Cover Story
Digital Forensics – An Enabler 7

Article
An Intelligent Prototype to Lay the Road to Secure Next Generation Networks 29

Practitioner Workbench
The Secure Shell – SSH 34

Security Corner
Digital Forensics in Cloud Computing Environments: Current Challenges and Solutions for Effective Forensic Investigation 38
an individual.
- 2 are friends.
- 3 is company.
- more than 3 makes a society. The arrangement of these elements makes the letter ‘C’ connoting ‘Computer Society of India’.
- the space inside the letter ‘C’ connotes an arrow - the feeding-in of information or receiving information from a computer.
Cover Story
7 Digital Forensics – An Enabler
by Sandeep Godbole
9 Digital Video Forensics: Description Based Person Identification
by Mehul S. Raval
12 Digital Forensics in Virtual Environments
by Ezz El-Din Hemdan and Manjaiah D.H.
14 The Role of Cyber Forensics in Legal and Ethical Aspects of Cyberspace
by Vijith T. K. and K. V. Pramod
18 Overview of Digital Forensic Investigation
by K. Nithya and M. Saranya
20 Digital Forensics: Need of the Hour
by Gobi Ramasamy
21 Introduction, Goals and Challenges in Digital Forensic Process
by Dilpreet Singh Bajwa and Satish Kumar

Research Front
23 Purity of Clusters: Kernel K-Means and Beyond
by Pranab Kumar Das Gupta, Bindu Patnala and Asit Kumar Sahu
26 Digital Forensics and its challenges in Big Data
by Sunita A. Yadwad

Articles
29 An Intelligent Prototype to Lay the Road to Secure Next Generation Networks
by R. Nagarathna and S. Mercy Shalinie
32 Web Application Vulnerabilities – The Hacker’s Paradise
by B. Janet, Nirmal K. and R. Kumar

Practitioner Workbench
34 The Secure Shell – SSH
by A. Bharanidharan

Security Corner
38 Digital Forensics in Cloud Computing Environments: Current Challenges and Solutions for Effective Forensic Investigation
by Anand Nayyar and Vikram Puri

PLUS

| Book Review | 33 |
| Membership Form | 36 |
| Brain Teaser | 41 |
| CSI Reports | 43 |
| Student Branches News | 47 |

Complaints of non-receipt of CSIC may be communicated to Mr. Ashish Pawar, 022-29267124, ashish@csi-india.org, indicating name, membership no, validity of membership (other than life members), complete postal address with pin code and contact no.

Printed and Published by Mr. Sanjay Mohapatra on Behalf of Computer Society of India, Printed at G.P. Offset Pvt. Ltd. Unit-81, Plot-14, Marol Co-Op. Industrial Estate, off Andheri Kurla Road, Andheri (East), Mumbai 400059 and Published from Computer Society of India, Sampudhi Venture Park, Unit-3, 4th Floor, Marol Industrial Area, Andheri (East), Mumbai-400093. Tel.: 022-29261700 • Fax: 022-28302133 • Email: hq@csi-india.org Editor: Dr. A. K. Nayak
Dear Fellow CSI Members,

Digital forensics is an emerging area in the digital age that deals with acquisition, recovery, documentation, and analysis of information generated by the digital devices. It generally deals with finding evidences to deal with questions like: what happened, why happened, when happened, how it happened, and who was involved. Digital Forensics is very challenging due to involved technical complexity of digital evidence as courts find it difficult to understand the true nature and value of that evidence. It is increasingly common for criminal trials to rely on digital evidence. Digital evidence is used these days in the court proceedings.

Keeping in mind the importance of Digital Forensics in today’s context, the publication committee of Computer Society of India, selected the theme of CSI Communications (The Knowledge Digest for IT Community) March 2016 issue as “Digital Forensics”.

The first cover story of this issue “Digital Forensics – An Enabler” by S. Godbole describes importance of digital forensics capabilities for an organization. In next cover story “Digital Video Forensics: Description Based Personal Identification”, M. S. Raval has described challenges and possible solutions in person identification using soft biometrics. Cover story “Digital Forensics in Virtual Environments” by E. E. Hemdan and Manjaiah D.H. discusses about the digital forensic investigation process in the virtual environments. Next, Vijith T. K. and K. V. Pramod have suggested certain steps which should be taken by the government, people, law enforcement agencies, public and private organisations for getting benefits of cyberspace for society in cover story “The Role of Cyber Forensics in Legal and Ethical Aspects of Cyberspace”. In “Overview of Digital Forensic Investigation”, by K. Nithya and M. Saranya, digital forensics investigation has been described. Short Article “Digital Forensics: Need of the Hour” by G. Ramasamy describes the importance of digital forensics in present time. Last cover story “Introduction, Goals and Challenges in Digital Forensic Process” by D. S. Bajwa and S. Kumar gives various aspects of digital forensics process.

In Research Front category, “Purity of Clusters: Kernel K-Means and Beyond” by P. K. D. Gupta, B. Patnala and A. K. Sahu highlights the limitations of K-Means and how they are handled by the other methods. In next article “Digital Forensics and its challenges in Big Data”, S. A. Yadwad emphasized on need of a new set of E-Discovery tools to take large numbers of documents, emails, posts and other messages to automatically filter out the major evidences.

Article “An Intelligent Prototype to Lay the Road to Secure Next Generation Networks” by R. Nagarathna and S. M. Shalnie provides a gist on the various security issues that may arise in nextGen networks. Another article “Web Application Vulnerabilities –The Hacker’s Paradise” by B. Janet, Nirmal K. and R. Kumar gives importance of security awareness to promote secure software development in today’s cyber era.


This issue also contains CSI Membership form, Book Review, Crossword, CSI activity reports from divisions, chapters, student branches and Calendar of events.

I would like to thank Ms. Ritika Wason from BVICAM, Delhi, all staff members from CSI HQ and CSI ED for their timely support in bringing all issues during the year.

I take this opportunity to express my sincere thanks to Dr. Vipin Tyagi, Guest Editor, for bringing this issue successfully. I extend my gratitude to the entire ExecCom and Publication Committee for their continuous support in bringing all the issue successfully. With the support of all, we were able to brought all the issues from April 2015 to March 2016 without any financial support from CSI for administrative requirements.

On behalf of publication committee, I wish to express my sincere gratitude to all authors and reviewers for their contributions and support to this issue.

I hope this issue will be successful in its aim of creating awareness about Digital Forensics, providing information about latest trends in digital forensics research and new ideas of research in the area.

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

Prof. A.K. Nayak
Chief Editor
Greetings!

I am completing my term as President of this largest and oldest professional society on 31st March, 2016. It was a challenge for me to steer this august society at the national level. I am happy to mention that I put my all efforts for the development of the CSI in all respect inspite of many challenges. It was indeed a difficult task for me to meet the expectations of my ExecCom colleagues, Chapters, Student Branches and members. But with whole hearted support from ExecCom and staff members at CSI HQ and ED, I could be able to do justice to my role as President, CSI.

There are many opportunities for CSI. Be it a role in advisory capacity at Central and State Governments, training and certification in advance technology, publications, promotion of research and innovation, etc. These will require skilled manpower at HQ and ED with sufficient budgetary provisions besides support from Chapters and members who can play active role in promotion and growth of CSI. There are many challenges for the new ExecCom and Office Bearers but I am confident that new team will be able to meet the expectations of members and stake holders.

I attended and delivered a key note address in the 10th National Conference on IT in Defence-2016 hosted by CSI, Bangalore Chapter in association with CSI SIG on Security and Formal Methods on 12th February, 2016. The conference was well attended by the delegates from various sectors. Congratulations to CSI Bangalore Chapter for successfully organising this conference.

COMNET-2015, International Conference on Communication and Network with a theme “Issues and Challenges with IOT revolution” was successfully organised by CSI Ahmedabad Chapter during 20-21 February, 2016. The speakers were Prof. Andrzej Rucinski, University of New Hampshire, Durham, New Hampshire, USA and Dr. Sumit Chowdhury, a global thought leader in the field of Telecom and Information analytics and the founder of Gaia Smart Cities, a telecom and solutions operator of Smart Cities. More than 80 research papers were presented by young researchers.

During March, 2016, many activities are planned by chapters and student branches to celebrate CSI Foundation Day. I am sure members and professionals at large are able to participate in these events.

Prime Minister Narendra Modi launched “Make in India” programme in September, 2015 as a part of sustainable national building initiative to transform India into a hub for global design, innovation and manufacturing. The Make in India week was celebrated during 13th to 18th February, 2016 at Mumbai. Prime Minister said, “We want to present to the world the enormous opportunities that India presents. This is the best time to be in India, even better to ‘Make in India’”. Let us work together to Make in India.

I thank the Chief Editor Dr. A.K. Nayak and Guest Editor Dr. Vipin Tyagi for sustaining the timely and quality publication of CSI Communications during the year.

With best wishes,

Bipin V. Mehta
President, CSI

 prof. Bipin Mehta, Director, School of Computer Studies, Ahmedabad University, Ahmedabad, president@csi-india.org
1. ExecCom Meeting of the new Members will be held in Mumbai on 2 & 3 April, 2016. It will be start of another eventful year with new plans.

2. Our Membership is showing an upward trend. New Student Branches are starting in different institutions across India. We are trying to open new Chapters in different areas.

3. I have been stressing on the need to improve CSI Conferences and bring out useful and attractive proceedings. For this purpose talks are at the final stage with Springer to have a MOU so that proceedings of conferences which meet their international standards can get it published by Springer. This will definitely boost the quality of the conferences as well improve the publications.

4. CSI Student Branches and Chapters are requested to send the reports of the different activities conducted with high quality photographs. The email ids are given again for the benefit of the coordinators:

Reports on Student Branch activities should be sent to: sb-activities@csi-india.org. The report should be brief within 50 words highlighting the achievements and with a photograph with a resolution higher than 300 DPI.

Reports on Chapter Activities should be sent to: chapter-activities@csi-india.org. The report should be within 100 words highlighting the objective and clearly discussing the benefits to CSI Members. It should be accompanied by a photograph with a resolution higher than 300 DPI.

Conference/ Seminar reports should be sent by Div. Chairs and RVPs to conferences@csi-india.org. Again the report should be brief within 150 words highlighting the objective and clearly discussing the benefits to CSI Members. It should be accompanied by a photograph with a resolution higher than 300 DPI.

5. Now we are in the process of finalizing an agreement with PMI (Project Management Institute) to offer trainings on different aspects of Project Management. The skills in Project Management are in demand all over India and it will be great help if we can offer the certification trainings to our members at reasonable cost.

6. Long term Institutional Membership for academic institutes is in place and institutions are encouraged to apply for long term membership.

7. CSI Foundation Day happens to be on March 6 and all Chapters and Student Branches are requested to celebrate CSI Day on March 6 or in the week of March 7 with Seminars and other knowledge sharing events. The events should be widely publicized to create awareness about CSI activities.

Best wishes,

Dr. Anirban Basu
Vice President, CSI

Prof. Dr. Anirban Basu, Vice President, vicepresident@csi-india.org
often, things that do not seem to exist to a naked eye, do exist and reveal much more than they hide. Like an iceberg that lies hidden below the surface of water, digital evidence and traces remain hidden from an untrained eye. Those who know how to explore these hidden aspects are much better suited to comprehend this reality. Edmond Locard (1877-1966) is credited with the famous Locard’s Principle. He wrote ‘it is impossible for the criminal to act, especially considering the intensity of a crime, without leaving traces of his presence’. This statement has been the basis for the ‘principle of exchange’, that often forms the basis or rationale for the discipline of forensics. The principle states that — with contact between two items there will be an exchange. While this was discussed in the era before the advent of computers, it’s applicability to computer and information technology is no exception. When an entity uses computers and relevant infrastructure traces of these activities are created and exchanged in this eco system. Discovery of these traces forms the basis for digital forensics. Given the complexity of information technology, our actions and activities leave an imprint at multiple places — on servers, on desktops, in switches and routers and even the database. Mundane actions like file creation, web browsing, deleting content leave behind a trace that can be discovered by those who know the principles, tools and techniques. Digital Exhaust is a recent term that refers to the traces that are unknowingly generated by users especially in the context of the Internet, social media and the connected world. The traces range from cookies, log files to many others that directly or indirectly identify the activities of the user. This digital footprint is often the cause of concern in the context of ‘data privacy’ since it enables traceability and establishes identity associated with the actions. For the forensic investigator though it provides a treasure trove of information.

Digital Forensics is not a single action but refers to a collection of multiple activities and techniques that involve different approaches and tools. At a high level though, the objective remains consistent, that of obtaining in a legally consistent manner evidence that proves or supports assertions regarding actions, activities or events. Considering that our conclusions not only have to be accurate but credible and stand scrutiny, its not just the usage of right technology that is important. Forensic requires deploying the right approach, utilising the appropriate tools, following the correct methodology for the analysis, collection, custody and presentation of information. Many a time the evidence obtained from the digital forensic activity needs to be presented in the court of law. Admissibility and acceptance of the evidence in the court would hinge upon whether the evidence was collected in a lawful manner, using techniques that maintain the integrity of the evidence. Maintaining, preserving and presenting the information is equally important after it has been collected. That the digital evidence continues to retain its integrity and is not tampered with from the point of collection though its transfer to different custodians needs to be established.

Digital forensic comprises of multiple approaches, each one with its own utility and relevance. The appropriateness of the technique varies based on the technology, the purpose of forensics investigation, nature of data and the forensic techniques to be used. Based on the nature of analysis, forensic techniques are classified into:

- a) Live system analysis
- b) Disk Forensics
- c) Network Forensic

Live analysis includes examining live systems for insights, information and evidence from the live system that is booted, live and running. Certain types of information like volatile memory content, certain types of temporary storage content are available only till the time that the systems are live. They are lost when systems are shut down. Thus, certain types of data require collection when the system is live.

Disk Forensic, generally refers to analysis of computer disks to locate data elements that are not apparently visible with general purpose business software. These include data elements like deleted files, temporary files, residual data that has not been overwritten. Performing disk forensic requires a good knowledge of file systems and their structure besides that of forensic software. Disks are a good source for information retrieval. Most of the operating systems do not physically ‘clean up’ the disk space occupied by files when files are deleted. They merely delete the logical existence of the file and make this space available for other data to be stored. However, till such time that the space is actually over written it retains remnants and bits of information from the files that have been deleted. Specialist disk forensic software enables the investigator to view the disk sector wise and look for the actual content stored on the disk.

Network Forensics refers to information that can be obtained from the network and related devices. For example, traces of access from a specific external IP can be looked up from the Firewall logs. Packet analysers can see inside the data packets that flow through the network. In the era of the connected world and where actions can be performed by entities located thousands of miles away, the importance of network forensics is quite significant.

A general principle associated with forensic analysis is to perform analysis on the forensic copy rather than on the original information. This is done to ensure that original evidence is not accidently tampered with during the process of analysis. This is especially relevant for disk forensics where analysis on the original evidence can lead to modifications, thus impacting the evidentiary value in the court of law. Through an acquisition process, a bit by bit image of the disk is created. This is different than simply copying the files using the operating system commands. The forensic copy is a mirror image of the disk with all data – existing and residual that resides on the disk. This copy is used for analysis and the original disk is retained with care as part of the evidence. The bit by bit copy that creates an identical forensic image is generally done using devices that prevent any modification or write operation on the original disk when the copy is under progress. A hash value based on the disk content of the original disk is computed by the software that creates a forensic copy, to help establish integrity of the forensic
copy. Independent calculation of the hash value of the forensic copy and matching it with the hash can help to establish the authenticity of the copy.

