vulnerability discovered on the website by financially compensating for it.

The Digital and Network technologies has taken us from the industrial era to the information era. This information era created cyberspace which is never a secure space. As an interconnected society, we are committed to building this Better Connected World. Social media is here to stay and become more powerful. The organisation need to put in policy of usage and make the employees aware of the policies as the use of social media brings challenges for organisations, because it is a new communication tool that needs to be implemented in the already existing communication goals, strategies and daily activities of the organisation. Be a responsible netizen, extend it to the society and make cyberworld a safe and secure place to digitally coexist.

Acknowledgement
Authors wish to acknowledge the inputs of Ms. Deepika Suri, TCS-Cyber Chevening Fellow- 2014 towards the compilation of this article.

References

About the Authors

Mini Ulanat, Systems Manager of Cochin University of Science & Technology is a senior Life Member CSI and Chapter Patron, CSI Cochin Chapter. She was the National Student Coordinator of CSI for 2013-2015. Ms. Ulanat is the recipient of Chevening TCS Cyber Security fellowship and is undergoing training on Cyber Security and Information Assurance at UK Defence Academy, Cranfield University, UK.

Prof. K Poulase Jacob is the Pro-Vice-Chancellor of Cochin University of Science & Technology. He is senior Life Member CSI and Chapter Patron, CSI Cochin Chapter. He was Professor of Computer Science at Cochin University of Science and Technology since 1994, and Director of the School of Computer Science Studies prior to this. Dr. K Poulase Jacob is an active researcher and has published more than 100 publications in refereed journals, conference proceedings, several edited books. He has given several invited talks at various conferences in Europe, USA, UK, Australia and other countries.

- The word Netizen was coined by Michael Hauben
- Netizen is someone who spends considerable time online
- 5P mantra for Netizens for online security is (a) Precaution (b) Prevention (c) Protection (d) Preservation
- (e) Perseverance
- For cybersafety remember “Stranger is Danger”
- Report every cybercrime, that comes to your knowledge
Importance of Morality, Ethical Practices and Cyber Laws as Prelude to Cybersecurity

The 20th century saw evolving of scientific management methodologies, modern techniques of industrial administration, organization and practices that aimed at attaining higher efficiency, increase in production capacity, enhancing firms’ positioning and greater profitability. The notable developments in the field of communication due to the introduction of devices such as thermionic valves (Thomas Alva Edison) - used in electron microscope, radar, the electronic computer, cathode ray tube of television set; diode (Sir John Ambrose Fleming) - used as rectifier; triode (Lee Dee Forest - 1906) that led to broadcasting of live-voice across Europe and America. The subsequent development in field of electronic engineering created a new world of computer technology, remote controlled devices, shrinking of circuit sizes and instantaneous communication.

Communication is the exchange of meanings between individuals through a common system of symbols. It is difficult to comprehend the entire meaning of the term communication using one single definition. Communication can assume different perspective depending upon varieties of discipline and subjects such as architecture, anthropology, psychology, politics etc.

Cyberspace refers to a notional environment that facilitates communication over computer network. With respect to computing world, the term security needed for safe communication over network gets extended as cybersecurity. It deals with consortium of bodies, evolving technologies, processes and practices aimed at protecting networks, computers, programs and data from attack, damage or unrecognized access i.e., denying access to the unauthorized user with malicious intention.

Moral responsibility, ethical practices and cyber laws are three important guiding parameters that a digital firm needs to look into before deciding and framing policy for cyber security.

Propagating Moral Values and Ethical Practices in Organisations

Moral implies conformity with the generally accepted standards of goodness or rightness or wrongness in conduct or character. Morals are those principles and values that have internalized automatic response to the system. They are part of who we are and our unique personality. We make moral decision without much thought because they are based on the principles and values we believe in most deeply; we learn them from parents, teachers, religions, places, and friends and by our learning experiences. All these lay foundations or framework for our moral actions.[1]

Moral theory is made up of three components:
1. Moral Standards: A criterion (parameter) used to decide what is right or wrong.
2. Moral Principles: Actions or activities categorized as right or wrong.
3. Moral Judgments: Statement/s about the rightness or wrongness of particular actions.

Ethics as a term was first invented and coined by German philosopher Immanuel Kant (1724-1804). It deals with the determination of what’s right or wrong with the action or activity and then doing it the right way. Kantianism is an ethic of duty. According to Kant - Ethics [3]:
- is the basis for life;
- principles are based on moral values;
- generates respect for individuals and therefore the opinion of his/her is considered and preferred in professional matters; and
- aims at creating norms for providing justice to each of the stake holder/s.

Being ethical implies conformity with an elaborated, ideal code of moral principles that is used to describe how people perform, operate, conduct and behave within and outside the organisation. Fig. 1 describes actions that can be classified as Ethical and Unethical[3]:

Importance of Ethical Practices to Secure use of Information Technology in Business

Apart from having sound knowledge in the field of management (activities such as planning, organizing, controlling, forecasting and budgeting) and information technology (tasks such as scheduling, procuring, maintenance, upkeep and repairs of component of IT infrastructure – hardware, software, storages, networks and telecommunication devices); professionals are expected to understand the importance of moral values and ethical practices.

Responsibility of a digital firm is to promote ethical uses of informational technology within and across the organizational boundaries. Natural fallout being impact on employment, privacy, individuality, privacy, health, working conditions and crimes that use of IT has on business and society[1].

For instance, computerizing a manufacturing process may have adverse effect of eliminating people’s jobs but also have the beneficial result of improving working conditions and producing products of higher qualities with a reduced cost. Ethically responsible use of information technology in this case would be to communicate to all the stakeholders...
those bringing in the change and those impacted by it – about detrimental effects of business applications of information technology and the ways it can optimize beneficial effects.

Some of the very ethical issues that creep up especially in a digital firm are(3):

1. Electronic monitoring of employees’ work activities and electronic email.
2. Using work computers (office nodes) for personal and private business activities.
3. Electronic access to employees’ personal records and/or workstation files.
4. Using of company’s software for personal use.
5. Selling of customer information extracted from transaction processing systems to other companies.

Basic grouping of business processes leading to ethical issues are (indicative list):

Rapid changes in information technology have made dramatic changes in the very structure and characteristics of human life making it information driven society. The social and judicial structure of society has improved and matured which in turn provides better standards of human life.

The diversity of IT applications and increased use of technology have resulted in many ethical issues that the organisations across the globe are attempting to resolve. An attempt to identify, organize and classify these issues into a framework was undertaken by Mason in 1986(3). He categorized ethical issues into four groups as exhibited in table 1.

The newer programs such as intelligent agents - the software that assist people and act on their behalf and software robots - are increasingly being used to deal with vast amount of information available on the Internet. This increases the complexity of computer systems and software. Since such agents are frequently used to find or filter information for a user, identify patterns and trends from a very large amount of data (data mining), and act as interactive assistants for computer interfaces. These agents came into existence with the development of the Internet and the World Wide Web (WWW), and will continue to play a very large role on the web. They play an integral role in the function of search engines, e-commerce portals, shopping carts management, bargain determiner and bots (short cuts for software robots)(2).

Task typically associated with computer professionals are analysis, specifications, design, development, implementation, testing and maintenance. Each of these tasks requires certain skill set. Along with the expertise in the task, ethics too is needed to be followed by computer professionals in order to help maintain standards and therefore improve organisations brand image.

As a professional, the responsibilities include:

- Ensuring privacy and secrecy of data,
- Data confidentiality,
- Prevention of data-misuse,
- Promotion of data-integrity (accuracy,

<table>
<thead>
<tr>
<th>Category</th>
<th>Issue pertaining to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>• Collection</td>
</tr>
<tr>
<td></td>
<td>• Storage</td>
</tr>
<tr>
<td></td>
<td>• Revealing of information about individual</td>
</tr>
<tr>
<td>Accuracy</td>
<td>• Authenticity</td>
</tr>
<tr>
<td></td>
<td>• Fidelity</td>
</tr>
<tr>
<td>Property</td>
<td>• Ownership</td>
</tr>
<tr>
<td></td>
<td>• Value of information</td>
</tr>
<tr>
<td>Accessibility</td>
<td>• Right of access to information</td>
</tr>
<tr>
<td></td>
<td>• Payment of fees to access it</td>
</tr>
</tbody>
</table>

Table 1: Grouping of Ethical issues

reliability and completeness),
• Facilitate data-inspection,
• Achieve utmost quality of services,
• Creation of efficient product
• Working Knowledge; understanding of the existing laws.

Code of ethics defines norms and principles to be followed and it is a way of setting standards. These amongst many include fair treatment; privacy; communication; system integrity; cooperative; honesty; education; division of labor; social responsibility; quality and discipline. These guidelines are based on; common sense; decency to protect privacy and ensuring equal access to resources for everyone.

Every organisation is expected to provide ethical guidelines (outlining the policy statement/s) that would:
• Cultivate the respect for privacy of other users
• Educate the users about the importance of not sharing the account and password
• Facilitate the fair use of computer facility
• Reduce (if not eliminate) the unauthorized access of data
• Prevent unethical and illegal use of software
• Promote effective use of communication facilities
• Appropriate clause of applicable laws and copyright protection
• Minimize the misuse of computer resources.

**Cyber (Computer) Crime**
The cyber criminals are the individuals or the group of individuals with intention of taking advantage of the widespread use and vulnerability of computers and the internet and other networks. Cyber crime is becoming one of the Net’s growth businesses[1].

Computer crime as defined by AITP (Association of Information Technology Professionals - https://www.aitp.org/) includes:
• the unauthorized use, access, of hardware/software and network resources;
• the unauthorized release of information;
• the unauthorized copy and piracy of software;
• denying an end user access the resources that lawfully belongs to him or her
• using or conspiring to use IT resources to illegally obtain information or tangible property.

<table>
<thead>
<tr>
<th>Hacking Terms</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of service</td>
<td>This is becoming a common networking prank. By hammering a website’s equipment with too many requests for information, an attacker can effectively clog the system, slowing performance or even crashing the site. This method of overloading computers is sometimes used to cover up an attack.</td>
</tr>
<tr>
<td>Scan</td>
<td>Widespread probes of the Internet to determine types of computer, services, and connections. That way the hackers can take advantage of weaknesses in a particular “make” of computer or software program.</td>
</tr>
<tr>
<td>Sniffer</td>
<td>Programs that covertly search individual packets of data as they pass through the Internet, capturing password or the entire contents.</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Faking an email address or webpage to trick users into passing along critical information like passwords or credit card numbers.</td>
</tr>
<tr>
<td>Trojan Horse</td>
<td>A program that, unknown to the user, contains instructions that exploits a known vulnerability in some software.</td>
</tr>
<tr>
<td>Backdoors</td>
<td>In case the original entry point has been detected, having a few hidden ways back makes reentry easy - and difficult to detect.</td>
</tr>
<tr>
<td>Malicious Applets</td>
<td>Tiny programs, sometimes written in the popular Java computer language, that misuses the computer resources, modifies files on the hard disk, sends fake emails or steals passwords.</td>
</tr>
<tr>
<td>War Dialing</td>
<td>Program that automatically dials thousands of telephone numbers in search of a way in through a modern connection.</td>
</tr>
<tr>
<td>Logic Bombs</td>
<td>An instruction in a computer program that triggers a malicious act.</td>
</tr>
<tr>
<td>Buffer Overflow</td>
<td>A technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer’s memory.</td>
</tr>
<tr>
<td>Password Crackers</td>
<td>Software that can guess passwords.</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>A tactic used to gain access to computer system by talking unsuspecting company employees out of valuable information such as passwords.</td>
</tr>
<tr>
<td>Dumpster Diving</td>
<td>Shifting through a company’s garbage to find information to help break into their computers. Sometimes the information is use to make a stab at social engineering more credible.</td>
</tr>
</tbody>
</table>

Table 2: Common hacking techniques
Schwalbe[4] produces the media snapshot indicating the menace the computer viruses (hacking) have caused across the globe (see table 2) and the anecdote is “What do Melisa, Anna Kournikovo, Code Red, and Sobig have to do with quality and information technology? They are all the names of the recent computer viruses that have cost companies million of dollars. A quality issue faced by computer users around the world is lost productivity due to computer viruses and spam – unsolicited e-mail sent to multiple mailing lists, individuals or newsgroups. Spam currently accounts for more than 70 percent of the total e-mail volume worldwide.”

Information Technology Act of India 2000 (IT Act): Some Preliminary Facts
IT Act 2000 apart from providing legal recognition for transactions (see Table 3) carried out by means of Electronic Data Interchange (EDI) and by electronic communication (referred to as electronic commerce) also:
- encourages paper-less office i.e., involves the use of alternatives to paper-based methods of communication and storage of information,
- facilitate electronic filing of documents with the government agencies.
IT acts covers the following areas:
- E-mail: E-mails could become the basis for launching litigation in a court of law, therefore companies and individuals should be careful while sending e-mails.
- Digital Signature: Digital signature refers to authentication of any electronic record by a subscriber with the help of an electronic method or procedure.
- Electronic records: Electronic records refers to filing of any form or application (on line/or in any other electronic form) in a particular manner with any office or appropriate government department. Table 2.4.4 provides the importance of the attribution, acknowledgement and dispatch of electronic records
- Electronic Gazette: Publication of rules, regulations, order, bye-law notifications, or any other matters published in the electronic gazette. The date of publication shall be deemed to be the date of the gazette which was first published in any form (paper or electronic).

Conclusions
Business ethics are moral principles that define right or wrong behavior in the world of business. What constitutes right or wrong behavior in business is determined by the public interest groups, and business organisations, as well as an individual’s personal morals and values organizations need to deal with the ethical issues of their employees, customers and suppliers. Ethical issues are important because they can damage the image of an organisation. What makes ethics difficult is that what is ethical to one person or in one country may not be so in another. Law indicates the rule and regulations to be obeyed in the organisation. It makes it binding on all the employees to follow it. The fact that an action is legally permissible does not mean that it is morally and ethically permissible. Legal provisions make working for computer professionals, users and society easier.

References
Do You Need an Operating System to Run an Application

Introduction
Our traditional computing platform for running a business application is to have an Operating System (OS) hosted in a set of hardware or computing device supported by a network and other peripheral accessories in a data center. As Information Technology (IT) industry is getting matured more and more in the cloud computing environment, most of the large scale organization or business enterprise has shifted their paradigm of application hosted into cloud platform. Today’s IT scenarios of Cloud computing is broadly categorized as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). However, there are quite a few emerging cloud services came up into the limelight of cloud computing arena and one of them is application containerization.

The most common cloud platform is based on virtualization or a bare metal servers with additional support service wrapping around the virtualization or bare metal to support client’s cloud platform for a cloud consumer. Deploying an application into a cloud platform, the first question comes into the mind is the cloud supported platform i.e. Operating system. Technologists spend significant time to determine the right platform for an application so that it can be supported by a right Operating system into the cloud platform. However, if we think from the enterprise business point of view, operating system is not the business or application service requirement to support its customer. All we need is a mechanism to deploy and manage the application into the cloud platform.

Today’s Operational Challenge
The reason for this is that most Cloud hosting is based on virtualization or bare metal servers. Neither of these technologies run applications, they run Operating Systems. What most of us really want is just a way to make the application up and running. In today’s cloud platform, most of the service provider runs multiple virtualized machines (VM) on a set of hardware that supports industry leading hypervisors which are capable of hosting multiple VMs. Now from business perspective, managing a VM needs large overhead such as computing power, memory, storage, network allocation etc. the most of important part is the management overhead for supporting this peripheral components and their associated support & license costs. However, business needs a deployment space where an application can be hosted. It doesn’t really matter from business perspective whether it needs full-blown OS or a container which is capable supporting the business application without having additional overhead or management cost.

Technology Solution to Support Next Generation Virtualization in Cloud Platform
Today’s advance technology of an Operating System (OS) does support a building block where business doesn’t really need to buy an entire OS platform with stack of middleware loaded in it to deploy or support their business application into the cloud platform. One of the most industry recognized pattern is the Linux X container. It’s based on the container concept where application needs a space which can be self contained within the operating system. In a container model, a service provider can run an OS that hosts containers with applications.

Containers are lightweight virtual machines (VMs) which are realized using features provided by a modern Linux kernel, VMs without the hypervisor.

Application Containerization of:
1. Linux Operating Systems or other similar OS who supports containerization e.g. Solaris, Microsoft Hyper-V features of Windows 2008 and 2012.
2. Single or multiple applications.

So in Linux world, LinuX Containers (LXC) is an operating system level virtualization technique to run multiple isolated Linux systems we call it containers on a single host or Operating system Instance (OSI). It provides a virtual environment that has its own process and network space.

Similar principle of application containerization works in case of Windows OS with Microsoft Hyper-V or Solaris container in case Oracle OS.