Though forensic can seem to be a glamorous task, fed by by the detective stories and popular fiction, in reality it is a highly technical and intensive work. Looking for a piece of information is many a time looking for a needle in a haystack. For proper discovery of evidence therefore it is important to know and define the objective and specifics of what is being searched.

For example, an investigator who is given a disk to look for proof of tax avoidance may be able to achieve little. However, if the investigator is told to locate existing content, deleted content or residual content that has reference to company ABC Ltd will be able to perform the task better and quicker. Similarly, a forensic investigator who is told to identify a stealthy malware attack from outside may not be able to scope the activities and provide evidence. However of the investigator is requested to look for evidence of a malware attack that has happened in a given time window and that has probably impacted a list of data bases or servers is in a much better position to launch herself into the task. However, a lot of times the requirements cannot be defined and require certain trial and error analysis. For example, investigating a hard disk for suspicion related to anti-company activities like stealing source code, sharing corporate secrets with competitors etc does require a lot of ingenuity on the part of the investigator.

A forensic project has its own life cycle. The first step in the cycle is to identify the objective of the analysis. Defining the objective ensures that the activities to be performed are defined and performed in a planned manner. The next step is to identify and secure the object for evaluation and analysis eg identify the disks, servers or logs that need to be analysed. If relevant a forensic copy of the evidence along with a forensic hash value needs to be prepared based on the nature of forensic analysis is to be performed. The next stage - evidence or information identification and collection activity phase requires the knowledge of tools and techniques to search, identify and acquire it. The insights or evidence obtained have to be reported with the supporting evidence as part of the last phase. It is important that adequate documentation with respect to the chain of custody of the evidence be maintained all along. This would support assertions related to appropriate and controlled acquisition and maintenance of evidence to substantiate the integrity of evidence.

It is important to understand the dependencies and limits associated with the digital forensic process. The role of forensic software is not to generate new data but to help uncover existing data or correlate the different sets of data to create a storyline of the activities under investigation. A significant amount of forensic information is captured based on the nature, features and capabilities of the underlying operating systems, other system software and utility as well as application programs. If the information does not exist no extent of efforts in locating it would yield results. Analysis of windows registry can identify the serial number of the USB device connected to the laptop or desk top but falls short of identifying further details including the date and time as well as the content that has flown through. Analysis of the file system reveals when the last change to the file was made but is unable to identify dates of the changes. Analysis of temporary files may probably provide a clue if they exist but it then becomes a probabilistic venture. Thus it is important that the limits of what can be achieved is understood. This brings to fore the point that for critical systems the environment should be designed in a manner that has enough capabilities to support forensic investigation. If these are not planned and implemented, it impacts the possibilities of future forensic analysis. The emergence of virtualization, cloud computing and mobile devices has introduced new challenges. With the exception of mobile devices virtualization and cloud rely on images that are well beyond the capabilities of traditional forensic tools. A lot of reliance on tracking and logging mechanism is therefore relevant for gathering information and evidence.

Organizations should have a forensic program in place with the necessary capabilities, tools and policies. This ensures that organizations are well prepared for eventualities including investigation of malafide activities, incident management and for maintaining a robust compliance program.

About the Author

Mr. Sandeep Godbole, CISM, CGEIT, CISSP, CEH, CISA [CSI-10083291] is currently working as General Manager, Information Security at Syntel, Pune. He has about two decades of experience in Information Security, Assurance and IT Governance areas. He has contributed articles on IT Security in various publications. He is a speaker at various national and international conferences in the areas of security, assurance and governance. He can be reached at sandeep_godbole@yahoo.com.
Digital Video Forensics: Description Based Person Identification

Mehul S. Raval
Associate Professor, Institute of Engineering and Technology, Ahmedabad University, Ahmedabad

Introduction

A very interesting problem in digital video forensics is as follows. Consider a typical unconstrained video surveillance frame as shown in Fig. 1, then the task is to identify subject(s) in a video sequence based on the description. For example, a typical description could be:

- **Age**: 25 - 45, **Gender**: Female, **Hair Colour**: Black, **Hair Style**: Short, **Cloth**: Pink Colour Coat, **Accessories**: Handbag. Output of such algorithm should be probable subject(s) in a given video sequence. For example two such possibilities in a frame are highlighted in Fig. 1.

Conventionally, biometrics provide a mechanism to identify the person based on physical or behavioral traits. Several primary biometric traits like face, finger print, iris, palm print, gait, ear, signature, key stroke dynamics and many more are used for the person identification. Biometric system using single trait for identification is known as unimodal system\(^{[7]}\). Such systems are heavily affected by:

1. The sensor noise.
2. Non universality of the biometric trait.
3. Lack of security.
4. High error rates.

Non universality has been a biggest challenge as observed during implementation of UIDAI\(^{[2]}\) project in India. Many senior citizens finger prints could not be enrolled due to high quality enrolment requirements.

Moreover, it has been found that every biometric trait has a theoretical upper bound in its ability to segregate two individuals \(^{[3]}\). Unimodal systems suffers from high error rate when deployed for security applications. Problems with unimodal systems can be removed by using traits from multiple sensors. Such a system is more immune to a noise, it overcomes non-distinctiveness of the trait, improves the security against spoof attacks and above all improves matching accuracy. However, multimodal system requires many high class sensors, increasing the cost and storage requirements. It is more invasive for a user; as they have to supply multiple traits during verification, causing inconvenience.

**Soft Biometrics**

One of the possible solution to improve the accuracy and also be less invasive to a user is to utilize additional information like height, weight, skin colour, hair colour, ethnicity, gender, age, eye colour, etc. of the user along with the primary biometric trait. This ancillary information about the user is known as soft biometrics. It has been defined as “those characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals.”\(^{[4]}\). Authors in \(^{[11]}\) defines it as “Soft biometrics traits are physical, behavioral or material accessories, which are associated with an individual, and which can be useful to identify an individual.” In probabilistic framework soft biometrics like ethnicity, gender, age, can be characterized by discrete random variable, while traits like height, weight, skin colour are typified by the continuous random variable. Some of these soft biometric traits are Gender, Ethnicity, Skin colour, Height, Weight etc.

The soft biometrics can be easily integrated with a way human describes an individual. For example, “A young Indian male within age group of 15 - 18 year, wearing Blue T-Shirt, medium height, ...." This results into semantic representation of soft biometrics with human understandable labels. Soft biometrics can be used in number of ways:

1. Combination of multiple soft attributes can improve the detection accuracy of the biometric system\(^{[5]}\). This means soft biometric based human identification system will have two stages; first stage based on primary biometric trait and second stage based on soft biometrics. The primary biometric trait results into coarse identification and fine tuning is done by the soft biometric stage.
2. They can be used to minimize the search space dimensionality of the primary biometric database\(^{[6]}\). This can significantly reduce the search time for a given query.
3. Soft biometrics can be used for tuning performance of a biometric system such as threshold for matching scores\(^{[7]}\).

However, this article is focused on using soft biometrics for the digital video forensics in the surveillance video and the motivation for using soft biometrics is discussed in the next section.

**Soft Biometrics for Digital Video Forensics**

Utility of the primary biometric trait decreases significantly when they are derived from a low quality video footage. Identification from a distance is the prime requirement from a security perspective. Fortunately, there is an increase in deployment of the close circuit TV (CCTV’s) across the World. Primary purpose is to fight against the crime in the society and also to provide...
evidence when it happens. Many CCTV cameras suffer from the low frame rate and poor image resolution but number of soft biometric features like hair colour, skin colour, arm length can be extracted unobtrusively without cooperation from the subject. From the surveillance perspective the soft biometrics offers the following advantages [11]:

1. Soft biometrics can be derived from the low quality video footage, making them ideal for a surveillance application. Thus, they have inherent robustness to low quality.
2. Soft biometrics can be described using human understandable labels. They bridge the gap which exists in a manner machine and humans approach identification.
3. Soft biometrics allow smooth conversions between human descriptions and biometrics.
4. It opens a strong possibility of searching based only on the human description and without any apriori features of the subject. This is useful while searching a surveillance footage based on the witness description about the previously unobserved person.
5. Soft biometrics are non invasive to the user as they can be captured without subject cooperation.
6. However, such descriptions can preserve privacy as particular soft biometric feature can be mapped to many individuals.

Due to large number of CCTV deployment in the city it is difficult to monitor minutest details by a human operator. It can be even more tedious and time consuming when looking for a particular person in the video. Soft biometrics can potentially solve this problem. The human describable features of soft biometric traits can also be used to perform searches based only on a human description - possibly obtained from an eyewitness at the crime scene. This allows for use of soft biometrics when primary biometric traits are unavailable or cannot be obtained.

As discussed in the introduction, given an unconstraint video stream following set of questions can be solved.

**Problem Statement One:** Locate a person in an un-constrained video stream based on soft biometrics (Person identification).

**Problem Statement Two:** Given an image / video frame with a subject, automatically extract soft biometric features and search for the match in a video stream (Person re-identification).

Objectives for such problems could be as follows.

1. Locate a person-of-interest based on specific set of soft biometric attributes from surveillance video without prior registration.
2. Integrating and minimizing semantic gap between human descriptions and soft biometric traits.
3. Extracting soft biometric features from an input image or a video frame and use these features to locate a matching individual in the video stream.

This is relatively newer but very exciting domain. Many researchers are paying attention to solve problems defined earlier. One must take note of such efforts to understand root of the problem and also to develop better solutions.

**Prior Art**

Denman et al.[8] used soft biometric traits to identify people when conventional biometrics are not available. The height and color of the torso, legs, and head are used to represent the subjects. Persons are located using segmentation and then analyzed from the color in each row. After region location, a color histogram is found and the real-world height is estimated. The PETS 2006 surveillance database was used to test the system. This dataset features four cameras monitoring a train station: four recordings of 25 people were obtained. The system achieved an equal error rate of 6.1% when evaluated using the leave-one-out cross-validation scheme.

Demirkus et al.[9] proposed a technique to identify persons moving between multiple surveillance cameras for face recognition. They used gender, ethnicity, and session-based soft biometrics like skin color, upper and lower body clothing color, and hair color. Once a person is identified in the footage, the directionality is determined, e.g. the face of the person walking toward the camera is analyzed to determine ethnicity and gender, which is combined with the color-based traits that are extracted automatically. A custom low-resolution surveillance dataset was constructed featuring 100 subjects. An average correct classification rate of 60% and 83%, for gender and ethnicity are observed by them.

Many attempts have been made at the problem of person re-identification i.e. identifying previously observed individual in a surveillance video. Such approaches focussed on colour and texture based features which are view independent [13] - [16]. One must note that description based searching is not possible using them. Attempts [16] - [17] have been made to describe a person using set of features and match them in the video. Authors in [16] used colour, height, and build to represent a subject. A query with the desired features can be submitted for search in the video. Authors in [17] tackled the problem using attribute search. Various facial features like beard, moustache, eye glass, hair, hat as well as colours of torso and legs are extracted. Query in terms of above features are submitted to the video. Nevertheless, these approaches require subjects to be segmented, modeled and then compared against the set of attributes. These methods are incapable of searching the images directly (without preprocessing) based on the query.

Recently, state-of-the-art techniques based on soft biometric have reported localization accuracy of 21% over entire video sequence[16]. Description based person identification is maturing but there are many key challenges to be tackled. These are discussed in the following section.

**Key Challenges and their Possible Solution**

1. View-invariance is a key in determining the soft biometrics from the surveillance video. One should be able to identify the soft biometric from any view of the subject. This challenge can be partially solved by using view invariant features or predict features based on the partial observations.

2. Human descriptions are often erroneous due to: a. their subjective-ness; b. human psyche. Soft biometrics should be corrected using the known pattern in the human measurements to reduce...
error in their description.

3. Obtaining correct and detailed narrative is utmost important while searching on basis of the human description. Quantification of the soft biometric traits is extremely vital while searching the database. This is done by developing a vocabulary which maps semantic description to class or category. For example, description about height can be categorized as Very Short, Short, Medium, Tall and Very Tall. The observer can be asked to choose description amongst this category labels.

4. Statistical analysis determines performance of a soft biometric scheme and specifically, it is vital for determining discriminating abilities of the soft biometric traits. Many studies have been undertaken by the researchers and for most common traits, robust vocabulary is now available.

5. Fusing many biometric traits can lead to enhanced recognition accuracy but it is important to identify the most discriminating traits. It is also essential to identify weights given to each biometric traits while fusing them. However, traits can be identified based on the application context and availability of the side information.

6. Soft biometric features should be automatically detected during the time of recognition[11, 12]. This is the ultimate goal of the soft biometric based person identification system.

Conclusion
The goal of this article is to explore an idea of locating a person-of-interest based on specific set of soft biometric attributes from a surveillance video. This has an excellent application in digital video forensics. It is useful when subject is not previously registered i.e. the description is not available at the time of person identification. It is necessary to integrate and minimize semantic gap between human descriptions and soft biometric traits. Moreover, soft biometrics can also be used to solve slightly easier problem of person re-identification. It aims at extracting soft biometric features from an input image or a video frame and then use these features to locate a matching individual in the video stream. The idea is very exciting. It can add another dimension to digital video forensics by using human cognitive perceptions while searching the video streams.

Acknowledgement
The author would like to acknowledge Professor Mark S. Nixon, University of Southampton, U.K. for hosting author, invigorating discussions on soft biometrics and sharing his experiences in this domain.

References

About the Author
Dr. Mehul S [CSI - 00091380] is currently working as Associate Professor with Institute of Engineering and Technology, Ahmedabad University, Ahmedabad. He is an alumnus of College of Engineering (COEP), Pune. His research interests are in the areas of computer vision, digital watermarking, digital image forensics, soft biometrics. He is a CSI distinguished speaker for Region 3. He can be reached at mehul.raval@ahduni.edu.in.
Introduction

In recent time, virtualization technology has become one of the most important and popular technologies for individuals and companies. The virtualization technology introduced many advantages like cost benefits through decreasing number of physical machines required within an environment as well as best utilization of hardware resources such as storage, processing and computing resources. The virtualization technology will be the default option to the companies over the future. There are several companies providing and producing virtualization products such as VMware, Microsoft, Citrix, Oracle, Red Hat and many others.

New techniques and methods of cybercrimes against virtual environments are different from the classical techniques and methods which are used by attackers because the virtual environments have characteristics that differ from traditional IT systems. This makes digital investigators and examiners to think about designing and developing new techniques and tools to cope with these virtual environments to investigate new type of cybercrimes. Virtual Environment Forensics is the process of performing the digital forensics in virtual environment.

In the virtual environment, the users can run multiple virtual machines inside a single physical computer or server to reduce costs and best utilization of available hardware resources through the usage of virtualization technology. Virtual machine has become well known for enterprises and criminals. The enterprises get many business benefits and advantages from using the virtual machines. In the other side, criminals can use the virtual machines for illegal purpose by launching various types of attacks and performing illegal activities then deleting them without leaving any traces or evidences behind them. Digital forensics strategies, methodologies and techniques have to evolve to become efficient and effective to investigate these type of severe attacks and crimes in the virtual environments. This article discusses briefly about the digital forensic investigation process in the virtual environments.

Digital Forensics

Digital forensics is the process of collecting, extracting and recovery of digital evidence as an admissible proof about committed crime that will present it in the court of law. Digital forensic is defined at the first Digital Forensic Research Workshop (DFRWS) as: “The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations”. Digital forensic investigation process involves many essential steps such as identification, collection, analysis, examination and presentation as shown in Fig.1.

Virtualization and Hypervisors

Virtualization is a technology that enables and helps users to run multiple Virtual Machines (VMs) in the same single physical computer/server. The virtualization manager creates, manages and monitors these and simulates set of hardware such as hard disk, processor, memory, and other hardware components and software needed for each virtual machine. Hypervisor has various characteristics such as the hypervisor has full control of managing and monitoring system resources, providing an environment for programs to run as running in the physical machine and these programs that run in this environment have very little speed degradation compared with the physical machine (i.e. host machine).

There are two types of hypervisors which are Type-1 and Type-2 as shown in Fig.2. Type-1 is called Bare-Metal Hypervisor that installs directly on top of the physical machine and has direct access to resources, which makes its performance comparable to that of native execution. Type-2 is called Hosted Hypervisor that runs on top of an already installed standard operating systems such as Windows, Mac and Linux.
packages such as analysis of viruses and malware software without causing any problem for the surrounding virtual machines which are running in the same system or other systems that is running in the same network.

Virtual Environment Forensics

Virtual Environment Forensics is a cross discipline between virtual environment and digital forensics. Also, it can be defined as the process of performing digital forensic investigation of cybercrimes in virtual environment. The core element of the virtual environment is a virtual machine. In the digital forensic field, the virtual machine can be used in two cases as follows:

- **First Case**: To help digital investigators to perform the digital forensic investigation process by running suspected/compromised computer system in the virtual machine to test and extract digital evidence data about the committed crime.
- **Second Case**: The digital investigators can perform the digital forensic investigation process in the virtual machine itself by analyzing and extracting data artifacts as a digital evidence about the committed crime by or against the virtual machine.

In the virtual environment, performing the digital forensic investigation process requires new procedures and methodologies to collect and extract digital evidences in forensically sound way to be accepted as an admissible proof in a court of law about the committed crime. There are two types of investigations to collect the digital evidences from the virtual environment as follows:

1. **Investigation of Dead Virtual Environments**: In this type of investigation, digital investigators and examiners deal with virtual machine offline by acquiring hard drive of the virtual machine then performing investigation process to extract and analysis digital evidence which are collected from it.

2. **Investigation of Live Virtual Environments**: In this type of investigation, digital investigators and examiners deal with virtual machine online by acquiring volatile data of the virtual machine from memory which contains vital and valuable information that may help digital investigators to reconstruct an event about the committed crime.

Conclusions

In this article, digital forensics in the virtual environment is introduced. Virtual machines can be used by digital investigators and experts as a forensic tool for performing the investigation process. In addition to this, the digital investigation process can be performed in the virtual machine itself as digital evidence or a tool to launch attacks. Digital investigators and practitioners have to design and develop new strategies, methodologies and techniques for investigation of severe attacks and crimes in the virtual environments in timely fashion and forensically sound manner.

References


About the Authors

Mr. Ezz El-Din Hemdan is working towards his Ph.D. degree in Department of Computer Science, Mangalore University, Mangalore, India. His research area of interests includes: Virtualization, Cloud Computing, Digital Forensics, Cloud Forensics, Big Data Forensics, Internet of Things Forensics, Networks and Information Security and Data Hiding. He can be reached at ezzvlp@yahoo.com.

Dr. Manjaiah D.H [CSI-00002429], is currently working as a Professor in Computer Science Department at Mangalore University. He holds more than 23 years of academic and Industry experience. His area of interests includes: Advanced Computer Networks, Cloud and Grid Computing, Mobile and Wireless Communication. He can be reached at manju@ mangaloreuniversity.ac.in and drmdhm@gmail.com.

Dr. Vipin Tyagi, Guest editor 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 Cyber 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 serving CSI Communications as Guest Editor since May 2015 issue.

He is an expert in the area of Cyber Security, Cyber Forensics and Image Processing. He can be reached at drvipin.tyagi@gmail.com.
The Role of Cyber Forensics in Legal and Ethical Aspects of Cyberspace

Vijith T. K.
Research Scholar, Dept. of Computer Applications, Cochin University of Science and Technology, Cochin, Kerala

Abstract: Advances in technology lead people to a new space called cyberspace. It introduces a radical change in every span of society. Legal and ethical aspects of cyberspace are new problems before every government. To cope up such a situation, governments and stakeholders have to consider many factors such as legal validity of the transaction, ethical violations, preserving privacy of persons, data access right, harmful actions on internet etc. Cyberspace has opened new track for criminal activities that have different names like cyber defamation, password sniffing, identity theft etc. Government of India enacted a law (Information Technology Amendment Act)ITAA 2008 inorder to strengthen the existing law by adding sections covering the cyberspace. Rapid growth of cyberspace leverages the proliferation of cyber crimes in India. Use of advanced cyber forensics tools gives confidence to the law enforcement agencies for investigating cyber crimes. This paper suggests certain steps which need to be taken by the government, people, law enforcement agencies, public and private organisations for getting benefits of cyberspace for society; and discusses the role of cyber forensics in cyberspace.

Introduction

Cyberspace introduces a radical change in every span of society. This space is created with many active and passive components like computers, network devices, software, I/O devices and users that range from mobile phone/Smart phone to cloud servers. Legal validity of the activities on cyberspace and its affective use is a crucial issue before every government.

Flexibility, location transparency and a feel of confined room security motivates people to do anything what they can on cyberspace without bothering about legal and ethical aspects. This increases the rate of crimes in this area. Present crime statistics shows that for most of the crimes, criminals choose cyberspace as a tool. Depending on degree of involvement and effect cyber crimes can be classified into two categories(1) Computer crime (2) Computer related crime[1-2]. ITAA 2008 is a powerful law to govern cases and issues of Indian cyberspace.

Ethics is a philosophical approach dealing with what is to be considered good or bad? It is important to note that unethical is not always illegal. For example, government organisations and companies monitoring its employees email. In general, ethics in cyberspace is related to security, privacy, access rights, and positives and negatives of cyberspace. There are advances in the area of cyberspace to ensure legal and ethical aspects of it. Advanced cyber forensic tools can be used for handling of cyber crimes and ethical violations. How these efforts and cyber forensics tools can be used for effective utilisation of cyberspace is the topic of discussion.

This paper demystifies the terminology - Cyberspace, Cyber crime, Cyber forensics, Ethics in cyberspace. It briefly introduces cyber laws and its effects in Indian cyberspace by discussing cyber crime statistics. Then it discusses the role of cyber forensics in cyberspace and proposes certain suggestions for its effective utilisation.

Cyberspace

Formally, we can define “cyberspace is a time dependent set of interconnected information systems and the human users that interact with these systems”[3]. A set of intrinsic and extrinsic protocols govern this space. Intrinsic protocols are communication protocols like TCP, SMTP etc. and extrinsic protocols are ethics and laws enacted by government for communication and use. Almost all the people around the globe are benefited from cyberspace in one way or the other. Because of the advances in internet technology, the reachability of this space has grown rapidly. Social networking technology creates new groups in this space. The traditional computer users, technocrats, teachers, students and smart phone users all take major roles in this space.

The growth of internet, Mobile phone technology, smart phone users, technology enabled services, technology based jobs etc shows the importance of cyberspace, its use and indispensability. ‘Go digital’ is the slogan of every regime, where governance is fast moving from traditional to e-governance and m-governance; And every domain is now being transferred to digital domain. With this explosive growth, the major issue here is the security of cyberspace and its use to promotion of ethical use of the cyberspace.

Cyber Crime

Computer and computer networks are the backbone of the cyberspace. Increased dependency on cyberspace increases cyber crime. In general it can be said that cyber crime is “any unlawful or unethical act performed in cyberspace”.

Based on the victim of the cyber crime it can be classified as[1].

1. Against Property: Crimes on financial transactions, online money laundering, data theft, email fraud etc.
2. Against Intellectual Property: Copyright violation
3. Against person: Identify theft, cyberstalking, online defamation
4. Against nation: Cyber terrorism

The objective and motive of the persons who commit crime (Cyber criminals) on cyberspace is different. Cyber criminals can be classified into three types[4].

1. Type I: Aim for recognition and popularity (e.g. Terrorist
2. **Type II:** For Intellectual joy (not interested in recognition) (e.g. psychological perverts)

3. **Type III:** For revenge (e.g. former employee of organisation seeking revenge)

Email spoofing, phishing, spamming, cyber defamation, cyber-stalking, computer sabotage, pornographic offences, password sniffing, credit card crimes, intellectual property crime, Internet time theft, denial of service attack, virus attack, email bombing, salami attack, logic bomb, trojan horse, data diddling, industrial spying, computer network intrusion, software privacy, forgery, cyber terrorism, web jacking, identity theft, unauthorised access of computer, morphing, image doctoring, hacking, online fraud etc. are the various types of cyber crimes in the cyberspace.

**Laws Governing Cyberspace**

In the past decade, business organisations began to reap the benefits of Information Technology. They perform their business transactions on the internet that obviously speeds up the movement of business. Because of the widespread acceptance of technology-based transactions and communications, the governments have taken-up legal validity of this.

The United Nations Commission on International Trade Law (UNCITRAL) has framed a model law on E-commerce in 1996. Later the United Nations general assembly in 1997 has recommended all nations associated with it to consider this model law for policy creation.

The parliament of India has passed the Information Technology Act 2000 (ITA 2000), which came into force on 17th October 2000. The act mainly focuses on handling legal validity of electronic transactions, digital signatures and cyber crimes. Even in the presence of ITA 2000, cyber crimes rely on Indian Penal Code 1860 for its legal validity. This act was inadequate to handle new developments in technology and cyber crimes. Under these circumstances, debates and discussions on ITA 2000 lead to an amendment of it; resulting in the Information Technology Amendment Act 2008 (ITAA 2008).

Table 1 is the summary of sections 66 and 66 A to E of ITAA 2008. From these details it can be understood that most of the innocent activities on cyber space is unethical and may become cyber crime. In many cases which are committed because of the lack of awareness of the law and its consequences.

The latest advancement in this area is that in March 2015, the Supreme Court of India struck down the 66 A of ITAA 2008 by stating that it is unconstitutional. There are many negative comments on ITAA 2008, even though it addresses most of the ethical violations and legal validity of the technology enabled services.

**Cyber Crime Statistics in India**

As the population rate of India is increasing, crime rates are also increasing. Figs. 1 and 2 show the last ten years crime statistics in India. Reports of cyber crimes appear frequently in the media.

Cases reported and persons arrested for cyber crime in 2014 is 12248. 5548 cases are under computer related offences (sections 66 and sections 66 A to E).

Figure 3 shows an alarming data about Indian cyberspace, the rate of increase in cyber cases registered under the ITAA 2008 in last five years. Cases related to cyber crimes not only come under ITAA 2008 but also under IPC and SLL (Special and Local Laws) in India. For example, cyber defamation is a cognizable offence. In law, the term defamation is defined in IPC section 499. So it will be accounted under IPC.

**Cyber Forensics**

Cyber forensics is a comparatively new branch in the area of information technology. The term forensics means the scientific procedures and techniques are systematically used for investigating...
Moreover, these are agreeable to the court of law. Synonyms of cyber forensics are computer forensics, digital forensics science and digital forensics. This is a branch of forensics science that deals with the investigation on digital devices. Initially the techniques used for recovering deleted information from digital devices referred to as digital forensics. Later, it is specialised for various areas such as the following[1, 4, 11, 12].

1. Hardware/Memory forensics: recovery of data from storage media
2. Network forensics: recovery and analysis of information distributed in computer networks
3. Device forensics: recovery and analysis of information from hand held devices like PDA
4. Mobile phone forensics: recovery and analysis of information from mobile phone
5. RAM forensics: recovery and analysis of data from primary storage media (live data recovery)
6. Cloud computing forensics: recovery and analysis of data from cloud
7. Email forensics: recovery and analysis of email etc.
8. Image forensics: detection of image forgery and its analysis.

Today there are many sophisticated and specialised proprietary and non-proprietary tools available for cyber forensics. EnCase, FTK (Windows operating system based and proprietary) and CAINE Linux (Linux operating system based and non-proprietary) are the examples of multi purpose cyber forensics tools[11, 12]. After the enactment of ITA 2000, the courts in India are accepting the reports generated by these tools as evidence in cyber crime cases.

### Ethics in Cyberspace

The state of mind determining what is right and wrong is called ethics[13]. Being ethical means behave like what the law demands. Ethics is actually meant for acceptable, safe and responsible behaviour in everyday life. Association of Computing Machinery (ACM) has proposed commitments to ethical professional conduct, a new policy on professional ethics[14].

Domains like medicine, government services, education etc have been following a policy on ethics. Since 1992 in USA, accredited universities in their computing sciences curricula include mandatory instructions in the social and ethical effect of information technology. Their national agencies are following a professional ethical policy in cyberspace[13].

### Role of Cyber Forensics in Cyberspace

Why we need ethics in cyberspace? Consider a situation; no one will not be ready to place vulgar or defaming argument about a person in public. Because people know that, it is against ethics or it may become a crime. But they are ready to do that on the social media. If a person who sits in front of computer in a confined room posts a bad or defaming statement about a person is a crime or ethical violation. People have a feeling that, if they are in a confined room with a computer or a smart phone and

<table>
<thead>
<tr>
<th>Section</th>
<th>Crime</th>
<th>Punishment</th>
</tr>
</thead>
<tbody>
<tr>
<td>66</td>
<td>Computer Related Offences specified in section 43</td>
<td>Imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both</td>
</tr>
<tr>
<td>66A</td>
<td>Sending offensive messages through communication service</td>
<td>Imprisonment for a term which may extend to three years and with fine</td>
</tr>
<tr>
<td>66B</td>
<td>Dishonestly receiving stolen computer resource or communication device</td>
<td>Imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.</td>
</tr>
<tr>
<td>66C</td>
<td>Identity theft</td>
<td>Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.</td>
</tr>
<tr>
<td>66D</td>
<td>Cheating by personation by using computer resource</td>
<td>Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees</td>
</tr>
<tr>
<td>66E</td>
<td>Violation of privacy</td>
<td>Imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both</td>
</tr>
</tbody>
</table>

**Table 1: Summary of Section 66 and 66 A to E of ITAA 2008**
do anything in the cyber space, it will not create any problem to them. But the reality is entirely different. Actually all activities they do on the system is recorded somewhere. Any action on internet will recorded in many locations, that are systems browser history, operating systems registry, internet service providers log file, service providers (email, social media) log file etc. With the advancement in cyber forensics, every action can be traced out and all information can be recovered. A detailed report can be generated from cyber forensics tools for the case it was investigated; And this will be an accepted document in court of law. So it is essential that users of cyberspace must know what is right and wrong. What are ethical violations in cyberspace?

Presently in research and academic community faces serious issue of intellectual property right violation, mainly plagiarism. Plagiarism is unethical and may become a crime. There are many software tools for detecting plagiarism.

The basic ethical issues in cyberspace are personal privacy, data access right, and harmful action on the internet. The major ethical violations that contributed to cyber crimes in Indian context are[7-10]:

1. Cyber defamation: The term defamation is mentioned in IPC as “Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person”[11]. If it takes place in cyberspace then it is a cyber crime

2. Internet time theft: Unauthorised access of a person’s paid internet time by another person using ISP user ID and password.

3. Forger: Manipulation or creation of legal documents like stamp paper, mark sheets, certificates etc.

4. Web jacking: Forcefully take control of someone owned website by cracking password

5. Hacking: The act breaking any kind of security for accessing computer and/or computer network.

6. Software piracy: Access, use, copy and distribution of software by dishonouring its copyright

7. Identity theft: Using another person identity for illicit purpose

It is impractical to limit all ethical violations in these categories only. Ethical borders are narrow and it is highly complicated to define them in a rigid manner.