So net-net Containers are going to be next generation virtualization in the cloud era. Some of the highlights shown below which are eye catchers for CIOs and CXOs of the business enterprise:

Agility to run in cloud:
- Provision of application space into cloud in seconds / milliseconds
- Application performance is near bare metal runtime which is mostly offered today by the cloud service provided.
- VM-like agility – it’s still “virtualization”
- Flexibility
  - Containerize a “system”
  - Containerize “application(s)”
- Lightweight
  - Just enough Operating System (JeOS), this is applicable more for
Implementing container vendor support, consistent performance license, large ecosystem, wide hardware in the cloud space for lower cost of choice for most of the IT service requester definitely a preferred operating platform the current technology trend, Linux is it operates in a large scale. If we look into get more consistent performance when of them have switched back to VMs to IaaS environment however, some of them into this as a precursor to cloud PaaS or server providers, which may have looked machines (VM) in cloud space. Many provider compared to traditional virtualization for long and Sun Microsystems was one of the concept of container has been around i.e. Solaris Zones. Now virtualization using container concept represents a new interesting alternative to cloud service provider compared to traditional virtual machines (VM) in cloud space. Many server providers, which may have looked into this as a precursor to cloud PaaS or IaaS environment however, some of them of them have switched back to VMs to get more consistent performance when it operates in a large scale. If we look into the current technology trend, Linux is definitely a preferred operating platform choice for most of the IT service requester in the cloud space for lower cost of license, large ecosystem, wide hardware vendor support, consistent performance and reliability. Implementing container features requires to adopt standardization of the client application deployment model into the cloud platform. Let us take a deeper look on the implementation side of the container vs. VM with respect to application deployment.

The above Fig. (B) represents Open Source technology of KVM vs. Linux Container (LxC). Here the key difference is the additional guest OS layer and the management overhead to manage the application and respective database. As long as application or database standard technology platform meets the requirement of the operating platform and its underlying files system (e.g. root volume group, data volume group), service management and network requirement, it can be very well deployed into the container level than managing through guest OS. Usually the VM is very in terms of isolation and separation of duties from the guest's perspective but they add overhead when sharing data between guest VMs or between the guest VM and the hypervisor, for running an application in a cloud computing environment, the VMs generally access storage through emulated block devices that is nothing but an image files. Now for day-to-day management, creating, updating, and deploying such disk images is a time consuming work and many in instances, disk images will have duplicate contents barring application binaries and data. This is also a wastage of storage space which is a costly affair in the cloud operation. So instead of running a full OS on a virtual platform, a container-based virtualization modifies an existing OS to provide an extra isolation level. For example, adding a container ID to every process and adding new access control checks to every system call. So container can be leveraged as additional level of access control in addition to the user and group policy. This way it can provide similar separation of duties and requirement of application while saving the storage space of common file systems for OS which are same across multiple VMs.

Another import aspect of leveraging container concept in the cloud is to standardize the client application and database to run into a homogenous platform than heterogeneous operating environment. The following Fig. (C) shows the demand for standardize environment.

In Hypervisor-based virtualization, we have a flexibility of choosing our own OS e.g. Red hat Linux or Ubuntu or SUSE etc. where as if we go to container or Docker based implementation in the cloud the application or database need to choose a similar operating platform in order to take vantage of Docker or container concept and this type of standardization is anyway welcome for a client organization to reduce the operational cost not only from cloud platform but also for application management and support cost. Docker is nothing but an application container which supports a mechanism for packaging application into a virtual container so that it can be run across different distributions of Linux who support Docker.

As we discussed the implementation view here, it’s good to compare the difference also between container and docker so that client can take an appropriate judgment to choose the right deployment pattern based on their application requirement.

Here Fig. (D) shows that docker is just additional layer abstraction with an available client interface, application programmable interface (API) and set of files to manage the application...
uniformly without getting into too much details of platform details as it would be managed by cloud vendor e.g. IBM BlueMix environment. The key takeaway here is that docker decouples the service provider from the operations so LxC provider agnostic where docker “images” run anywhere docker is supported.

**Conclusion**
CoreOS was announced in 2014 as part of new Linux distribution to minimize the operating platform complexity and simplify the container deployment at a large scale deployment model. So Docker, Linux Container, CoreOS all open source technologies are on the limelight to attract the industry into the container management and simplification of application management environment into cloud platform. So, early-adopters of these technologies will have its own challenges but there is a significant motivation of IT giants to invest their energy to get a quick ROI for companies seeking better agility and lower costs. It may not be applicable for all and complex applications landscape however if 80% of the non-critical applications can be an early adopter of these technology while other 20% critical apps can follow later to maintain a hybrid cloud computing environment. So in summary, with the advancement of technology in containerization and docker, there will be more standardization in system managements and system integration cloud computing environment for monitoring and health check and support mechanism. So cloud customer will have lot less requirement of direct access of OS to manage their application into the cloud like a Software as a Service (SaaS). Most of the IT big players such as Microsoft, Amazon, Google, IBM are keen to play their role in containerization.

**Reference Sites**
[1] https://linuxcontainers.org/

**Figure (D)**

Debasis Roychoudhuri is an IBM Certified Senior Architect and Enterprise Solution Architect of Cloud Modernization in IBM Australia. He has 16 years Industry experience, encompassing roles across the verticals, specializing in application infrastructure design, server consolidation and workload migration from legacy IT environment to various virtualized and cloud environment. He has been instrumental in IBM Global Delivery for developing several cloud computing initiatives such as open source Cloud integration with IBM software, enabling client and business partners in various cloud environment. He is involved in several cloud education initiative in various universities and engineering institutes as part of IBM University Relationship program. He is also Certification Review Board member for Architecture Review Board (India). He is currently supporting large financial and mining organization of Australia as a lead architect, modernization. He can be reached at dchoudhu@in.ibm.com.

Biswajit Mohapatra is an IBM Certified Consultant and Global Integrated Delivery Leader for IBM Application Development and Innovation Digital Modernization Service (DMS) practice. He is IBM India Competency Head for Global Specialized Application Modernization, Application Workload Optimization and Cloud Migration Competency. Biswajit is a known thought leader in Indian IT community for leading Application Modernization and Cloud modernization initiatives from concept to realization. Biswajit leads consulting, solution architecting, offering incubation, technology innovation and delivery of large cloud modernization engagements at IBM. Biswajit is founder member of IBM Faculty of Academy specializing in creating signature client experience, passionate participant of various Industry Academia initiatives around Cloud Computing and has several international journal publications on cloud modernization. He can be reached at biswajit.mohapatra@in.ibm.com.

**About the Authors**
Context Aware Intelligence: Approach for Multi-Dimensional Security

Abstract: In this paper, a novel approach to implementing contextualized security features for enterprise applications is presented. This approach provides adaptability to existing security infrastructure of enterprise applications, thereby enhancing information security. Our framework provides a context engine that uses intelligence to extract and analyze contexts, and identify actions as demanded by the security situation. The viability of the context engine is exemplified by a simple web application featuring security aspects such as authentication, authorization and transactional security.

Introduction
Enterprise security includes the measures taken to ensure security of enterprise applications and sensitive data. Earlier, security was thought of as physical security, and emphasis was on securing physical space and premises that contained enterprise application infrastructure. However, increasing exposure of applications over cloud has resulted in application data being highly vulnerable to a wide variety of threats. The enterprise security space has already gone through one transformation with a shift in focus from parameterized to de-parameterized security solutions that protect the point of access to the data, rather than the physical database and servers. The next wave of transformation will be the use of more than one dimension of the users in order to take security-related decisions. The use of context aware intelligence for security, as described in this paper, is a step in that direction.

Context awareness originated as a term from ubiquitous computing and has been a topic of research since the last few decades\(^1\), \(^2\), \(^3\), \(^4\), \(^5\). However, recent developments in smart mobile devices, ubiquitous presence of sensors, affordable wireless communications, big data technologies and proliferation of social networks enable organizations to leverage technologies related to location tracking, proximity awareness, voice recognition, social media integration and so on, to build context aware intelligent solutions. The contextualization in security will bring in more than one aspect of the user, e.g. access to other information such as user’s location, to take well informed security policy decisions. Also, by leveraging data about what is happening in real-time, enterprises can better prioritize their policy adaptations, remediation activities and attack-response practices.

This paper describes how enterprise applications can implement security features that uses context to take security decisions. We present a conceptual framework for modeling Context Aware Intelligence\(^6\) (CAI). The architecture of our platform, based on this framework, is discussed in the next section. How such a platform can be used to enhance application security is also described through a case study in subsequent sections.

Context Aware Intelligence & Security
Context Aware Intelligence (CAI) framework helps enterprises identify and develop adaptive enterprise applications. The CAI framework is designed to define situations that can be evaluated based on current context any point of time. Due to its highly adaptable design, the framework has wide level of applicability across various domains including enterprise security. The section below explains the key concepts of CAI and how it can be used in implementing security features.