**Discussion and Conclusion**

Cyber space opened a new horizon to the world. It is necessary to understand security, privacy issues, positive and negative impact of cyberspace. The majority of users of the cyberspace are youngsters. In India, most of cyber criminals are below 45 years[9, 10], following Suggestions are made:

1. Framing a professional cyber ethics policy by government and organisations.

2. Inclusion of Cyber ethics in academic curriculum.

3. Conducting awareness programs on legal and ethical aspect of cyberspace in public domains.

4. Mentioning a statutory warning on illicit material present in cyberspace.

5. Restricting access right of websites for intended users.

6. Taking steps for including plagiarism as a topic in research community.

7. Including a warning pop-up in social media while users upload materials (especially multimedia contents).

8. Developing a professional and advanced procedure to be used by law enforcement agency for the investigation of cyber crimes.


10. Wider media publicity about cyber crime cases and its consequences.

**References**


**About the Authors**

Mr. Vijith T. K. [CSI -11503994] is currently a research scholar in cyber forensics (UGC-JRF) at Department of Computer Applications, Cochin University of Science and Technology (CUSAT), Cochin, Kerala. He is working as Assistant Professor at College of Engineering Vyttila (now on study leave). He has more than 10 years of teaching experience. His area of research is cyber forensics specifically digital image forensics. He is a consultant of law enforcement agencies and judiciary in the area of cyber forensics. He can be reached at vijithtk@cusat.ac.in.

Dr. K. V. Pramed [CSI - 8001328] is working as Associate Professor at Department of Computer Applications, Cochin University of Science and Technology (CUSAT), Cochin, Kerala. He has 25 years of teaching and research experience, produced many PhDs and more than 100 publications in his credit. His research interests are Simulation Modelling, Mathematical Morphology, Cryptography, Image Processing and Cyber Forensics. He can be reached at pramod_k_v@cusat.ac.in
Overview of Digital Forensic Investigation

K. Nithya
Asst. Prof., Dept. of CSE,
Nandha College of Technology, Erode

M. Saranya
Asst. Prof., Dept. of CSE,
Nandha College of Technology, Erode

Background - Over the past few years computer crimes or misuse increased in a wide range, which includes an unauthorized modification or deletion of data on a computer system. The main purpose of digital forensics is to identify the crimes related to the computer. This includes recovering the deleted files and photos, searching unspecified memory on the hard drive, places where a plenty of data habitually resides, tracing artifacts, those little bit of data left behind by the operating system. Usually, experts know how to find these artifacts and, more importantly, they know how to evaluate the value of the information they find. In many cases computers contain evidence of a crime that took place in the real world. The computerization has made the evidence harder for investigators to analyze than paper records. The victims are identified for that investigators had few tools with which to make sense of data. In order to solve the problem most of the organizations are hiring digital forensic professional to identify the crimes.

Forensic is the process of gathering, protecting, and analyzing scientific proof during an inquiry. Digital forensics is a division of forensic art, the recovery and investigation of impression found in Digital Devices. The Digital Forensic examination is separated into several sub-branches, based on the type of digital devices like Computer, Network, data analysis, mobile device and database.

Computer Forensics - The aim of computer forensics is to make clear about the current state of digital devices; such as a computer system, storage medium etc., It analyze the unstructured data. It is very helpful to detect the crime which is related to computer. Computer forensic investigators check the authenticity, reliability, completeness and conformity.

Network Forensics - It deals with the computer network traffic analysis and monitoring in both local network and internet. It performs evidence collection, pre-intrusion detection and post-intrusion detection. Network forensic method helps to record the traffic, offer the ability to view the transaction also reconstruction of data.

Mobile Device Forensics - It is related to the identification of digital evidence or data from a mobile device. In this, mobile devices will have an internal communication system like GSM. Investigations mainly focus on call and communications information (SMS/Email) rather than recovery of deleted information.

Forensic Data Analysis - It inspects ordered data with the aim to determine and analyze patterns of false behavior resulting from financial crime.

Database Forensics - It related to the forensic study of databases and their metadata. Investigations use database contents and files to recover related information.

Investigative Mindset - An investigative mindset to interrogating multiple complex data sets, understands their content and its implications, and then presents the findings as evidence. It is also intended to give digital device examiners exposure to the multiple forensic tools now available, as well as insights into current and upcoming legislative procedures and best practice. An investigative mind-set in examining and obtaining data from a variety of devices use appropriate forensic tools and procedures to retrieve data.

Evidence Investigation Process

Evidence Acquisition - In this stage forensic specialist gather evidences or findings regarding crimes. Once the evidences have been identified then data is duplicated it is called as imaging or Evidence acquisition. This evidence acquisition specialist undergone various training for correct handling of evidences also they aware of evidence preservation. The duplicate is created using imaging tool or drive duplicator.

Evidence Analysis - The acquired evidences are analyzed using some notable online analysis tool like “Microsoft’s COFEE”. COFEE is Computer Online Forensic Evidence Extractor using this tool forensic investigators extract evidences from a computer. It is installed on some external disk drive then automatic analysis is performed using this tool. It performs following steps for analysis of evidences.

Step 1: External disk drive is connected to a USB port
Step 2: Devices is loaded with various tools for collecting the data
Step 3: Select the forensic data from a source computer
Step 4: Data is exported to a USB drive
Step 5: Analyze

This tool performs the tasks like history recovery, data recovery from volatile memory and decryption of file from a computer. Also an unofficial group has developed a tool DECAF against this COFEE. DECAF is “Detect and Eliminate Computer Acquired Forensics”, it performs tasks against COFEE like log clearing and USB ejecting. It creates awareness on security.

Evidence Reporting - When investigation is completed all the informations are recorded and reported. It contains conclusion for the crime. Using COFEE report is generated.

Advancements in Digital Forensics

Advanced Smartphone forensics - is one of the major advancements in digital forensic. This helps the investigators in an easier way than ever for investigators to acquire physical evidence from these devices. There are number of tools available that allow investigators to connect a digital device and retrieve raw
image files by simply pressing a button or accessing the device’s internal memory prior to boot-up.

**Advanced network forensics** - Network connectivity is no longer a complicated computing requirement. The explosion of network connectivity has also generated a corresponding increase in the use of that same connectivity for malicious purposes. While defensive and preventative measures have helped to thwart countless attacks. The fundamental tenets of an investigation remain consistent regardless of the domain being examined. Network forensics provides even greater evidence collection potential, but introduces some unique challenges that an investigator must understand and address to provide meaningful findings.

**Conclusion**

Though Digital Forensics is the widely used method of effective investigation of crimes, the internet crimes are continuously growing day by day. Because of continuing growth of internet crimes, the legal community can no longer ignore the challenges.

**References**


---

**About the Authors**

**Ms. K. Nithya** [CSI-11502370] is currently working as Assistant Professor in the Department of Computer Science and Engineering at Nandha College of Technology, Erode. Her area of specializations are Image Processing, Biometrics and Cyber Security. She can be reached at nithya.k@nandhatech.org.

**Ms. M. Saranya** [CSI-11502379] is currently working as Assistant Professor in the Department of Computer Science and Engineering at Nandha College of Technology, Erode. Her areas of interest are Image Processing and Data Mining. She can be reached at saranyamcse88@gmail.com.

---

**Computer Society of India**

Unit No. 3, 4th Floor, Samruddhi Venture Park, MIDC, Andheri (E), Mumbai-400 093
Tel. 91-22-2926 1700 • Fax: 91-22-2830 2133
Email: hq@csi-india.org

**CSI - Communications**

<table>
<thead>
<tr>
<th>COLOUR</th>
<th>Colour Artwork (Soft copy format) or positives are required for colour advertisement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back Cover</td>
<td>Rs. 50,000/-</td>
</tr>
<tr>
<td>Inside Covers</td>
<td>Rs. 40,000/-</td>
</tr>
<tr>
<td>Full Page</td>
<td>Rs. 35,000/-</td>
</tr>
<tr>
<td>Double Spread</td>
<td>Rs. 65,000/-</td>
</tr>
<tr>
<td>Centre Spread (Additional 10% for bleed advertisement)</td>
<td>Rs. 70,000/-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MECHANICAL DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Page with Bleed</td>
</tr>
<tr>
<td>Full Page</td>
</tr>
<tr>
<td>Double Spread with Bleed</td>
</tr>
<tr>
<td>Double Spread</td>
</tr>
</tbody>
</table>

**Special Incentive to any Individual/ Organisation for getting sponsorship** 15% of the advertisement value

**Special Discount for any confirmed advertisement for 6 months** 10%

**Special Discount for any confirmed advertisement for 12 months** 15%

All incentive payments will be made by cheque within 30 days of receipt of payment for advertisement.

All advertisements are subject to acceptance by the editorial team.

Material in the form of Artwork or Positive should reach latest by 20th of the month for insertion in the following month.

All bookings should be addressed to:

**Executive Secretary**

Computer Society of India

Unit No. 3, 4th Floor, Samruddhi Venture Park, MIDC, Andheri (E), Mumbai-400 093
Tel. 91-22-2926 1700 • Fax: 91-22-2830 2133 Email: hq@csi-india.org

---

**ADVERTISING TARIFF**

Rates effective from April, 2014

---

---
What if there was no internet or mobile technology? Imagine not being able to talk to your loved ones for months? How would you google about your problems? Or how would you Youtube your favorite videos? Not only these micro benefits but macro features like e-commerce, infrastructure, electricity, transportation, banking, etc. all would collapse as they all banked on the internet.

Reasons like these and many more important reasons that are well beyond our comprehension (like nuclear facility integrity), establish internet as the most valuable asset of our planet! And safeguarding it has become the unanimous agenda of governments all over the world.

"Cyber security is giving sleepless nights to the heads of states of nations across the world. Is it not possible for us to create a foolproof mechanism against cyber threats so that the world can sleep well" says Indian PM Narendra Modi.

Every now and then we read in newspapers about accounts being hacked or groups like Anonymous declaring Cyberwar against ISIS. But is it real? The fact is, situation is much worse in the Cyber world. Howard Shrobe, Director of Cybersecurity at MIT says "There are two kinds of companies today. Those that have experienced a security breach and those that don't know it yet."

The sophistication of attacks is rising insanely with the skills required to do it falling even faster. But "Why is hacking so easy and security so hard?" Hackers like Wakelam say "The defenders trying to secure the computer networks have to close off every possible vulnerability. They have to get everything right, every time. The attackers just have to find one mistake."

Digital Forensics is the need of the hour. Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.

A Digital forensic expert is like the WBC of the internet's immune system. The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved: computer forensics, network forensics, forensic data analysis and mobile device forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence.

Digital forensics unlike the real world forensics much more complex and extremely challenging. Internet, not being a monopoly of any country is very hard to tame under common laws. Hackers use proxy servers to exploit this vulnerability which makes back tracing impossible. Also challenges like vastness of data at incident site and lack of skills to analyse it pose a major challenge in this field. Joe Franzi, who heads up the Cyber Security Branch of Australia—says part of the problem is a skills shortage. 'The demand for cybersecurity professionals is insatiable at the moment, and this is not just an Australian problem. It's a global problem,' he says.

Prevention is better than cure. More than 90 percent of the attacks occur because of not following common security practices like changing passwords regularly, connecting to a trusted network, downloading untrusted files, etc. While a common netizen can safeguard himself to some extent by following secure internet practices, however the world certainly needs a swarm of security professionals to fight the crisis that if not catered to, might prove to be catastrophic!
Introduction

Today is an era of globalization. The rapid advancement in technology has made computers a tool for communication, data storage and processing. Our life is incomplete without computers and computer networks. It influence our lives from daily basic chores like shopping, sharing information, communication and more specific important services like banking, business etc. As computers are the need of hour and provide us numerous benefits but it also act as a tool in hands of criminals to commit cyber crimes. Cyber crimes are the biggest challenge today. Various types of cyber crimes like hacking, fraud, defamation, credit card cloning, software piracy, SPAM distribution, virus/Trojan distribution, unauthorized use of personal information, pornography, obscene publication, perjury, forgery, sexual harassment, e-mail spoofing, e-mail bombing, phishing, denial of service attacks (DoS), cyber terrorism, data theft, industrial espionage etc., are on rise. Cybercrime is a crime in which digital devices like computers, communication devices and networks can be used as a medium to commit crime and it is harder to stop and detect these cyber crime related activities. To tackle these activities and punish criminals in court of law, a new field has evolved called as Digital Forensics.

Digital Forensic Process

Digital forensics is defined as a process used to identify, preserve, extract, analyze, validate, interpret, document and present the digital evidence. This process is carried out by using proven methods and techniques in such a way that the evidence so collected is admissible in court of law. This process further facilitates the reconstruction of events to punish the culprits. Actually, it is considered as a branch of cyber forensics that deals with investigation and recovery related to digital devices involved in computer crimes. It is generally considered as synonym for computer forensics but includes all digital devices capable of storing digital data. So Digital forensics not only covers computers but all digital devices meant to deal with digital data like networks, mobiles, laptops, PDAs, USB drives etc.

Further, Digital Forensics is broadly categorized into Computer Forensics, Network Forensics and Mobile Forensics depending upon the type of digital devices involved in investigation.

Phases in Digital Forensics:

Digital forensics rapidly emerged in last few years as a new field to counter cyber crimes and prosecuting criminals. Prior to the existence of this proven methodology, tools and techniques, many crimes left unsolved. Digital forensics is a process and there are various points the investigators have to keep in mind while investigating the case. The most important point to keep in mind is that the evidence extraction is performed in such a sound manner so that it can be admissible in court. For this purpose certain steps must be follow in particular order. Various researchers and practitioners proposed various frameworks for digital investigation purpose but generally the below given steps are followed while performing digital forensics:

- Identification
- Preservation
- Extraction
- Interpretation
- Documentation
- Presentation

Identification

It is the initial phase, in which an investigator identifies the devices or containers which possibly contains crime related evidence such as hard-disks, floppy drives, USB Drives, RAM etc.

Preservation

Before performing any forensic analysis, forensic investigator must preserve original data and media. Analysis cannot be directly performed on original media but first we make a forensically sound copy or image of original device containing data and then perform the task of analysis on this forensic copy.

Extraction

In this phase, we extract the evidence pertaining to be found relevant according to the investigation in hand from the forensic image of media.

Interpretation

In this phase, the investigator interprets or relates the extracted information with the crime and culprit. Extracting information is one thing and properly interpret it according to particular investigation is altogether different thing. Many tools are available to analyze the media and extract information but to relate this information with crime is a daunting task that not only needs tools and techniques but expertise and experience too.

Documentation

This phase is going in parallel to other phases that are carried from the start to the end of investigation process. This step is used to create documentation; we called as chain of custody i.e. all the complete documentation/report pertaining to what steps have been taken, tools and techniques used during the whole process especially while performing extraction and analysis of the evidence. This documentation helps the investigating team to present their case in court strongly. In court the investigators have to authenticate and validate the various tools/techniques used during the steps/processes followed during investigation on demand.

Presentation

In this phase, the investigating team presents their findings or results in a standard format and produce the same before court or some other legal authority. The results, reports and evidences etc. must be based on some proven methodology, tools and techniques that can reproduce the same results when required on demand by court. The evidence produced must be authentic and admissible in court.

Digital Forensics is not only concerned with the evidence, computer or digital containers of evidence but also with the forensically sound procedure, tools, techniques used and legal proceedings. The whole process must be performed in lawful manner and must...
take care of chain of custody to prove every aspect of the investigation in court with reliability and authentication otherwise the evidence may not be admissible in court.

Goals
The primary goals of Digital Forensics are as follows:

- Identification of criminal and unauthorized activities that is not permissible under law in a given state.
- Preserving, extracting, storing, analyzing and presenting the evidence in a lawful manner.
- To gain insight into criminal activities and techniques used by criminals to perform cyber crimes and make system more secure by proposing methods and techniques to counter crimes. This not only helps in prosecuting criminals in court but also helps in reducing crime in future.

Challenges for Digital Forensics
Various issues need to address during Digital Investigation process are as follows:

Different Media Formats and Devices:
A variety of devices, from different vendors, is available in market. Similarly, different formats for data storage and communication are defined. So, it is not possible for a single forensic examiner to have expertise in all. With time more and more formats for image, text data, video and audio file formats are available to use. Further, various types of operating systems and hardware architectures adds in problem.

Media Volume: In earlier devices, the size of storage media, like hard-disk, were small in size but with time its size increased gradually. Now a day, Tera bytes of data is a normal thing. With growing size, it takes more time to create and analyze forensic images. This delays the investigation process.

Encryption: Encryption refers to the process of encoding information and messages with help of keys/passwords such that only the persons having access to keys can read the message. Many efficient encryption algorithms are available. In addition, the tools like TrueCrypt are available to encrypt the data. Even full encryption of a disk is possible. Moreover, sometimes, it is easier to recover data during forensic process but it can’t be interpreted or further processed due to non availability of encryption passwords.

Steganography: Steganography is a technique used to hide a message so that it could not be detected or used by an unauthorized person. Text, file, image or video can be concealed within another message, file, image or video. Steganography poses a big challenge for digital forensic practitioners.

Anti Forensics: Digital Forensics is a set of techniques used to collect and analyze the evidences to punish culprits. To escape themselves, the criminals are using anti-forensic techniques. The overall purpose is to counter and forestall the digital investigation process and continue illegal activities. The example is the use of an artifact wiping technique that erase the potential data and traces of criminal activities from the system.

Acquisition and Analysis of Live Systems: In traditional digital forensics process, examiner first shutdown the system by removing the plug or through proper shutdown mechanism. In both cases, the potential evidences like system state, recent open process list, traces of malwares and anti-forensic activities, unencrypted data etc. reside in volatile memory are lost. Some time, it is not possible to shutdown the system. So in both scenarios, live acquisition of evidence and analysis is required on running system. This process of live data acquisition is also a difficult task in context of forensic procedure as the memory state of a working system change continuously. Second, the tools used for acquisition and analysis may also affect the memory and can overwrite potential evidence present in memory. Further, the malicious softwares and anti-forensic softwares can interfere and manipulate the investigation results.

Lack of availability of proper Tools and Expertise: Digital forensics field is a new field. There is lack of available standard tools, procedures and/or methodologies to deal with criminal activities. In addition, there is a vast number of devices, data formats, softwares and operating systems present in market and a single tool and/or technique is not perfect for all. The investigators need to update all these regularly. Similarly, a single investigator can’t have full expertise in all such techniques. Hence, there is dire need of hour to train the experts in field.

Legal Issues: Several legal issues roadblocks the investigation process. A cybercrime can happened on Internet that can extend beyond the jurisdiction boundary of a state. The different states have different law and legal procedure. An activity may be legal in one country but illegal in another. For example pornographic sites are allowed by some countries but are not allowed in another. As technology is growing very fast. The new systems give birth to new crimes too. There is no proper law defined to tackle with such crimes and punish the criminals. The progress is going on and the legal procedure is in process to get mature corresponding to cyber crime.

Conclusion
Digital forensics is required to counter cyber crime, unauthorized activities in cyber space and punish the culprits through legal process. Cybercrime is much more disastrous and have vast effect than traditional crimes. Digital Forensics is a new field and gaining maturity with time and can be used efficiently to produce evidence in lawful manner to punish criminals and to counter criminal activities. Since, the crimes are on rise with the use of digital technology and any one can be victim of it. Such rise in crime can be tackled with the use of digital forensics. Some tools and techniques are available but much more is required to be done to boost the digital forensics.

About the Authors

Mr. Dilpreet Singh Bajwa is a Research Scholar at Department of Computer Science and Applications, Panjab University Chandigarh and currently works with CGC, Landran, Mohali, Punjab. His areas of interests include Cyber Forensics, Digital Forensics, Volatile Data Forensics and Cyber Security. He can be reached at pu.dilpreetbajwa@gmail.com.

Dr. Satish Kumar [CSI - I1501531] is Associate Professor in Department of Computer Science and Applications in Panjab University (PU), Chandigarh (India), currently posted at Panjab University SSG Regional Centre, Hoshiarpur, Punjab, India (a multi faculty prestigious campus of PU). He has more than fifteen years experience of teaching post-graduate classes. His areas of interest are Image Processing, Pattern Recognition, computer graphics and Artificial Intelligence. He can be reached at satishnotra@yahoo.co.in.

About the Authors

Mr. Dilpreet Singh Bajwa is a Research Scholar at Department of Computer Science and Applications, Panjab University Chandigarh and currently works with CGC, Landran, Mohali, Punjab. His areas of interests include Cyber Forensics, Digital Forensics, Volatile Data Forensics and Cyber Security. He can be reached at pu.dilpreetbajwa@gmail.com.

Dr. Satish Kumar [CSI - I1501531] is Associate Professor in Department of Computer Science and Applications in Panjab University (PU), Chandigarh (India), currently posted at Panjab University SSG Regional Centre, Hoshiarpur, Punjab, India (a multi faculty prestigious campus of PU). He has more than fifteen years experience of teaching post-graduate classes. His areas of interest are Image Processing, Pattern Recognition, computer graphics and Artificial Intelligence. He can be reached at satishnotra@yahoo.co.in.
Purity of Clusters: Kernel K-Means and Beyond

Pranab Kumar Das Gupta  
Scientist ‘F’, Proof & Experimental Establishment  
DRDO, Chandipur

Bindu Patnala  
Research Scholar, Proof & Experimental Establishment  
DRDO, Chandipur

Asit Kumar Sahu  
Junior Research Fellow, Proof & Experimental Establishment, DRDO, Chandipur

Abstract: A clustering method is considered successful if it gives high quality clusters that have high intra-class similarity and low inter-class similarity. Purity is an external criterion for measuring clustering quality. Purity of cluster quantifies the extent that cluster contains points only from one (ground truth) partition. The methods reviewed in the paper are, Kernel K-Means, DBSCAN, CURE, and CHAMELEON that were developed after the widely used K-Means. This paper highlights the limitations of K-Means and how they are handled by the other methods. The objective of this paper is to present complex clustering algorithms, their advantages and disadvantages in a lucid manner.

Introduction

One of the most widely used terms and studied problems in data mining theory is clustering. Cluster analysis involves grouping similar objects into one cluster and dissimilar objects in another cluster. Unlike classification, clustering is learned by observation, rather than learning by examples. The uses and application of cluster analysis is far and wide. It ranges from market research, management, pattern recognition, data analysis, image processing etc. As a data mining function, cluster analysis serves as a tool to gain insight into the distribution of data to observe characteristics of each cluster. Different clustering aspects may be considered more significant depending on the application domain. The different types of data that is seen during cluster analysis are numerical, categorical, text, multimedia, time-series, sequence, stream, graphs and homogenous networks, heterogeneous networks, uncertain data and big data. Good results are often dependent on the data and algorithm chosen. In data mining and statistics, connectivity based clustering is known as hierarchical clustering. This clustering is based on the idea that nearby objects are more related than the one located farther away. The clusters are represented with the help of a dendogram. This method of clustering does not require specifying the number of clusters and is more deterministic. Two noteworthy hierarchical algorithms are, AGNES (A(lglomerative) N(ESTing) and DIANA (Divisive Analysis) developed by Kaufmann and Rousseeuw.

Related Concepts

Proximity measure usually refers to either similarity or dissimilarity. The most frequently used proximity measure is the Minkowski distance. Some special cases of Minkowski distance are Manhattan distance, Euclidean distance and Supremum distance. Euclidean distance is the most followed proximity measure in clustering. As an unsupervised learning task, it is necessary to find a way to validate the goodness of partitions after clustering. Clustering validation is the evaluation of goodness/ purity of clustering results, and helps in determining the clustering tendency of a set of data. It also helps in comparing the results of a cluster analysis to externally known results. External measures compare a clustering with prior or expert-specified information. One subtype of external measure that is highlighted in the subsequent section is purity. Purity is the percent of the total number of objects (data points) that were classified correctly. In case of purity, the values lie between 0 and 1. Purity of 0 is the lowest and a purity of 1 is the highest. Closer the value of purity to 1 implies that the data objects are alike and lower the values implies low purity.

K-Means

One of the extensively used partitioning methods is K-Means algorithm. MacQueen, & Lloyd put the term forth. The first step in this iterative process involves selecting K points as initial centroids. Formation of clusters using the K points as centroids constitutes the second step. The centroids of each clusters is recomputed in the third step. The second and third step is repeated until convergence is attained. K-Means algorithm is popular for its implementation ease and computational efficiency. The applications of K-Means algorithm are far and wide. Due to its effortless application, endeavor in mastering clustering algorithm ends with K-Means algorithm most of the time. In the subsequent section we will explore the limitations of K-Means algorithm and how they are overcome.

Limitations of K-Means

One major limitation of K-Means algorithm is that it does not work well with non-convex clusters and outliers. When all the points on a given line lie entirely within the cluster, it is known as a convex cluster. Conversely, in a non-convex shaped cluster, all the points on a given line lie do not fall entirely inside the cluster. In addition, the need to specify the number of clusters in advance is another major limitation of K-Means. As, initialization in K-Means clustering is an important phenomenon K-Means++ was developed. K-Means algorithm requires supervision from the user to specify the number of cluster centers unlike other algorithms. Different initializations can result in different number of final clusters. Lack of proper supervision during the initialization of clusters would result in erroneous clusters as seen in Fig. 1.b & 1.d.

Fig. 1c demonstrates how K-Means algorithm produces clusters of convex
shapes with great accuracy and high purity from the original data set. However, this cannot be held true for non-convex shaped clusters. In case of non-convex shaped data the resulting cluster would be of low purity, as the algorithm would try and produce convex shaped clusters thus distorting the data. To overcome this problem faced by K-Means clustering, other methods such as K-Medoid, K-Median, and K-Mode have been introduced, with not much success. To overcome the disadvantages in the previous sections four different clustering algorithms, namely, Kernel K-Means DBSCAN, CURE, CHAMELEON are pictorially illustrated in this paper. The benefits and shortcomings of these algorithms are compared with respect to the purity of cluster and K-Means algorithm in the succeeding sections.

**Kernel K-Means**

Kernel K-Means was introduced to handle non-convex clusters that cannot be performed by K-Means algorithm. Here points are mapped onto a high-dimensional kernel space using a nonlinear function, and K-Means clustering is then performed. While high purity cluster is obtained from the original data, as depicted in Fig. 2, Kernel-K Means has high computational complexity when compared with K-Means. In Fig. 2 it can be seen that the raw data (Fig. 2.a) has non-convex clusters and Fig. 2.b represents the clusters that is perceived as the end result by the human. When K-Means algorithm is applied on the original data set the resulting clusters are convex in shape that are of low purity (Fig. 2.c). Kernel K-Means has however, produced clusters of high purity and retained the non-convex shape of the clusters (Fig. 2.d). This concept can also be proved mathematically by computing the purity of clusters. In case of Fig. 2.c the purity of red colored cluster is 0.41 and the purity of blue colored cluster is 0.26. Purity of the red colored cluster has diminished as the K-means algorithm tried to form convex clusters by accumulating data points from the blue colored cluster, thus compromising the purity of both the clusters. In Fig. 2.d however, the Kernel-K Means algorithm has successfully formed one convex and one non-convex cluster of high purity of value 0.99.

**DBSCAN**

A Density-Based Spatial Clustering of Application with Noise (DBSCAN) is a well-known density based clustering that majorly helps in determining clusters of arbitrary shape. DBSCAN is one of the most common clustering algorithms and also most cited in scientific literature. Given a set of points in some space, it groups together points that are closely packed (points with many neighbors), and marks the points that lie alone in low-density regions (whose nearest neighbors are too far away) as outliers. Since, DBSCAN uses a density-based definition of a cluster, it is relatively resistant to noise and can handle clusters of arbitrary shapes and sizes. In Fig. 3, it is seen that applying K-Means algorithm on the original data has produced concave clusters without ignoring the noise; resulting in low purity clusters (Fig. 3.c). The purity of red color cluster is 0.43, green color cluster is 0.57 and blue color cluster is 0.58 respectively. However, DBSCAN accurately handled the noise and produced clusters of high purity (0.99) (Fig. 3.d). In addition, the number of clusters need not be predetermined as opposed to K-Means algorithm. However, DBSCAN cannot produce clusters of varying densities. Also, dealing with high-dimensional data becomes difficult, as density is more difficult to define for such data.

**CURE**

Clustering Using Representatives (CURE) is an agglomerative algorithm where clusters are formed using a set of well-scattered representative points. Initially a constant number of well-scattered representative points of a cluster are chosen. The points chosen are then shrunk towards the center by a fraction. The points after shrinking are used as representative points of cluster. Finally, merging the closest pair of representatives at each step forms clusters. Therefore, CURE algorithm enables in identifying arbitrarily shaped clusters accurately and makes it less sensitive to outliers. However, CURE fails to take into account special characteristics of individual clusters, and can thus make incorrect merging decisions when the underlying data does not follow the assumed model, or when noise is present.

**CHAMELEON**

In case of CHAMELEON, clusters are merged if the inter-connectivity and proximity between two clusters are highly related to the internal interconnectivity and closeness of objects within the clusters. Primarily objects are clustered into a large number of relatively small sub-clusters using graph-partitioning algorithms. Subsequently, by applying agglomerative hierarchical clustering algorithm the genuine clusters are found by repeatedly combining these sub-clusters.

With respect to Fig. 4 it is observed K-Means algorithm would try and produce convex shape clusters thus distorting the original data leading to low purity clusters (Fig. 4.c). The purity value of red colored cluster is 0.77, blue cluster is 0.66 and the black colored...
CHAMELEON can find natural clusters of different shapes, sizes and densities in two-dimensional space as it vigorously adjusts to the diverse clustering model portrayed by the clusters. CHAMELEON can also discover natural clusters that many existing clustering algorithms fail to find (Figure 4.d). The only drawback of CHAMELEON algorithm is that it cannot be applied on high dimensional spaces.

Conclusion

There are various ways to assess the quality of the clusters formed. Purity is such measure to evaluate goodness of the clusters formed. In the present paper, we introduced K-Means algorithm followed by latest algorithms such as Kernel K-Means, DBSCAN, CURE and CHAMELEON and the complex theory has been presented in a lucid manner with the help of diagrams. Illustrations provided above will enable the reader for a better selection of clustering algorithm. Detailed literature of all the concepts and algorithm discussed in this paper is available in Internet.

Acknowledgment

The authors gratefully acknowledge the support of Sri R Appavuraju, Director, PXE, DRDO.