Context Aware Intelligence Framework
Context Aware Intelligence (CAI) framework provides a scalable and flexible solution for integrating information from different sources, and incorporating context awareness within an enterprise application. For simplicity and completeness of context modeling in enterprise applications, CAI classifies contexts into the following four categories:

- **Identity Context** - This category considers data about an entity such as user profile, intent, actions, characteristics, demographics, preferences, interest and history.
- **Location Context** - Location can be described in different ways, depending on the application requirements such as local vs. remote, relative vs. absolute, location point vs. location area, and so on. The two main groups that we have considered are physical vs. geographical. Physical location is related to a global geographic coordinate system and provides an absolute, accurate, grid based position in the form of a \(\langle{\text{latitude, longitude}}\rangle\) pair. Geographical location is used to deal with natural geographic objects, such as countries, cities, and also zip codes, postal addresses and so on.
- **Time Context** - This category deals with information required to handle dynamic environment in the application such as change of situation over time, support for inference on various changes that may take place over a period of time, time zones, time interval and so on.
- **Environment Context** - This category deals with physical objects and devices that exist in an application environment, and participate in data acquisition, reasoning and action.

Conceptual Security Framework
The core security model is not very different from industry norms as shown in Fig. 1. Hence, the core functions of the framework are:

- **Identify** - Identify risk, critical resources and systems performing critical business function. The functions such as identity and content management could be defined by this core function.

![Fig. 1: Security model](www.csi-india.org)
• Detect – Detect any unwanted event that can be a threat to the critical resources and information. The activities such as continuous intrusion and tamper detection, fault handling, etc. are examples of the detect function.

• Act – Take preventive action, sometimes known as countermeasure. Some of the countermeasures that can be implemented under Act function include authentication, access control, message protection, etc.

For the purpose of this paper, we will focus on Act functions of security frameworks. Hence, it is important to have a basic understanding on some of the key countermeasures and their challenges that we can address by contextualization. Some of these countermeasures are covered here:

• Authentication – The most prevalent form of authentication is username and password. Unfortunately, it is also one of the most insecure methods. For example, system asks for a password when a person is trying to login. The person will be allowed to access the application providing the correct password. However, system does not establish that the person who is given access is the genuine user of the application.

• Access Control – Access Control, also known as Authorization – is mediating policy-driven access to resources on the basis of identity. The permissions are mostly implemented using Access Control List (ACL) where access permissions are defined for each user. ACLs are normally static in nature and it becomes difficult to define when we have a large number of resources with varying permissions for each user. E.g., setting permission for too many files in the file system.

• Audit – (a.k.a Accounting), is log statements for the purpose of reporting some key user activities. Most of the time, audit logs are not given its due importance. It has been observed that not much attention is given to identify critical situations reported in an audit log. The audit logs can be a crucial piece of information to identify fraudulent transactions and the user performing it. It could result in big loss if evidences of audit logs are not recorded appropriately. It would be a good idea if we can generate audit situations dynamically based on contextual data so that applications can capture critical information about any critical transaction.

CAI Security Architecture
In order to come up with contextualized security architecture and address some of the challenges described in the above section, we start with the standard and very basic security architecture, which suggests that an entity trying to access an application or data should be controlled by Authentication and Authorization. Audit log should be kept to keep a check on the activities of the entity. In order to build a secure application, we need to implement these three services namely Authentication, Authorization and Audit (AAA) properly.

Context aware security architecture provides a scalable and flexible solution for integrating information from different sources and building dynamic policy driven security services that provide security features such as AAA. For example, consider a situation where a phishing attack is launched with an email containing a link to a targeted attack download. Signature-based mechanisms will not stop this — the organization’s antivirus software will not detect the payload and that the URL is known to be “bad”. However, before the user is allowed to navigate to the site, the secure web gateway performs a look-up of the URL’s reputation (which is a form of context), and navigation will be blocked, preventing the virus attack.

At present, industry analysts such as Gartner recommends that organizations begin the transformation to context-aware and adaptive security infrastructure as they enhance static security infrastructure, such as firewalls, and web security gateway and endpoint protection platforms. The next section provides some insights into how we can use simple contexts and implement basic security functionality such as authentication, access control to prevent threats and fraud transaction.

Case Study – CAI Security in Banking
The use case considered here is to enable a financial services application to detect vulnerable events using various contextual information such as: (a) User details (name, date of birth, username, password), (b) Financial details (account details, account type), (c) Location details (base location, current location), and (d) social details (social network details). This is depicted in Fig. 2 below.

![Fig. 2: CAI Security in Banking](image-url)

**Objective**
The finance application built using CAI security provides simplistic and dynamic security to the financial institutes such as banks, in order to protect sensitive data. It also provides opportunities for reducing security needs of a user depending on intent (type of activities to be performed) and other contextual information such as ...
time and location. The main objective of this sample application is to demonstrate the following aspects of CAI security:

• Easy-to-define situations in a finance application that can be evaluated to detect any threat without referring to static security policy.

• Situations that can consume data from various sources and capture contextual information of the user in order to define application’s security behaviour.

Demonstrate a few security situations in Authentication, Authorization countermeasure using contextual information from different sources.

**Business Scenarios**
The application demonstrates three scenarios where a user is provided with authentication option and data access control depending upon context. The situations that were implemented as a part of this case study are hypothetical in nature and implementation may vary depending on the business needs of financial institutes. The details of the situations implemented are as follows:

• **Personality association using pairing of personalized device(s):**

  Consider the situation where a user can pair his personal device such as mobile or smartwatch, and the business app is installed on that device. Whenever the user tries to access the net banking application, or mobile app or smartwatch app, the availability of paired devices can be used to strengthen the parameters that define authenticity of user. The existence of the person’s registered mobile device that gets paired to the computer from where the net banking application is being accessed strengthens the parameters that define authenticity of the user.

• **Restricted access on multiple attempts in a time period:**

  The situation used the information such as number of access attempts in a duration, local time zone, access channel (web, mobile) and location of access. If there are multiple access attempts made and contextual information is varying drastically then access can be blocked for the security reason. The user will be notified to change credentials on possibility of compromised account.

• **Social network analysis (a):**

  The situation uses social network details of user in order to generate dynamic security questions in order to personalize security parameters. This type of situation can be used to enhance user experience by reducing security overheads on the user to (re) set the answers to these questions. The system can determine what questions to ask and when to ask.

• **Social network analysis (b):**

  The situation uses social network details of user as available. It analyses the social behavior of user and determines any indicator suggesting change of location by the user, which is different from his base country. If there is a request for money withdrawal from any ATM in his base country, security level can be increased to get some more personalized information from the user such as security questions to establish the authenticity of user. The user will be notified on unsuccessful attempts to change credentials on possibility of compromised account.

---

**Fig. 3: Contextualized security solution**
Solution
The context aware security solution is built using Context Aware Intelligence framework that enables us to define situations, by providing the intent and environmental information (context) that can recognize the situation. The environmental information we have considered for these situations are personal details, account details, address details, social details, time related details and social network details. The solution is depicted in Fig. 3.

In this solution, we used the CAI framework to integrate with various data sources such as social network (Facebook), and enterprise data stores in order to extract information such as user details, account details. We are fetching a huge amount of data from social networks and pre-populating them for further analytics like NLP for location detection. CAI framework uses query based data retrieval for the context manager to periodically evaluate contextual data, identify & evaluate impacted situations. The events & notifications generated by CAI framework are used by the sample application to take security decisions. Some implementation details on the situations are as below:

• Personality association using pairing of personal device(s): In this situation, the account details context can be used to keep information about the personal device that will get paired. So, whenever there is an attempt made to access user account from any of the personal devices or using a web channel the password can be used in conjunction with paired devices to ensure the user is the same person by authenticating the person.

• Restricted access on successive attempts in a time period: In this situation, user context stores base location details; time context stores base time zone, time of request, number of occurrences; and location context stores base location and transaction location details. All these contextual information will be validated on successive access attempts made on a user account.

• Social network analysis (a): In this situation, the contexts used are user context, social context to analyze social network behavior of user and identify some personalized questions that can be used as security questions. This should allow systems to be dynamic and present personalized user experience instead of static security questions.

• Social network analysis (b): In this situation, the contexts used are user context, social context to determine status/ post suggesting travel, location context storing base location, and any indicative location, account context for debit/ credit card details.

Implementation Challenges
Using context aware computing for security is an emerging area. The finance industry will need lots of research in this space to establish benefits and value add to the financial business process. One of the main objectives of security is to prevent frauds happening with financial transaction that involves transfer of money. Hence, there are a few challenges that we identified in adopting contextualization for implementing security in financial applications which are as below:

• It is very critical to identify reliable sources of information in order to take security decisions. It is a challenge to use social media as contextual information source due to its perceived lack of security and questionable quality of data.

• Financial transactions are very critical and time sensitive. It will be a huge challenge to ensure real-time performance with different types of contexts used for implementing security features for large number of concurrent users.

• Data retrieval and aggregation is a challenge since information can come from many sources supporting different data formats.