References


Institutional Membership Subscription Fee

(Academic and Non-Academic) w.e.f. 15.11.2015
(The membership period is on Rolling Year basis)

<table>
<thead>
<tr>
<th>Details of the Membership Categories</th>
<th>Period - Wise Membership Fee + Service Tax Extra, as applicable (in Rs.)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>01 Year</td>
</tr>
<tr>
<td>Institutional Members (Academic) With 03 free Nominees</td>
<td>6,000</td>
</tr>
<tr>
<td>Service Tax @ 14.5%</td>
<td>870</td>
</tr>
<tr>
<td>Total Membership Fee</td>
<td>6,870.00</td>
</tr>
<tr>
<td>Institutional Members (Non-Academic) With 04 free Nominees</td>
<td>10,000</td>
</tr>
<tr>
<td>Service Tax @ 14.5%</td>
<td>1,450</td>
</tr>
<tr>
<td>Total Membership Fee</td>
<td>11,450.00</td>
</tr>
</tbody>
</table>

Individual and Life Membership Subscription Fee

(The membership period is on Rolling Year basis)

<table>
<thead>
<tr>
<th>Membership Category</th>
<th>One Year (Within India)</th>
<th>Two Years</th>
<th>Three Years</th>
<th>Four Years</th>
<th>Life Membership</th>
<th>Special Life Membership Fee with 30% Golden Jubilee Discount (Valid upto 31.03.2016)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Membership Fee (Within India) (in Rs.)</td>
<td>Rs. 1000 + 14.5% Service Tax = Rs. 1145.00</td>
<td>Rs. 1800 + 14.5% Service Tax = Rs. 2,061.00</td>
<td>Rs. 2600 + 14.5% Service Tax = Rs. 2,977.00</td>
<td>Rs. 3500 + 14.5% Service Tax = Rs. 3,893.00</td>
<td>Rs. 10,000 + 14.5% Service Tax = Rs. 11,450.00</td>
<td>Rs. 7,000 + 14.5% Service Tax = Rs. 8,015.00</td>
</tr>
<tr>
<td>Total Membership Fee Outside India (Inclusive of Service Tax) (in USD)</td>
<td>USD $60</td>
<td>USD $110</td>
<td>USD $150</td>
<td>USD $180</td>
<td>USD $650</td>
<td>USD $435</td>
</tr>
</tbody>
</table>

About the Authors

Dr. Pranab Kumar Das Gupta [CSI-0005676] is Scientist ‘F’ in PXE, DRDO, Chandipur. He is Head of Computer, Met, Quality & Reliability, HR and Material Management. Dr. Das Gupta is first author of four books related to Computer Science, all published by PHI. The textbook entitled Database Management System Oracle SQL and PL/SQL (2/e) is formally included in the syllabus by more than 15 reputed Academic Institutions throughout India. He can be reached at: pkdasgupta@gmail.com.

Ms. Bindu Patnala, is presently working as a Research Scholar in PXE, DRDO, Chandipur. Her areas of interest lie in Application of Clustering concepts in management. She can be reached at bindu.90@gmail.com.

Mr. Asit Kumar Sahu is presently working as Junior Research Fellow in PXE, DRDO, Chandipur. He has completed his B.Tech in Computer Science from Biju Patnaik University of Technology, Rourkela. His areas of interest include Data Mining and Database. He can be reached at asitsahu39@gmail.com.
Digital Forensics and its challenges in Big Data

Sunita A. Yadwad
Asst. Prof., Dept. of CSE, Anil Neerukonda Institute of Technology and Sciences, Vishakapatnam

Introduction

In today’s times Digital Forensics is an integral part of Forensic Sciences. What is Digital Forensics? Digital refers to the representation of physical value in terms of binary digits. Whereas Forensics refers to tests or techniques used in connection with an investigation of a crime.

Forensics is a Latin Adjective which means before the Forum. Ancient Roman Society solved cases involving criminal offenses by presenting the stories of victim and the suspects before the Forum and determining the outcome based on the best argument. The idea of using Science to fight against crime was common in the late Middle Ages, but became prevalent only after the frequency of human poisoning spread across Europe and the detection was difficult due to the similarities it had with other infectious diseases. This led to the beginning of analyzing the corpse for toxic substances or other causes of the death.

Forensic Science has gained high popularity by authors such as Sir Arthur Conan Doyle, whose infamous character Sherlock Holmes increased the awareness of the Science and curiosity among people in investigation stories of crime. This led to the evolving of a new Science altogether called Forensic Science and a new generation of Expert called Forensic Science Experts. But how did the term Digital forensic get coined? With the roots of computer revolution in the late 70s and early 80s of the Twentieth century the Discipline evolved in a much haphazard manner in the 90s and in the early 21st century the National policies emerged. The Federal laws began not only considering the Computer offenses like child pornography, cyber stalking, cyber bullying, hacking, online predation, but also started examining the Computers for the purpose of extraction of evidence. Canada was the first to pass the legislation followed by the United States of America and Australia for amendments of Computer fraud and abuse.

Digital Forensics

Fig. 1: http://null-byte.wonderhowto.com

We quote here one of the most commonly used definitions of digital forensics. This was developed during the first Digital Forensics Research Workshop (DFRWS) in the year 2001 and it is still very often quoted even today:

“Digital Forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

[“Pear01”]

The forensic investigations recover acts Reus or objective evidence of a criminal activity through, the diverse range of data held in digital devices for their inquiry[3]. The dependence on digital evidence has grown exponentially and has posed a humungous challenge towards modeling the huge amounts of data. And so has Cloud computing also immensely increased traffic across the network. Digital revolution has swept away the prices of hard drives and thrashed their sizes. The computers which could hardly support hundreds of MB are now capable of housing hard drives of 1TB, 2TB to up to 10 TB within them or externally.

It has become difficult to sift this data generated in the process of investigation through cyber security. This leads to the amalgamation of analysis of vast or big data and following the principles of forensics to maintain the evidential credibility of the data. Data mining and the machine learning techniques play a vital role in treating the images and the network’s traffic output and converting them to substantial evidences for further investigation.

Forensic examiners are trained to make a forensic image or duplicate of a suspect’s hard drive to a storage device fully secured to store the relevant data. It is commonly seen in the case of a search warrant on a home that there are multiple hard drives which could be a potential evidence. The forensic examiners can no longer just pick a few pieces of evidences from the crime scene and dump it to the keen examiners. The large storage of enumerable data of evidentiary value makes it difficult for examiners to store or process it as they could be already overloaded with backlogs of other cases. This limits the resources and their efficiency. Examiners or investigators have to collaborate with newer technological methods to view bits and bytes of data of a case. This is what leads to the issue of challenges with big data storage and processing.

As the systems increase the amount of information available for the investigators the process of investigation can either get complicated or may get benefited from the additional information. Generally the poor information may just be an outlier or may not affect the process of mining. But in case of investigations the data may tangentially increase the possibility of making false allegations or assumptions.

The forensic investigation is done under the jurisdiction and carried out with the support and cooperation of several agencies and also the parties involved. The digital evidences or information may be owned by different organizations who may not be willing to collaborate with each other. But digital information like camera footage, file logs, bank accounts, emails are not only be considered or recorded as evidences legally, but also to facilitate other issues like internal security and performance.
Phases in forensic workflow

There are several phases that usually make up the forensic workflow, here are some international standards available [ISO12]:

- Identification - The procedure of searching, identifying, verifying and documenting the physical device or devices on the scene of crime as a part of evidence.
- Collection - All the devices that are identified in the previous phase can be collected and transferred for analysis.
- Acquisition - The process involves producing an image or a copy of the evidence which is potent proof and can be considered as a source. Get most fleeting information first:
  - Running processes
  - Open sockets
  - Memory
  - Storage media
- Preservation - Ensure the integrity of the evidences in either logical or physical form. Even if a file is completely deleted from the disk, there is a possibility of having a trace:
  - Web cache
  - Some directories which were temporarily created
  - Data blocks created as a consequence of a move
  - Some storage
- Analysis - Interpreting the data from all the evidence acquired in earlier phases depending on the context, the aims or the focus of the investigation. The analysis could be malware analysis, image forensics, database forensics or content analysis. Methodology differs depending on the objectives of the investigation:
  - Locate bootlegged material
  - Reconstruct events that took place
  - Determine if a system was compromised
  - Authorship analysis
- Reporting - Disseminating or communicating of the results of the digital investigation to the parties concerned. Utilize system and external information:
  - Log files
  - File timestamps
  - Any information about the Firewall
  - Try to materialize a time of events of happening

Challenges

Data analytics indeed has an important role to play in support of investigations and performing the audit function for detection of frauds, making the process of investigation more efficient, continuous transaction monitoring and prediction of future events.

Forensic Investigations have made use of information forensics for several years to extract relevant information from the electronic devices:

- A document which was deleted on an individual laptop
- A messages that could be recovered from a mobile phones, tabs, ipads.
- A set of fragments posted from an individual browsing on Facebook, tweets, instagram on the laptops of suspect or victim
- An incriminating email on a corporate email server
- Illegal transactions in a financial system

The major challenge could be both data sources are of various varieties, Investigation could be of varying Complexity and Various data sources in an investigation need to be correlated despite the fact their being disparate. Most of the investigation problems are big data problems as they have to pass the test of volume velocity and variety. The dataset is too large in terms of size (volume), too long to extract useful information from the dataset (velocity) and the dataset is made up of a varied complex structures combination of structured & unstructured data belonging to varied sources (variety). Finally processing it requires understanding and implementation of cutting edge technology. Online activities are always being refreshed increasing the velocity of data.

Forensic’s model challenges require the Forensic analysts need to:
- Adapt methods to the new scenery
- Relax some requirements
- Add some new tools to the arsenal of tools and techniques to process and Search “big data”

Rethinking Digital Forensics

To face the existing challenges and to leverage the available opportunities the entire discipline of Digital Forensics has to rethink about the established principles and all the workflows have to be reorganized, include and use the tools not previously used and considered unviable for forensic use. The experts have to trained to use these tools in a better manner and integrate them in the forensic best practices. The involvement of Machine learning algorithms and Big data skills have to be identified and prioritized in every step of investigation. Other considerations to be made include:
- Do we need to remodel the postulates?
- Do Validation would be a greater challenge to determine accuracy?
- Would Documentation require proper management of accurate logs and descriptions related to investigation?
- Is a new workflow required?
- How to Prioritize the evidence collected from the very start?
- How to maintain the Log details of examinations, and apply precise machine learning algorithms?
- All these requirements are evident enough that Big data handling tools are a must.

Some Tools for Tackling the Big Data Challenge

The fast-changing data - science landscape makes it hard to categorize the tools and techniques. Here we list some of them.

MapReduce is a great start, but it requires to expend a significant amount of resources and developers to make it work. It is a framework for massive parallel tasks. This works well when the large data sets are existing but are not correlated.

Machine learning classification algorithms like logistic regression, support vector machines can be performed in...
parallel and the results can be combined and further optimized using evolutionary algorithms for higher accuracy.

The concept of Trees both decision tree and random forests are successfully used in fraud detection software to find statistical outliers in huge data set.

The classification Techniques are best suited for the review of big data sets of hundreds or thousands of files of type image forensics like the Bayesian Classifier.

There are unsupervised techniques also like k-means and the Natural Language Processing (NLP) techniques, which have been employed for verifying, classifying of large bodies of unstructured text. The Neural networks are suitable for pattern recognition and analyzing the neural network traffic. The snapshots of the filesystem are used for training the network.

Conclusion
The challenges posed by Big Data forensic as evidence have already resulted in several new techniques and algorithms in the world of data mining, and also revision of tenets and procedures. The workflow analysis, the investigation procedures, the use of forensic tools to implement the machine learning algorithm is still subject to Research. There is a need for a new set E-Discovery tools to take large numbers of documents, emails, posts and other messages, automatically filter out the major evidences, then present the remaining for review and Data analytics tools which transform raw structured data into information through processing, transformation, visualization, and statistical analysis.

References
[4] Case Study: Big Data Forensics Neil Meikle, Associate Director, Forensic Technology, PwC.
An Intelligent Prototype to Lay the Road to Secure Next Generation Networks

R. Nagarathna
M.E., Computer Science, Thiagarajar College of Engineering, Madurai

S. Mercy Shalinie
Prof. and Head, Department of CSE, Thiagarajar College of Engineering, Madurai

Abstract: This paper provides a gist on the various security issues that may arise in nextGen networks and also proposes a secure 5G prototype which incorporates intelligence through machine learning algorithms that are found suitable for resolving the various security issues. The main notion is to make the various key elements of 5G network model to act intelligently when they are subject to various attacks, thereby providing a secure network to end users.

Introduction

5G is the latest buzzword which is expected to soon plunge into our day to day life. As there is a surge in population of ambivalent networkers, roving nodes and mobile newbies, expectations from tech world also tends to infinity. Human want to have a relaxed life. They expect their habitat to exhibit smartness in all dimensions like automation of their home appliances, an instant doctor, traffic congestion updates even well before entering the lane, very quick indicator of natural calamity, high yielding crops, animal tracking etc. There is no full stop for this list. Tech people put the whole list under the umbrella of Internet of Things (IoT). Thus there is a need for 5G topology to extend its support for Internet of Things (IoT) and machine to machine (M2M) services apart from classical voice and data services and also they have to support stringent end to end latency smaller than 4G network.

Security of 5G networks would be a major focus of researchers as the number of attackers is increasing beyond imagination. Internet of Things (IoT) covers various verticals which require processing very sensitive data. For instance if a clandestine user modifies health readings of a user ultimately doctor would provide incorrect medication which is very much hazardous to public safety. It is high time to identify a secure 5G network which is as important as increasing speed of network and reducing the latency. To identify such a secure model it is necessary to identify the loop holes of existing architecture and fuse intelligence into the model to give nextGen networks the power of decision making when they are prone to attacks.

Thumbnail of NextGen Networks:

<table>
<thead>
<tr>
<th>Security issues</th>
<th>Technology components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security of 5G networks</td>
<td>Various research consortiums such as 5G Innovation centre in UK, Ministry of Science and Technology (MOST) in China, European Union, South Korea 5G forum etc have identified major technology components that will be part of next generation architecture.</td>
</tr>
<tr>
<td>Machine type communication</td>
<td>The architecture of 5G would be device centric architecture rather than a call centric one that is a part of current generation networks’ architecture. The various pillars of 5G networks are: millimetre wave transmissions, massive MIMO technology, overlay coverage through heterogeneous networks, machine type communication, self-organizing networks, densified small cell, multi-RAT, Ultra-Dense networks, Dynamic RAN, Software Defined Radio (SDR), network function virtualization and software defined networking.[1]</td>
</tr>
<tr>
<td>Self Organizing networks</td>
<td>The networks are made to behave in such a way that they require very little play from human. The networks are given power to manage, configure themselves and even do some self healing when they fail which paves way to optimized performance of nextGen networks.</td>
</tr>
<tr>
<td>Ultra Dense networks</td>
<td>This requires out of box way of deploying infrastructure components in such a way that each moving user device have an exclusive access of access node.[2]</td>
</tr>
<tr>
<td>Millimetre wave transmissions</td>
<td>Extremely high frequency radio waves of range 30 to 300 GHz and whose wavelength lies between ten and one millimetre which facilitates frequency reuse and is plentiful makes it a good choice to be a part of nextGen networks.</td>
</tr>
<tr>
<td>Massive MIMO</td>
<td>This technology focuses on projecting the key advantages of MIMO on a massive scale. This technology proposes usage of large sets of antennas based on spatial multiplexing concept so that many users are served best at the same time without any loss of quality.</td>
</tr>
<tr>
<td>Machine type communication</td>
<td>The device users can be enabled to have a straight forward communication between them without getting exchanged through conventional network flow.[3]</td>
</tr>
</tbody>
</table>

Due to the variegated underlying access network technologies of 5G networks, the profusion of interconnected communicating devices, massive deployment of ultra dense small cells lead to a very broad spectrum of security issues, extensive backhauling, interference and complex network management issues. Security issues in 5G:

Security issues in 5G:

- Machine type communication
- Self Organizing networks
- Millimetre wave transmissions
- Massive MIMO
- Network function virtualization
- Software defined networking
- Ultra Dense networks
- Security of 5G networks

Listed below are handful of security issues that may be prevalent in nextGen networks. The system assets that would
be the targets of attackers are user equipment, random access network (RAN), sleepy nodes, network switches, SDN controller, and lossy networks.