Conclusion
In the age of digital transformation, industry needs to offer innovative products & services, ease of use and ensure efficiency in service provisioning. Customers are expecting not just products and services but also convenience, comfort and assistance in making informed decisions. Hence, it is important to understand end-user needs, what worked for him/her, and what did not in order to provide personalized service experience to each and every end-user. The rise in IoT, data analytics, smart mobile devices and social networks are the catalysts that an enterprise can leverage in order to keep customers regularly informed with relevant information, to make decision making easier. CAI and context aware security are examples of how such personalized, decision-support capabilities can be provided to individuals in a relatively easy, configurable manner.

References
e-Learning for Effective Classroom Teaching: A Case Study on Educational Institutes in India

Abstract: The use of technology-based learning and electronic learning (e-learning) is one of major trends in the field of higher education. E-learning has advantage, that’s why more higher education institutes have implemented it. They are investing in this, so there is a need to analyze the methodology for effective use of e-learning in class room teaching. Jayawant Shikshan Prasarak Mandal is an educational Trust in Pune, India which is providing technical education in various disciplines. There are more than 70 institutes running under the trust. These institutes have organized a series of lectures for MCA students to implement effective e-learning in collaboration with Maharashtra Knowledge Corporation Limited (MKCL). However, it was observed that there is a lot more to e-learning than just technology. The effectiveness of these lectures was evaluated by feedback of students. This study also reviewed the literature available on implementation methods of e-learning and recommendations are given for the improvement of classroom teaching through e-learning.

Introduction
In today’s global society, e-learning may provide a lot of useful features in a wide range of learning and teaching situations. The emergence of Information technology and society has resulted in evaluation of e-learning. It has also impacted on socio-cultural and economic development globally. Some of the researchers suggest that the e-learning is not time tested and therefore a continuous research is required in this area and it needs lots of understanding in this particular area.

It is a type of learning supported by information communication technology that improves quality of teaching and learning, e-learning encompasses all computers and internet based activities that support teaching and learning both on campus and on distance. [1] e-learning can be implemented in the various ways including the synchronous, asynchronous and the computer based. Author defines the e-Learning as use and acquisition of knowledge facilitated and distributed by electronic means.

There are various form of learning and for the e-learning skills and technologies a mixed approach is to be adopted. As e-Learning provides the many opportunities to facilitate and support learning. The creation of an e-Learning experience has “to understand the various features of the medium, as well as various ways it can be used effectively to impart the learning”.

The environment facilitated by the e-learning where student takes the ownership of their own learning.

e-Learning: Evaluation and Development
The technology progression has been led to the wireless broadband development technologies which are supporting the learning with the portable devices. The above architecture is further developed including web based features leading to the emergence of intranet/extranet/ internet which are supporting the e-learning with web based environment. The network technology evolution is evidenced from wireless broadband access technologies to the development of client-server networks.

Factors affecting e-Learning Implementation
The implementation will depend on the level of readiness in terms of the budget, infrastructure and human resources such as experience, skills, knowledge and attitude.

Literature review shows that there is various works done on the e-learning implementation and development and it is presented in the literature. The comparison of the studies is done. The topics are the perception, evaluation, and the pedagogy and monitoring studies. In this direction researchers and practitioners have given methods for implementation. Table 1 below summarizes the various methods, issues, and challenges for implementation of e-learning. There are several development and e-learning implementation models are there.

Review of the Literature
The existing literature on e-learning is reviewed and presented in summary form in the table 1. It can be concluded from the literature that although there are various implementation methods for e-learning, the organization has to decide which method is suitable and applicable on their structure and environment.

Research Objectives and Methodology
Objectives
Main objective is to find out methods to implement e-learning for effective classroom teaching. To achieve main objective following sub-objectives are set:
- To find out the impact of technical support and arrangements on the effectiveness of the teaching.
- To compare the effectiveness of teaching through ICT and e-learning, with traditional method of teaching this is physical presence of teacher in the class.

Methodology
Universe of the Study
Higher education Technical Institutes in Pune region of India are included in the study as Pune is the educational hub in west of the India. Students associated with various institutes, forms the universe of the study.

Sampling Frame
List of higher technical institutes in...
<table>
<thead>
<tr>
<th>S.No</th>
<th>Authors</th>
<th>Implementation /Methods/Factors</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>[3]</td>
<td>Karim and Hashim</td>
<td>At UPSI e-learning has been implemented in three phases: Design and development  Evaluation  Implementation and institutionalization</td>
<td>Phases of Implementation</td>
</tr>
<tr>
<td>[6]</td>
<td>Brodsky</td>
<td>Aligning and communicating expectations  Addressing IT issues and needs</td>
<td>Effective e-learning Implementation</td>
</tr>
<tr>
<td>[8]</td>
<td>Govindsamy</td>
<td>Customization of system  Content Integration  Integration with HRIS  Ongoing administration  IT issues  System performance</td>
<td>Six challenges in e-learning implementation through LMS: Research Themes</td>
</tr>
<tr>
<td>[9]</td>
<td>Conole</td>
<td>Pedagogy of e-learning  Research into the underpinning technology of e-learning  Issues which arise at organizational level including, effective strategies, development of organizational level</td>
<td>Challenges</td>
</tr>
<tr>
<td>[10]</td>
<td>Allen and Seaman</td>
<td>Technological trends  The economic trend  Increasing Competitive of the educational market  The social demographic trend</td>
<td>Implementation</td>
</tr>
<tr>
<td>[13]</td>
<td>Nicolas and Anderson</td>
<td>What are the technical, managerial and infrastructural requirements to develop effective learning environments?  What protocols and standards are needed to ensure materials can be easily transferred between systems?  How can we ensure accessibility and dealing with copyright and plagiarism issues?  What new pedagogical models are possible and what is their impact?</td>
<td>Challenges</td>
</tr>
<tr>
<td>[14]</td>
<td>Sile et al.</td>
<td>Lack of systematic approach to ICT implementation  Awareness and attitude towards ICTs  Administrative support  Technical support  Transforming higher education  Staff development  Lack of ownership  Inadequate funds</td>
<td>Emerging Issues</td>
</tr>
<tr>
<td>[15]</td>
<td>Divjak and Begovic</td>
<td>The challenges at the state level are:  Overreaching “soft strategy” (effective and with planned resources)  Education development fund (interlinked with university/faculty funds)  General infrastructure for e-learning  Motivation for HEI, professors and students to use e-learning  Intellectual property rights protection  Standardization etc</td>
<td>Challenges</td>
</tr>
<tr>
<td>[16]</td>
<td>O'Neill</td>
<td>Technology uptake is limited to the instruction delivery method  To support learning ineffective use of technology</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Summary of literature on e-Learning implementation
Pune Region was considered, which forms the sampling frame.

**Sampling Method**

The sample technique selected is random sampling.

**Sample Size**

As per list there are 12 higher learning Technical Education Institutes, offering Post graduate degree in Business administration and computer Applications in the JSPM trust. Total number of the students are about 3000. From each of these institutes 10 fully filled questionnaires were collected. In total 120 respondents participated in the study. Duration of the data collection was May 2013 to July 2013.

**Data Collection**

Primary data collection was done using two pre-tested questionnaires and interviewing method. The efficacy of the questionnaires (schedules) was tested on a small group of respondents and the necessary modifications were made on the basis of the feedback received from these respondents. The modified questionnaires were used for collecting the data. The questions were framed so as to cover all the dimensions for the study.

**Empirical Data Analysis**

To find out the impact of technical support, and arrangements on the effectiveness of the teaching.

**Tool Applied:** Multiple Regression

**Dependent Variable:** Effectiveness of teaching

**Independent Variables:** clarity of voice, continuity of data, vision quality, Conversation ability

**Predictors:** (Constant), clarity of voice, continuity of data, vision quality, Conversation ability

The tables above represent the regression model, it can be seen that the value of ‘R square’ in table 1 is .314 which is significant too. From table 2 the F value is 7.919 significant at 0.01 level. It can be analyzed that the impact of the clarity of voice, continuity of data, vision quality, Conversation ability on Effectiveness of teaching is 31 percent. Rest of the performances affected by the other factors. From the coefficient’s table 3 it can be analyzed that continuity of data, vision quality are significant at 0.01 level.

To compare the effectiveness of teaching through ICT and e-learning, with traditional method of teaching this is physical presence of teacher in the class. Students were asked to rate the e-learning lecture as better, same, or worse in their choices and the data is analyzed as and presented as in Fig. 2.

It shows that students were satisfied with the virtual lectures and are ready to accept the e-learning along with the traditional teaching method, as 51 percent have rated the virtual lectures better than that of actual presence of the teacher, 32 percent did not find any difference between the two, and 17 percent find the presence of teacher better than the virtual teaching.