The attacks on user equipment are commonly heard jargons such as Denial of Service, zombie army, malware such as worms, viruses etc. Attackers would try to jam the service of user equipment through SMS/MMS which is also widely prevalent in current generation networks. Apart from the single device DoS attack distributed DoS attack is sure to jam the whole network. Owing to an expectation of fully connected and moving network in 2020 these attacks will cause inconvenience to users. Also device location privacy is under the stake of foray. With increase of various services based upon user location like food delivery service, cab service etc the detailed location details and user/equipment identity are being transferred to the firms, which malicious hackers eavesdrop or perform man in the middle attack to retrieve the details\(^5\). To avoid such forays strong encryption algorithm and secure channel to transmit the garbled information can be used. There is a need to have a secure key exchange and authentication protocols that cannot be very easily broken.

Software Defined Networking is expected to be a major part of 5G owing to the advantages it offers over traditional approach. The perfect separation of control plane and data plane is not only going to address the high bandwidth requirements of Big Data and easy and efficient management of dynamic traffic patterns, but also offers security gain to the booming nextGen networks. The centralized controller maintains a global view of the whole network and each and every element maintain a data structure consisting of traffic statistics which paves way to detect intruders better than traditional network approach\(^4\). SDN maintains a repository of attacks known and detects the misfeasor by running a match algorithm. As all the elements have to report periodically it is possible to even identify black hole attack which is nearly impossible in classical networks. By probing the controller’s log we could make an analysis of foray which mostly goes undetected. SDN can be effectively made to provide a strong fort against DoS attacks by framing intelligent rules by the master controller. Even though SDN seems to offer a secure environment the attackers are growing at a rate very much higher than Moore’s law. If at all misfeasor captures the centralized controller which is the heart of 5G, the whole system is under control of attacker. He will feel free to divert the packets to destination of his choice, drop packets, use this network as a hub for launching attacks on other components and also diminish the precious resources of network. Worm hole attacks, sink hole attacks can also be done with higher probability of success. Thus the master controller turns out to be a bottleneck to the system. We could go in for multiple controllers distributed over the network instead of relying on a single controller. There is a trade-off between unnecessary overhead in providing resources to all the controllers who would end up having the same information, and security. DoS attacks are possible on network switches if there are no rules available with them to handle big packets: thereby they end up storing them in their buffer space and dropping other legal incoming packets. The nextGen network has to address the security issues carefully while designing the new paradigm.

As 5G network’s backbone is HetNets, sleepy nodes and lossy networks which are also a part of 5G are focused by attackers, as they are more vulnerable to attacks\(^3\). It is quite easy for an illegitimate node to join the network and can perform various malicious activities like attract traffic towards itself and generate false reports making successful black hole attack. Multipath technology along with Destination oriented Directed Acyclic Graph can provide security advantages to the network. But there is a trade-off between security, energy consumption and cost. Lossy networks are also vulnerable to Sybil attacks and hello type flood attacks. Firmware can also be brought under control by clandestine user and information about routing, topology of network can be easily manipulated or replayed. This is a great challenge for 5G architecture designers to prevent this attack.

**Proposed Methodology**

The notion is to use suitable Machine learning algorithms like decision tree learning or k Nearest Neighbour learning or candidate elimination learning for incorporating human reasoning capability to counter the attacks on the fly. Thus our proposed prototype will comprise: 1. SDN based routing protocol 2. Interface between the controller of control plane in SDN and the intelligent computer system 3. Suitable Machine Learning algorithm.

The decision of which Machine Learning algorithm to use will depend on the type of component under attack. The Training Experience for our system will be the study of the behaviour of the whole system. For instance power consumption of nodes, resource utilization of the nodes, congestion in the networks, adherence to rules laid by central controller of SDN by the nodes, keeping track of bytes transferred across the elements of the networks, number of packets been dropped, number of retransmissions, number of disconnections etc under normal conditions and while under attack will be studied. The system can learn though the forensics report of the previous attacks and reports generated from simulating attacks using tools. Therefore training examples given to the system will be the behaviour of system under normal conditions and while under foray. Our target function will be a secure system, say S: C\(\rightarrow\)B where ‘C’ is the input to the system which is current state of network as seen by the central controller of control plane of SDN and ‘B’ is the Boolean variable which denotes the conclusion made by the intelligent system (0 for system is working normally and no malicious activity is going on; 1 for system has been attacked). The system can also output what type of attack and which component is under attack. This is sent to the master controller of SDN for the controller to frame rules to safeguard the system from the attacker and also log in a database for forensics purpose.

A pictorial representation of our proposed SDN based intelligent prototype is given in Fig. 1.

**Conclusions**

Needless to say that it is necessary to not only focus on designing a self organizing network architecture that caters to the surge of mobile traffic and Big Data but also develop a secure architecture. Much focus is required on security aspects of 5G networks for the users to enjoy anywhere and anytime fast and safe networks. Due to the overwhelming population of hackers
and malicious clan it is highly impossible to expect a human intervention during attacks. It is high time to design intelligent systems to identify attacks and make necessary decisions to thwart the attacks. Through designing such systems, it is possible to greatly reduce the probability of system under attack.

References


About the Authors

Mrs. R.Nagarathna is pursuing M.E. Computer Science at Thiagarajar College of Engineering, Madurai. She completed her Bachelor degree in Information Technology in MIT campus, Anna University, Chennai. Her area of interests is Network security and Machine Learning algorithms.

Dr. S. Mercy Shalinie [CSI-00137526] is working as Professor and Head of the Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, TN. She has published over 130 research papers in referred journals and reputed conferences. Her area of research interest includes Machine learning and Security systems. She can be reached at shalinie@tce.edu.

Young IT Professionals Award (YITP)
Regional Round - Region 3
21 Feb. 2016 at Ahmedabad
In today’s cyber era, web applications are everything and are everywhere. A web application might be in the form of a web site, web portal or a mobile application. With the drastic surge in mobile applications, APIs are playing a crucial role. The rise in the need of web application have kept the field of software development busy in delivering products at a rapid pace. A web application vulnerability can be referred to a security loop hole in a web application that compromises integrity, availability or confidentiality of the web application. It ranges from the infamous SQL injection (SQLi), Cross Site Scripting (XSS) to a simple parameter tampering. Vulnerabilities such as XML External Entity can have devastating consequences on the target. A web application that is vulnerable to such an attack can facilitate a remote hacker to have the target system shut down. Certain vulnerabilities like DOM based XSS might be difficult to identify posing a big threat to the web application. DOM based XSS is a vulnerability that allows execution of malicious scripts which leads in the modification Document Object Model (DOM) environment of the web application. It is difficult to identify DOM based XSS using generic vulnerability scanners because there is no HTTP traffic flow between the client and server in an event where a DOM XSS is fired.

Open source project such as OWASP (Open Web Application Security Project) draws guidelines for software developers to have their code secured from security vulnerabilities. CVE (Common Vulnerabilities and Exposures) and the NVD (U.S. National Vulnerability Database) have been a boon for product vendors and users to address vulnerabilities in an effective way.

The consequences of web application vulnerabilities is overlooked and in most cases adequate importance is not given during product development phase. For instance, a Cross Site Scripting attack is often considered just as an alert pop-up and nothing more which is completely wrong. Exploiting cross site scripting on a renowned email service provider, we were able to log email content of victim remotely. CVE-2016-0031 was logged for the same. Programs such as bug bounty, CVE, etc. in the area of vulnerability assessment/security testing have made an enormous contribution leveraging the skills of security researchers across the globe. Any individual who is passionate about web application security can contribute to the field of web application security. Adhering to the responsible disclosure policy or any such policy levied by product owners or vendors, one can kick off his passion in this field by looking for vulnerabilities in the target application. The key ingredients of web application security assessment will be passion, patience and the ability to pay attention for minute details in the underlying HTTP traffic that is generated by the web application. Open source tools such as Burp Suite by Portswigger can be used to intercept HTTP traffic for analysis. Extreme care should be taken with regard to the target application’s usage policy before performing a vulnerability assessment. Automated scanners are often restricted and shall not be used on public websites.

In the field of web application security, security testing is broadly classified into two – Dynamic and Static. Dynamic Application Security Testing (DAST) is closely aligned to black box security testing where the input is the end product. Programs such as bug bounties fall under the category of DAST. To identify web application vulnerabilities at an early stage during the Software Development Lifecycle (SDL), a Static Application Security Testing (SAST) approach is followed. The input for this is the source code of the application. Both DAST and SAST are effective in its own ways. There are automated tools that are used to perform DAST and SAST. Tools such as Checkmarx[1], HP Fortify[2] etc. are widely used for SAST and tools such as IBM App Scan[2], HP WebInspect etc. are widely used for DAST for automated security testing of web applications. It is advisable to have the application testing through SAST and DAST to ensure maximum security for a product.

Secure Frameworks are widely used to mitigate common vulnerabilities that web applications are susceptible for. However, usage of secure frameworks for software development do not guarantee complete protection. Security awareness and relevant education for potential software developers is the need of the hour for computer science professionals. This cannot be superficial, but have to be at the ground level with practical exposure. There are Web Application Firewalls (WAF) that are used to mitigate web application vulnerabilities. However, fixing vulnerabilities at the web application level cannot be substituted by WAF.

Hackers are constantly on the lookout for web application vulnerabilities as much as security researchers are on the job. The critical risk is that a web application vulnerability exploit by a hacker can easily go undetected until there is a large scale breach on the target system. Exploiting critical security vulnerabilities, hackers will be able to steal sensitive information, take over user accounts, deface a website, cause huge financial damage, etc. which is a big threat.

For individuals who are passionate to contribute to the field of web application security, he/she can equip oneself by having a grip on the overall web application fundamentals and the way in which internet works focused on HTTP protocol. Materials and resources from projects such as OWASP will be a great value. With the required knowledge, using tools like Burp suite for HTTP traffic analysis and having a demo vulnerable target application such as DVWA (Damn

Continued on Page 33
**Book Review »**

**Discrete Mathematics**

<table>
<thead>
<tr>
<th>Book Title</th>
<th>Discrete Mathematics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>Vinay Kumar</td>
</tr>
<tr>
<td>Price</td>
<td>Rs.360/-</td>
</tr>
<tr>
<td>Publisher</td>
<td>BPB Publication, New Delhi</td>
</tr>
</tbody>
</table>

This is a Revised and Updated Edition of the Book first published in 2002. The Book written in a simple lucid style makes the reader go through it smoothly to understand the intricacies of Discrete Mathematics. Discrete Mathematics is being taught almost in all Universities of the Country in UG and PG courses and also NIELIT (National Institute of Electronics and Information Technology) accredited B & C level or equivalent courses in Computer Science.

The Updated and revised edition has chapters on Set, Relation, Number Theory, Function, Predicate Calculus, Poset, Lattice, Finite Boolean Algebra, Recursive Equations, Generating Function, Method of Proofs to name a few. There are a total of 23 Chapters.

Author has painstakingly written the book in a simple English to help the Indian students. He has taken a lot of care to ensure that there are no errors. The book seems to be the outcome of his flair for teaching he possesses. Thus, the book more or less appears to be like a lecture of a teacher in a class. The various Practice papers given by the author at the end are really worth attempting by the students prior to their semester exams. The pricing of the book too is reasonable.

There is an exhaustive Biography and Reference list at the end of the book. Any student for further reading can go across them. Keeping in mind of the present age of Internet, the author has also listed more than 50 web sites too. This enables the students to read further on these sites on Discrete Mathematics and related subjects. Overall a worthy book for students.

**Review by**: Mr. N. Anand Rao  
Life member: 006180, CSI Ex-Chairman Delhi Chapter,CSI
SSH is referred as Passwordless Remote login. It seems like unauthorized, but is highly authorized by public key cryptography architecture. SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user. Manually generated public-private key pairs are used to perform the authentication, allowing users or programs to log in without having to specify a password. The public key is shared among all machines that must allow access to the owner of the matching private key of owner and authentication is based on the private key. This protocol verifies whether the same person offering the public key also owns the matching private key.

This is going to be demonstrated for Single machine and distributed machines (Master & Slave) as follows:

**Single machine Configuration:**
1. Open a Terminal in Linux Machine (I have used Ubuntu 12.03 LTS) and give the command.
   $ ssh-keygen  -t  rsa  -P   "" / will create RSA key pair with empty password
2. For accessing local machine via SSH, perform the below command
   $ cat /home/hduser/.ssh/id_rsa.pub >> /home/hduser/.ssh/authorized_keys
   [Where “id_rsa.pub” is a public key to be shared with our localhost and can also be shared to any machine in Distributed cluster.]
3. For logging in to local machine with password, use the below command
   $ ssh localhost
   [This will create a new session to local machine via SSH, because public key is available in authorized keys file.]

**Distributed machines Configuration: (Master & Slave)**
1. Create two Linux machines like master and slave with the above 3 steps done at each machines.
2. Perform this command at master machine to share the public key of master machine with slave machines authorized nodes’ list.
   hduser@master:-$ ssh-copy-id -i /home/hduser/.ssh/id_rsa.pub hduser@slave
3. Login to Slave machine from master machine by issuing the below commands at Master machine only.
   hduser@master:-$ ssh master
   hduser@master:-$ ssh slave

---

**About the Author**

Mr. A. Bharanidharan [CSI-11503054] is currently working as Assistant Professor in the Department of Computer Science and Engineering at Sri Ramakrishna Engineering College, Coimbatore, Tamilnadu, India. He has 11 years of academic experience. He has rich hands on experience in Algorithms, PHP programming, Apache Hadoop, Arduino, Raspberry Pi. He handled around 12 workshops in the domain of Distributed computing, Big Data Analytics with Hadoop, Internet of Things at various Engineering colleges around Tamilnadu. He can be reached at abharanidharan@srec.ac.in.
Rules / Procedure for Approval of Technical Collaborations, for Technical Events Organized by the Non-CSI Entities like Organizations / Institutions / Universities, etc., by CSI Chapters / Regions / Divisions, without any Financial liability to CSI

Technical sponsorship / collaborations to good quality technical events, without any financial liability, subject to the following conditions, can be approved, on case to case basis:-

1. The concerned Organization / Institution must be a valid Institutional member of Computer Society of India (CSI). If they are obtaining fresh membership, they should be encouraged to take membership for longer duration like 10 / 20 years.

2. As part of this Technical Sponsorship, at-least one Life Member or 05 individual annual professional members must be generated, out of this event. For this, a copy of CSI Life Membership Form should be distributed, in the registration kit, to all the non-CSI Member delegates and arrangements should be made to collect the filled in membership form, payment details (Bank counter folio after depositing the payment in the bank or cheque, payable at par, in favour of Computer Society of India) of the interested delegates, on the spot. This can be done though keeping a counter of CSI having copies of CSI forms and other related information through a person deputed there by the organizers, on the venue of the event.

3. In order to justify the CSI Technical Sponsorship and also to motivate the delegates / participants to obtain the CSI Membership, delegates / participants must be given at-least 20% discount in registration fee, to existing CSI Members or would be CSI members (if they deposit the fee and CSI membership form on the spot).

4. If the Institution does not have the CSI Students’ Branch, at-least after the event is over, they should work hard to establish the Students’ Branch. This will be a compulsory condition for their 2nd event to be approved for technical sponsorship.

5. Quality of papers, technical materials and publications should be of high standard and be checked thoroughly by Turnitin or any other licensed antiplagiarism / cross check / similarity index softwares to avoid embarrassment to the society, at later stage. Open source softwares, for antiplagiarism checking, are not recommended, as their database is very limited and the reports are not authentic.

6. OBs and few related ExecCom members, with the consent of the sponsoring heads, be involved in the Advisory Committee or Steering Committee of the event.