**Results and Discussions**

- It is advisable to have a robust technical support system
implemented for conduction of virtual classroom lectures for e-learning.

- Continuity of data and the vision quality has an important role to play as they affect the teaching quality significantly while the lecture is going on.
- Adoptability of the e-learning methods among the students if they are ready to accept it in case the implementation is done.

**Talking About Future**

It is concluded that e-learning system has to be aligned at various levels including state, university, faculty and individuals. Problems and actions to be taken have to be identified at all levels. e-learning should be considered as an essential element of learning and teaching. It can be concluded from the survey that most ranking goal of e-learning is to improve the learning outcomes and educational processes. The requirement for development of strategy, network infrastructure, continuous training of faculty members and specialized e-learning centres is the outcome of the study.

**References**


Brain Teaser

Crossword »

Test your knowledge on Cyber Security

Solution to the crossword with name of all correct solution providers(s) will appear in the next issue. Send your answer to CSI Communications at email address csic@csi-india.org with subject: Crossword Solution – CSIC May Issue.

CLUES

ACROSS
1. A mathematical process applied on a set of data to represent that data.
4. A property achieved through cryptographic methods to protect against an individual or entity falsely denying having performed a particular action related to data.
5. The protocol which provides security at the network layer
8. A characteristic or specific weakness that renders an organization or asset open to exploitation by a given threat.
9. An attack which tries to make services and resources unavailable.
12. The device which checks all incoming and outgoing traffic for defined security
16. A malicious program which does not need a host program.
17. A network point that acts as an entrance to another network.
18. The property that ensures that the information is not modified
19. The protocol used for email security.
20. A tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.
22. Any computer that has full two-way access to other computers on the Internet.
23. A message in encrypted form.
24. The information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.
25. The mathematical science that deals with cryptanalysis and cryptography.

DOWN
2. Passive wiretapping, usually on a local area network, to gain knowledge of passwords.
3. A computer connected to the Internet that has been secretly compromised with malicious logic to perform activities under remote control of a remote administrator.
6. A digital form of social engineering to deceive individuals into providing sensitive information.
7. Software that compromises the operation of a system by performing an unauthorized function or process.
10. Faking the sending address of a transmission to gain illegal entry into a secure system.
11. An authentication service.
13. An unauthorized act of bypassing the security mechanisms of a network or information system.
14. Listening to a private conversation which may reveal information which can provide access to a facility or network.
15. The process of verifying the user.
19. A small update released by a software manufacturer to fix bugs in existing programs.

Did you know How to create strong password?

Creating strong password is very important while making an account anywhere as the attacker tries different combinations to hack your account. As a counter measure your password must contain as many characters as possible (typically minimum 8). Your password must be a combination of alphabets, special symbols, and numbers. It will become more difficult to crack if it is a combination of upper and lower letters. Do not use names, date of birth or mobile number with passwords as they can be easily guessed. Based on above suggestions if your password is weak, please change your password right now.

Rashid Sheik
Associate Professor, Sri Aurobindo Institute of Technology
Indore

Solution to April 2015 crossword

We are overwhelmed by the response and solutions received from our enthusiastic readers

Congratulations!

All Correct answers to April 2015 month’s crossword received from the following reader:

Er. Aruna Devi (Surabhi Softwares, Mysore),

www.csi-india.org
A Report from CSI Division IV Communications
Chairman, Dr. Durgesh Kumar Mishra

1. Expert Talk on “Quality Research and Plagiarism”

“Necessity is the mother of invention.” Famous quote by Plato always strikes that, that engineers should do something in right place to knock on earth. The methodical investigation into study and sources always requires establishing facts and determining way to reach conclusions. It can be written as Quality Research.

Department of CSE & IT of Swami Vivekanand College of Engineering, Indore has successfully organized Expert talk on “Quality Research and Plagiarism” in association with “CSI-SVCE” Student Chapter on April 15, 2015 and CSI Division IV Communications.

Dr. D K Mishra, Chairman, CSI Div. IV Communications was expert of happening. Dr. Mishra, shared his experiences with different research problems and discussed variety of practical solutions. He also enlightens a light of beam on importance of Plagiarism and unique quality solutions. The event was started with lighting of lamp followed by Prof. Pradeep Rusiya-CSE & Prof. Preetesh Purohit-CSE welcomed the chief guest. The occasion was managed by Prof. Surbhi Parnerkar along with Mr. Ashish Hardia & Mr. Neeraj Kushwah.

The complete talk was great success with participation of more than 60 students and faculty members. Prof. Vijay Birchha, Head-CSE facilitated the guest with souvenir of memories and gives vote of thanks.

2. All India Conference on Sustainable Product Development (AICON’2015)

CSIT Engineering College Durg organized AICON’2015 on 24th - 25th April 2015. The inaugural function of the AICON’2015 (All India Conference) with the theme “Sustainable Product Development” took place on 24th April 2015. The function saw the gracious presence of Dr. ING BVA Rao, Chairman, National Design Forum, Institution of Engineers (IE) as the Chief Guest, Er. Ajay Prakash Verma, Chairman CSIT and Dr. Anurag Verma, Director, CSIT and Organizing Chair, Dr. Anurag Verma welcomed the guests and highlighted upon the significance of the conference theme. He also said that it is a matter of great honor to have a person of stature of Dr. ING B.V.Rao to have as the Chief Guest.

The first day Session Chair & keynote speaker Dr. D K Mishra, Professor (CSE) and Director, Microsoft Innovation Centre at Shri Aurobindo Institute of Technology, Indore discussed the way of improving the research capability and way to do the research for research scholars. His lecture provided the guidelines how to choose the topic, how to write the algorithm and how to start the work. In second session, keynote speaker was Dr. Asha Ambhaikar, Professor & Dean(R&D), CSE, Raipur discussed about the role of Cloud computing in the research area. Total 21 papers are presented in first day.

Second day Dr. H S Hota, Associate professor, Bilaspur university was the key note speaker. He delivered the lecture on Data Mining in research area. Total 15 papers were presented in whole day.

AICON’2015 was concluded by Valedictory function addressed by Dr. N T Khobragade, Dean (Acad.). He addressed all the dignitaries and research scholars and invited Er. Ajay Prakash Verma, chairman CSIT and Dr. Anurag Verma, Director CSIT to distribute the certificates, also some dignitaries for collecting the feedback. The general feedback from the participants was to conduct many more such CSI events in the college campus.

International Conference on ICT for Healthcare

24-25 July 2015
Papers due : May 30, 2015
www.csi-udaipur.org/icthc-2015
Contact : Dr. Durgesh Mishra, Chairman Div - IV, CSI, drdurgeshmishra@gmail.com, Dr. A. K. Nayak, akn_iibm@yahoo.com, Mr. Amit Joshi, amitjoshiuadr@gmail.com
Computer Society of India – Rajkot Chapter
“Layer-3 Switching”

Computer Society of India – Rajkot Chapter, arranged a two hour Knowledge Forum Session on “Layer-3 Switching”. Total 35 participants attended this workshop.

The session taken by a very renowned personality, Dr. Atul Gonsai, Associate Professor, MCA Department, Saurashtra University. This seminar was conducted by CSI, Rajkot Chapter, under Knowledge Forum Session. The session got inaugurated by Dr. R. Sridaran, Immediate Past Chairman, CSI Rajkot Chapter. He welcomed new chairman, Prof. Sunil Bajeja, who further talked about CSI Rajkot Chapter and its various roles and achieved milestones. He also introduced and welcomed the speaker.

The session targeted many PG students, Research Scholars and doctorates of Rajkot Chapter. It added a feather in the list of successes by the CSI Rajkot Chapter.

Dr. Atul Gonsai provided different evolutions of networks devices and gave insight to Layer-2-3 switching. The Vice-President Prof. Nilesh Advani presented vote of thanks. Prof. Jobi Jose, Chapter secretary has made all the arrangements in connection with session.

All participants were provided with certificates for their participation.

Report on CSI Gwalior Chapter Meeting on 12 April 2015

Date: 24-25 July

• Chapter Chairman informed about the activities of CSI Gwalior chapter.
• A presentation was made by Dr. Vipin Tyagi, RVP- III on the activities of CSI to the gathering.
• A discussion was done with MC members and other CSI members. Advised all to increase CSI members and student branches in the chapter. Also advised to increase the CSI activities under chapter, to keep webpage and other information updated and to take necessary steps to get database uptodate.
CSI News

From CSI Chapters »

Please check detailed news at:
http://www.csi-india.org/web/guest/csic-chapters-sbs-news

<table>
<thead>
<tr>
<th>SPEAKER(S)</th>
<th>TOPIC AND GIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>AHMEDABAD / MATRUSHRI L.J GANDHI BCA COLLEGE (REGION III)</td>
<td><strong>Feb 19, 2015:</strong> “Computer Awareness Program in the villages Aravalli District”</td>
</tr>
<tr>
<td>Prof. Ankit S. Patel, BCA College, Modasa Prof. Sanjay G. Patel, BCA College, Modasa Shri Girish Darji, Aniyor High School Shri Surendrabhai Shah, Hon. Secretary, M.L Gandhi Higher Education Society, Paldi</td>
<td>Arvalli is a backward district on the border of Gujarat-Rajasthan. The area is hilly and rich with minerals and forest produce. The entire topographical sight of the district is rich in natural beauty and it has many spots which can be developed as picnic places. It is surrounded by the Arvalli Hills, the oldest mountain ranges in the world. Though the area is rich in natural wealth, it is populated by the people of this area contributed substantially. Under the able leadership of Mathuradas Laljidas Gandhi and his team. The M.L Gandhi Higher Education Society, Modasa is Blessing for Poor People who can not afford the Higher Education in Ahmedabad, Baroda, Vidhyanagar, so our campus is blessing for those people. The objective for open CSI student branch in modasa is provide skill for students of the different schools (Primary or secondary ) because the students of the rural area they don’t have technical skill. Our aim will be to develop technical skill in this district.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SPEAKER(S)</th>
<th>TOPIC AND GIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANITS CSI STUDENT BRANCH (REGION V)</td>
<td><strong>Event- 2 Day Workshop on “Web Design and Development”</strong></td>
</tr>
<tr>
<td>V Srinivas Raju, Assistant Professor, CSE</td>
<td>A 3 day Workshop on Web Design and Development has been organised by ANITS CSI Student Branch at ANITS from 19th to 21st of December, 2014 at E- Class Room, Department of CSE. This workshop has been conducted by V Srinivas Raju, Assistant Professor, Dept of CSE to enable the students and even the faculty to become familiar with web design and development. Participants have been introduced with all the news trending web technologies like php, html 5 etc. Around 50 people have participated in this workshop.</td>
</tr>
</tbody>
</table>

From Student Branches »

<table>
<thead>
<tr>
<th>(REGION - I)</th>
<th>(REGION - IV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITM UNIVERSITY, GURGAON</td>
<td>AMITY UNIVERSITY, NOIDA</td>
</tr>
<tr>
<td>REGION-III</td>
<td>REGION-IV</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>TRUBA COLLEGE OF ENGINEERING &amp; TECHNOLOGY, INDORE</td>
<td>SILICON INSTITUTE OF TECHNOLOGY, BHUBANESWAR</td>
</tr>
<tr>
<td>19-3-2015 – during Inter College Programming Competition : Code Combat ’15</td>
<td>26 to 28-2-2015 – Participants during Annual Inter College Technical Festival</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGION-V</th>
<th>REGION-V</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRINIVAS INSTITUTE OF TECHNOLOGY, MANGALORE</td>
<td>BNM INSTITUTE OF TECHNOLOGY, BANGALORE</td>
</tr>
<tr>
<td>4-4-2015 – Mr. Kartheek Kangala, Senior Engineer, Cisco during the workshop SDN and Data Center Networking</td>
<td>20-3-2015 – during Seminar on Awareness of secure programming</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGION-V</th>
<th>REGION-V</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRI KRISHNA INSTITUTE OF TECHNOLOGY, BANGALURU</td>
<td>BLDEA’S ENGINEERING COLLEGE, BJIAPUR</td>
</tr>
<tr>
<td>11-3-2015 – during one day workshop on Android Applications Development</td>
<td>18 &amp; 19-3-2015 – during Tech Fest on TECHSTORM 2K15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGION-V</th>
<th>REGION-V</th>
</tr>
</thead>
<tbody>
<tr>
<td>BVIT, HYDERABAD</td>
<td>PIIT, NEW PANVEL</td>
</tr>
<tr>
<td>9-4-2015 - Dr. Shekar Muddana, Google, Hyderabad during Guest Lecture on Computational Complexity and Theory of NP Completeness</td>
<td>27-3-2015 – during Magazine Launch event</td>
</tr>
<tr>
<td>(REGION-VII)</td>
<td>(REGION-VII)</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>SONA COLLEGE OF TECHNOLOGY, SALEM</strong></td>
<td><strong>VELAMMAL ENGINEERING COLLEGE, CHENNAI</strong></td>
</tr>
</tbody>
</table>

20-1-2015 – Dr Vijayaragavan Vishwanathan distributed certificates during the contest on Reverse Coding and Ethical Hacking

20-3-2015 – Dr Vijaya Chamundeeswari, Mr Somasundaram Jambunathan, Dr Duraiyandan & Mr Muralidhar during National Conference on Advanced Computing Technologies

<table>
<thead>
<tr>
<th>(REGION-VII)</th>
<th>(REGION-VII)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>M P NACHIMUTHU M JAGANATHAN ENGINEERING COLLEGE, CHENNIMALAI, ERODE</strong></td>
<td><strong>DR. N G P INSTITUTE OF TECHNOLOGY, COIMBATORE</strong></td>
</tr>
</tbody>
</table>

24-3-2015 – During National Level Conference on Emerging Trends in Information & Computer Science 15

19 & 20-3-2015 – During National Level Technical Workshop on Scalable Realtime NoSQL Datastores

<table>
<thead>
<tr>
<th>(REGION-VII)</th>
<th>(REGION-VII)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NANDHA COLLEGE OF TECHNOLOGY, ERODE</strong></td>
<td><strong>EINSTEIN COLLEGE OF ENGINEERING, TIRUNELVELI</strong></td>
</tr>
</tbody>
</table>

1-4-2015 – During National Conference Recent Trends in Computing Technologies & Applications

21-3-2015 – Prof. Sivaganesh, Dr. Velayutham, Mr. Karthick Natarajan, Mr. Mathivanan & Dr Ramar during seminar on Advanced Java Programming

<table>
<thead>
<tr>
<th>(REGION-VII)</th>
<th>(REGION-VII)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SHRI SHANKARLAL SUNDARBHAI SHASUN JAIN COLLEGE FOR WOMEN, CHENNAI</strong></td>
<td><strong>SRM UNIVERSITY, RAMAPURAM CAMPUS, CHENNAI</strong></td>
</tr>
</tbody>
</table>

20-2-2015 – Participants during the event on Research Forum

10-4-2015 – During the event on Acquisition or Innovation: Which is more favoured today

Please send your student branch news to Education Director at director.edu@csi-india.org. News sent to any other email id will not be considered. Please send only 1 photo per event, not more.
Babaria Institute of Technology, CSE department has organized CSI Project Competition cum Exhibition held on 18th April, 2015 under the umbrella of CSI Vadodara Chapter in which a total of 12 best projects were presented in front of IT Experts from different industries in the esteemed presence of Mr. A M Nayak, Chairman, Vadodara Chapter.

Projects demonstration to Jury members

Felicitation of Mr. A M Nayak by Prof. Saurabh Shah

A special lecture on use of HAM Radio in Emergencies and Disasters was conducted by OM Jayant S. Bhide VU2JAU, NC member, CSI Gwalior Chapter in I.T.M. University, Gwalior, on 27 March 2015. The possible advantages of HAM Radio during Disasters. He demonstrated that HAM Radio has always worked as supporting communication system when nothing works. He also pointed out different types of disasters faced and how HAMs have provided the necessary communication to mankind and authorities in difficult situations where HAMs could not find to set up the station at proper place. More than 100 University students attended the program. ITM University Advisor Mr. R.D.Gupta along with HOD CSE Mr. Sanjay Jain along with other faculties attended the program. OM Jayu VU2JAU was supported by OM Kamal Raj VU3RAE and OM Aditya Ashtikar VU3LKA during the program.

A Report on Special Lecture Disaster Communication and HAM Radio at Gwalior

Activity Report of CSI-Bangalore Chapter

Name of the Chapter: Bangalore
Region-V
Event Date: 19th April, 2015 (9.30 am to 4:30 pm)
Event Name: “Programming and Hands on Workshop on Design Patterns”

Computer Society of India (CSI), Bangalore Chapter organized a One day Programming and Hands on workshop on Design Patterns at CSI-BC premises on 19th April, 2015.

Mrs. Bhanumathi K S, Chairperson (Elect.) and Event co-ordinator welcomed the participants with a brief introduction of the speaker. She spoke about the upcoming events of CSI-BC. She proudly mentioned that CSI-BC has been the most vibrant Chapter.

Kind Attention: Prospective Contributors of CSI Communications

Please note that Cover Theme for forthcoming issue of June 2015 is planned as follows:

• June 2015 - Data Science

Articles may be submitted in the categories such as: Cover Story, Research Front, Technical Trends and Article. Please send your contributions before 20th May 2015. The articles may be long (2500-3000 words maximum) or short (1000-1500 words) and authored in as original text. Plagiarism is strictly prohibited.

Please note that CSI Communications is a magazine for membership at large and not a research journal for publishing full-fledged research papers. Therefore, we expect articles written at the level of general audience of varied member categories. Equations and mathematical expressions within articles are not recommended and, if absolutely necessary, should be minimum. Include a brief biography of four to six lines for each author with high resolution author picture.

Please send your articles in MS-Word and/or PDF format to Dr. R Nadarajan, Guest Editor, via email id nadarajan_psg@yahoo.co.in with a copy to csi@csci-india.org.

(issued on the behalf of Editorial Board CSI Communications)
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Details &amp; Organizers</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>May 2015 events</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07-09 May 2015</td>
<td>International Workshop on Intelligent Approaches for Object Oriented Modeling in Component Based Software Engineering (IAOOM-2015) to be organized at Jaypee University of Engineering &amp; Technology, Guna (MP) <a href="http://www.juet.ac.in">http://www.juet.ac.in</a></td>
<td>Dr. Shishir Kumar <a href="mailto:dr.shishir@yahoo.com">dr.shishir@yahoo.com</a></td>
</tr>
<tr>
<td>15-17 May 2015</td>
<td>International Conference on Emerging Trend in Network and Computer Communication (ETNCC2015) at Department of Computer Science, School of Computing and Informatics Polytechnic of Namibia in Association with Computer Society of India Division IV. <a href="http://etncc2015.org/">http://etncc2015.org/</a></td>
<td>Prof. Dharm Singh <a href="mailto:dsingh@polytechnic.edu.na">dsingh@polytechnic.edu.na</a></td>
</tr>
<tr>
<td>17 May 2015</td>
<td>WTSD 2015 - Telecommunications and ICTs: Drivers of Innovations at CSI Udaipur Chapter, IE(I) ULC At Udaipur</td>
<td>Dr. Y C Bhattacharya <a href="mailto:drybhatt@hotmail.com">drybhatt@hotmail.com</a> Amit Joshi <a href="mailto:amitjoshiudr@gmail.com">amitjoshiudr@gmail.com</a></td>
</tr>
<tr>
<td>30-31 May 2015</td>
<td>Two Day National Conference on ICT Applications “CONICTA-2015&quot; at IIITM Auditorium, Patna organized by CSI Patna Chapter in association with Division III ad Division IV of Computer Society of India.</td>
<td>Prof. A K Nayak <a href="mailto:aknayak@iibm.in">aknayak@iibm.in</a> Dr. Durgesh Kumar Mishra <a href="mailto:drdurgeshmishra@gmail.com">drdurgeshmishra@gmail.com</a></td>
</tr>
<tr>
<td><strong>July 2015 events</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-4 July 2015</td>
<td>International Conference on ICT for Sustainable Development, organized by CSI Division IV, Ahmedabad Chapter, ASSOCHAM Gujarat Chapter and Sabar Institute of Technology for Girls, Gujarat At Ahmedabad <a href="http://www.ict4sd.in">http://www.ict4sd.in</a></td>
<td>Amit Joshi <a href="mailto:amitjoshiudr@gmail.com">amitjoshiudr@gmail.com</a> Dr. Nisarg Pathak <a href="mailto:nisarg.pathak@gmail.com">nisarg.pathak@gmail.com</a></td>
</tr>
<tr>
<td>24-25 July 2015</td>
<td>International Conference on ICT in Health Care and E-Governance, at Sri Aurobindo Institute of Technology, Indore in association with Computer Society of India Division III, Division IV, Indore Chapter, ACM Udaipur Chapter. <a href="http://www.csi-udaipur.org/icthc-2015/">www.csi-udaipur.org/icthc-2015/</a></td>
<td>Dr. Durgesh Kumar Mishra <a href="mailto:drdurgeshmishra@gmail.com">drdurgeshmishra@gmail.com</a> Dr. AK Nayak <a href="mailto:aknayak@iibm.in">aknayak@iibm.in</a> Mr. Amit Joshi <a href="mailto:amitjoshiudr@gmail.com">amitjoshiudr@gmail.com</a></td>
</tr>
<tr>
<td><strong>Aug 2015 event</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7-8 Aug 2015</td>
<td>International Conference on Innovations in Computer Science &amp; Engineering (ICICSE-2015) Organized by Guru Nanak Institution, Hyderabad in association with Computer Society of India Division IV and Hyderabad Chapter. <a href="http://www.icicse2015.org">www.icicse2015.org</a></td>
<td>Dr. H S Saini <a href="mailto:md@gniindia.org">md@gniindia.org</a> Dr. D D Sharma <a href="mailto:drmca.gnipg@gniindia.org">drmca.gnipg@gniindia.org</a></td>
</tr>
<tr>
<td><strong>Sept 2015 event</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10-12 Sep 2015</td>
<td>International Conference on Computer Communication and Control (IC4-2015) at Medicaps Group of Institutions, Indore in association with Computer Society of India Division IV, CSI Indore Chapter and IEEE MP subsection.</td>
<td>Dr. Promod Nair <a href="mailto:Mitm.csedepartment@yahoo.com">Mitm.csedepartment@yahoo.com</a> Prof. Pankaj Dahore <a href="mailto:Pk_dahore@yahoo.co.in">Pk_dahore@yahoo.co.in</a></td>
</tr>
<tr>
<td><strong>Oct 2015 events</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9-10 Oct 2015</td>
<td>International Congress on Information and Communication Technology (ICICT-2015) at Udaipur, organized by CSI Udaipur Chapter, CSI Division IV, SIG-WNs, SIG-e-Agriculture and ACM Udaipur Chapter. <a href="http://www.csi-udaipur.org/icict-2015">www.csi-udaipur.org/icict-2015</a></td>
<td>Dr. Y C Bhattacharya <a href="mailto:drybhatt@hotmail.com">drybhatt@hotmail.com</a> Mr. Amit Joshi <a href="mailto:amitjoshiudr@gmail.com">amitjoshiudr@gmail.com</a></td>
</tr>
<tr>
<td>16-17 Oct 2015</td>
<td>6th Edition of the International Conference on Transforming Healthcare with IT to be held at Hotel Lalit Ashok, Bangalore, India. <a href="http://transformhealth-it.org/">http://transformhealth-it.org/</a></td>
<td>Mr. Suresh Kotchatill, Conference Coordinator <a href="mailto:mail@transformhealth-it.org">mail@transformhealth-it.org</a></td>
</tr>
</tbody>
</table>
Announcement and Call for Papers

Golden Jubilee Celebrations
Computer Society of India
50th Annual Convention
(CSI - 2015)
Theme
DIGITAL LIFE
(3rd-5th December, 2015)
Venue:
India International Centre, Lodhi Road, New Delhi - 110003
For paper submission and more details, visit us at: www.csi-2015.org
Proceedings of the accepted papers will be published by Springer
Selected few papers will be considered for CSI Transactions on ICT following its due process

Paper Submission Deadline: 02nd August, 2015

Computer Society of India (CSI):
CSI, founded in 1965, is India’s largest and oldest non-profit, professional body of IT professionals. CSI has over 1,00,000 members attached to 70 chapters and over 500 student branches spread across the length and breadth of the country. CSI also represents India in international bodies such as International Federation of Information Processing (IFIP) and South-East Asian Regional Computer Confederation (SEARCC). The purposes of the society are scientific and educational, directed towards the advancement of theory and practice of computer science, computer engineering and technology, systems sciences and engineering. CSI Delhi Chapter is one of the largest and most vibrant chapters in the country with several awards to its credit. Year 2015 being the 50th year of CSI, CSI – 2015 is the Golden Jubilee convention of the Computer Society of India.

Full length original and unpublished papers, based on theoretical and experimental contributions, related, but not limited to, the concepts covered under the following tracks, are solicited for presentation and publication in the convention.

Track #1: ICT Based Innovation
Track #2: Next Generation Networks
Track #3: 3-D Silicon Photonics & High Performance Computing
Track #4: Real Time Languages Translation

Track #5: Sensors
Track #6: Big Data Analytics
Track #7: Systems and Architecture
Track #8: Cyber Security

Important Dates

Submission of Full Length Paper: 02nd August, 2015
Submission of Camera Ready Copy (CRC) of the Paper: 18th October, 2015
Paper Acceptance Notification: 05th October, 2015
Registration Deadline: 18th October, 2015

Contact us:
CSI – 2015 Convention Secretariat
Computer Society of India (Delhi Chapter), #32, DDA CSC Market, Block Q (D), Pitampura, Delhi – 110034
Tel.: +91-11-25275055, Email ID: csi2015.delhi@gmail.com