7. Two delegates, based on the recommendation of the sponsoring / collaborating head, be given complimentary registration. They will be monitoring the execution / conduct of the event and submit a brief report, after the event, to the respective sponsoring / collaborating head.

8. After the event is over, a DVD having copies of the related presentations / papers / other technical materials be submitted to CSI for uploading them on CSI Digital Library (DL).

9. After the event is over, a post event report with few good quality photographs having CSI logo be submitted to the CSI HQ for its record and publication in CSI Communications.

10. The event must be planned in advance and be included, through the sponsoring / collaborating head, in the event calendar published in the CSI Communications.

11. The CSI logo, including the Golden Jubilee logo (till December, 2015), as available at CSI website www.csi-india.org and also available on the header line of this document be included at prominent places of all the flyers, backdrops, banners, publications, and other printed materials, under the head; Technical Sponsor, if there is only one sponsor, otherwise, as Technical Co-Sponsor.

A proposal giving details of the programme may be submitted to corresponding chapter/ region/division, at-least 06 months in advance.
Application Form for Individual / Life Membership

I, hereby, apply for new membership. On approval of Membership, I shall abide by the Constitution & Byelaws of the Society and the Code of Ethics. Please also attach / upload a good quality minimum 300 x 300 pixels / passport size photograph along with a copy of Voter ID / Aadhar Card / PAN Card / Driving Licence to be used for making your CSI Membership Card.

I. Select the membership type
Indian [ ] International [ ]

Please tick for Membership period
One Year [ ] Two Years [ ] Three Years [ ] Four Years [ ] Life [ ]

II. PERSONAL INFORMATION:
Please fill in your personal information so that we can serve you better
Title of the applicant  Mr.  Miss  Mrs.  Dr.  Prof.  
First Name  Middle Name  Last Name
Name you would like to be printed on CSI ID card

Date of Birth  Gender  
M  F

Primary Email ID  Secondary Email ID

Phone No. (Residence)
STD Code  Phone

Mobile (Mandatory for domestic membership)

III. Mailing Address (BLOCK LETTERS):
Address line 1  Address line 2

Address line 3  Pincode

City  State  Country

(City, State and Country to be filled in only for International address)

Name of the Chapter to be attached:
IV. Payment Details:

Please specify Mode of Payment: [Online Payment / Demand Draft] _________________________
If payment made through Online Payment Gateway*: Transaction ID _________________________
Date of Transaction _________________ for Rs.......................(Rupees          )
(*Please email copy of Payment Response page along with Application Form)
If payment made through Demand Draft DD / Cheque payable at par at Mumbai should be drawn in
favour of “Computer Society of India”.
Cheque  DD  Cash  (Please tick as applicable)

Amount Paid Rs./$ _________________________
Cheque / DD No. _________________________ Dated dd/mm/yyyy
Drawn on Bank Name _________________________ Branch Name _________________________

Please fill following details if it is direct deposit in Axis bank.

Date of Deposit dd/mm/yyyy
Mode of Deposit Cheque  DD  Cash  (Please tick as applicable)
Axis Deposit branch name _________________________
Axis Bank SB A/c. No.: 060010100082439

Attach photocopy of Pay-in-slip with application form and write your Name, Contact no. ,
Membership period on the reverse of the Cheque / DD / Pay-in- Slip.

V. Code of Ethics - Undertaking:

I affirm that as a CSI member, I shall abide by the Code of Ethics of the Computer Society of India (CSI). I further undertake that I shall uphold the fair name of the Computer Society of India by maintaining high standards of integrity and professionalism. I was not a member of CSI earlier. I am aware that my breach of the Code of Ethics may lead to disciplinary action against me under the Byelaws and rules of the CSI. I hereby confirm that I shall be bound by any decision taken by the CSI in such matters. Further, I hereby convey my consent to receive the information about the activities of the society by email or by SMS on my Mobile number, from time to time, by the society or the members of the society.

Date: / /
Place: ______________________ Signature: ______________________

FOR OFFICE USE ONLY

Application received date : ______________________ Received By : ______________________
Application processed by : ______________________ Membership No. ______________________
Digital Forensics in Cloud Computing Environments: Current Challenges and Solutions for Effective Forensic Investigation

Anand Nayyar
Assistant Professor, Department of Computer Applications & IT, KCL Institute of Management and Technology, Jalandhar, Punjab

Vikram Puri
Corporate Trainer and Embedded Systems Engineer, Enjoin Technologies, Jalandhar

Cloud Computing- A yet another form of computing which is transforming the face of computing from Top IT Organizations to SME’s and to individuals by providing facilitation of accessing applications anywhere and everywhere across any part of the world. As per Deloitte, by year 2020, 95% of top 100 corporations will integrate Cloud Computing technology in their day to day operations. A recent report from market research firm “Markets and Markets”, cloud computing industry is set to grow to $121 billion dollars by 2015. Even through the annual growth is above 75%, which is tremendous and eye stunning. But on the other hand, the crime rate related to computers and internet is also doubling and even tripling every year due to viruses, malwares, hacking, vulnerabilities and backdoors in systems. This in turn, has resulted in the development of digital forensics for ensuring the proper presentation of cyber evidence against cyber criminals in court of law. As per FBI statistics, in U.S., the size of digital forensics case reporting has increased to 50% in year 2015-16. Cloud computing has given rise not only to the problem of scale of digital forensic activities but also opened new issues and challenges for effective investigation.

As, cloud computing is very extensive computing involving large data centres, mainframes, centralized cum distributed computing and high speed optical networks, Digital Forensics investigators has to improvise their investigation knowledge and even new investigation tools requirement has come up to help both Cloud Computing Service Providers and even Cloud Computing Organizations using Cloud Computing as service. Individuals acting as cloud clients, need to have a specialized capability to reduce risks and threats in cloud security and provide effective defense mechanism against intruders.

Definition of Cloud Forensics:

“Cloud Computing Forensics is regarded as a specialized forensic science of applying scientific principles, technological tactics and various proposed and proven methods to cloud computing via identification, collection, preservation, examination, interpretation and reporting of digital evidence.”

As per NIST, Cloud Computing is regarded as “a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort of service provider interaction”.

Cloud Forensics=Cloud Computing+ Computer Networks+ Forensics (Digital + Network)

Cloud Forensics is regarded as combination of various disciplines i.e. Cloud Computing, Computer Networks and Digital Forensics. It is basically regarded as subset of network forensics. Cloud Computing is regarded as on demand computing in which users take desired and required services in terms of Software, Platform and Infrastructure from cloud service providers and pay as per their usage. An organization which provides cloud services is called CSP (Cloud Service Provider) and any person/organization which takes services is called CC (Cloud Client).

Digital Forensics is a combination of several forensics like computer forensics, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis and even computer examination and is composed of proper process based investigation of various sources like (Hard Disk, MP3 Players, Computers, or any other sort of gadget) handled by a digital forensic expert to recover crime evidence for reproduction in court of law.

Network Forensics is basically doing crime based investigation and forensics on computer networks for efficiently scanning out the digital fingerprints of attackers or intruders in the network and tracking the cybercrime.

Three Dimensions Surrounding Cloud Computing Forensics

A. Technical Dimension: Usage of forensic tools and following set of defined procedures for carrying out investigation in cloud environments. In this process, the investigator would be doing varied tasks of data collection, live forensics, evidence segregation, virtualized environments and proactive measures.
   • Data Collection: Comprises of identifying, labelling, recording and collecting forensic data.
   • Live Forensics: Comprises of live usage of tools and procedures to combine various evidences of crime happened.
   • Virtualization: It is regarded as key element/backbone which implements cloud computing.
   • Proactive Measures: Comprises of regular snapshots of storage, proper authentication and access control and full audit of computing resources.

B. Organizational Dimension: At the time of forensic investigation especially in cloud environments, two parties are involved: Cloud Service Provider and Cloud Client. In order to provide effective and efficient services and maintaining proper two-way interrupt and hassle free service relationship, organizations are required to create a structure involving staff, customer collaboration and external assistance to perform various jobs. The persons required are as follows:
   • Investigators: Overall responsible for carrying out investigations any time when any breach or illegal activity occurs and work closely with law enforcements.
   • IT Professionals: Comprise of various administrators like network, security and systems, ethical hackers, cloud computing deployment experts and even penetration terms. Working with Digital Forensic Investigators
closely to investigate the crime and assisting investigators in data acquiring.

- Incident Handlers: Main duty of these persons is to report any sort of breach, incident or illegal activity in terms of unauthorised data access, data breach, data loss, malicious/virus attack in the network.
- Legal Advisors: Closely work with Investigators to assist in how to properly report and present the various evidences and crime happened in court of law.
- External Assistance: Sometimes a major and serious cybercrime can take place which sometimes becomes impossible for internal staff to handle, so it is very important and wise part for cloud organizations to have external parties on standby for performing forensic tasks like data discovery, investigation of crime scene and other incident reporting activities.

C. Chain of Dependencies: Cloud service providers and lots of cloud apps have dependencies on other cloud providers. These dependencies are highly dynamic which means investigation in such a situation will depend on the investigations of each link in the chain as well as the level of complexity of dependencies. The cloud service providers, cloud clients with chain of dependencies has to coordinate with other parties as mentioned below for effective investigation:

- Law Enforcement: Basically does the work of prosecution of criminals.
- Third Parties: Responsible for auditing and ensuring compliance regarding cloud forensics, cloud providers has to work with third parties.
- Academic: Cloud organizations also work closely with academia for formulating and discovering new modes of investigation and cloud forensic research to contribute more and keep themselves well updated with latest threats and defenses against them.

Cloud Forensics-Digital Forensics Challenges and Solutions

The Following Table gives a Comprehensive Description of Various Challenges surrounding Digital Forensics and Solutions in Cloud Environments:

<table>
<thead>
<tr>
<th>S. N.</th>
<th>Challenge</th>
<th>Solution Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unknown Location of Attack Origin</td>
<td>1. Resource Tagging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Effective SLA (Service Level Agreement) with Cloud Service Providers</td>
</tr>
<tr>
<td>2</td>
<td>Decentralized Data</td>
<td>Proper Log Monitoring System with Regular Audit Checks</td>
</tr>
<tr>
<td>3</td>
<td>Data Duplication / De-Normalization</td>
<td>Resource Tagging</td>
</tr>
<tr>
<td>4</td>
<td>Dependency Chain</td>
<td>Non</td>
</tr>
<tr>
<td>5</td>
<td>Encryption</td>
<td>Usage of Public and Private Key Management Exchange system between the parties with atleast 512-bit and above encryption keys</td>
</tr>
<tr>
<td>6</td>
<td>Chain of Custody</td>
<td>RSA Signature, Well Defined Security Policies and Procedures</td>
</tr>
<tr>
<td>7</td>
<td>Evidence Segregation</td>
<td>Sandboxing</td>
</tr>
<tr>
<td>8</td>
<td>Violation of Data</td>
<td>Persistent Storage</td>
</tr>
<tr>
<td>9</td>
<td>Data Integrity</td>
<td>Usage of high end encryption algorithms like: MD5, SHA1, RC5, NEC etc.</td>
</tr>
<tr>
<td>10</td>
<td>Inaccessibility</td>
<td>Live Forensics, Management Pane</td>
</tr>
<tr>
<td>11</td>
<td>Trust</td>
<td>Hardware Trusted Platform Model (TPM), Virtual TPM’s, Detective Controls</td>
</tr>
<tr>
<td>12</td>
<td>Multi-Tenancy</td>
<td>Sandboxing</td>
</tr>
<tr>
<td>13</td>
<td>Deleted Data</td>
<td>Regular Backups on different backup locations, Regular Snapshots of Data</td>
</tr>
<tr>
<td>14</td>
<td>Jurisdiction</td>
<td>Cross Border Law, International Law</td>
</tr>
<tr>
<td>15</td>
<td>Cloud Complexity</td>
<td>Time Lining of events</td>
</tr>
<tr>
<td>16</td>
<td>Compliance</td>
<td>Defined Principles, procedures and process</td>
</tr>
</tbody>
</table>

Conclusion

Cloud Computing, is progressing day by day by leaps and bounds. But, cloud computing security threats are also growing. In order to detect various sorts of security threats in day to day cloud operations, security administrators apply various encryption and other data confidentiality maintaining techniques. To track the hackers, intruders and detect the digital fingerprints, digital forensics has to be used. Digital Forensics will help in overcoming all sorts of shortcomings in terms of security and threats detection and it will lay strong foundation for safeguarding the cloud server and environments against intrusions in cyber-crime world. Digital Forensics is yet another challenge in front of investigators as cloud computing environments are complex to handle and have
tons of data and complex servers to handle. In this article, we have proposed various threats and solutions that could be adopted by investigators for carrying out effective digital forensic investigation in real environments.

References


About the Authors

Er. Anand Nayyar [CSI-I1502825], working as Assistant Professor in Department of Computer Applications & IT at KCL Institute of Management and Technology, Jalandhar, Punjab. His area of interests includes Wireless Sensor Networks, MANETS, Cloud Computing, Network Security, Swarm Intelligence and Embedded Systems. He can be reached at anand_nayyar@yahoo.co.in.

Er. Vikram Puri is currently working as Corporate Trainer and Embedded Systems Engineer in Enjoin Technologies, Jalandhar. His area of interests includes Embedded Systems, Real Time Systems, Robotics, Microcontrollers and Programming in C/C++.
Crossword

Test your knowledge on Digital Forensics

Solution to the crossword with name of first all correct solution provider(s) will appear in the next issue. Send your answer to CSI Communications at email address csic@csi-india.org and cc to drdurgeshmishra@gmail.com with subject: Crossword Solution – CSIC March Issue.

ACROSS
1. A copy of data that is kept as an emergency measure
3. The art of hiding secret messages
6. The notional environment of data and computer communications
9. Digital media seized for investigation
12. A technology that allows increased storage and reliability
13. Examination and assessment of access records
14. A small file stored on the user’s computer during browsing
15. To locate deleted file

DOWN
2. A program that captures key strokes of user to capture secret information
4. The process of creating duplicate copy of digital media
5. A logical area of hard disk
7. A computer that is not connected to a network
8. A record kept by many applications and operating systems of various activities.
9. 1024 Petabyte
10. Use of hash function for verification purpose
11. The process of creating CD/DVD

Do you know how “File Slack” helps in Digital Forensics?

File slack is the difference in the actual file content size and the file size allocated by operating system on the disk. This is the area between the end of contents of the file and end of allocated disk space. The file slack area may contain previously deleted file contents, or even the data before the last format. It can help knowing previous uses of the computer, and could contain much important information for investigator. For example pieces of email messages, office documents etc. This area can be used as Digital Evidence during investigation.

Dr. Durgesh Kumar Mishra, Chairman, CSI Division IV Communications, Professor (CSE) and Director Microsoft Innovation Center, Sri Aurobindo Institute of Technology, Indore

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

Congratulations!

All nearby Correct answers to January 2016 month’s crossword received from the following readers:

Sapna Shukla, Assistant Professor, Amity School of Engineering and Technology, India.
S.Saroja, Assistant Professor, Mepco Schlenk Engineering College, Sivakasi, India.
Amit Kumar Mishra, Asst.Professor, Anand Engineering College, Agra, India
Ravi Sundaram, Consultant, TCS Chennai, India
Inauguration of CSI Student Branch at APS College of Engineering, Bangalore

CSI Student Branch was inaugurated at APS College of Engineering, Bangalore on February 17, 2016 by Padma Bhusan Prof. V Rajaraman, CSI –Life Time Achievement Awardee in presence of Dr. Anirban Basu, Vice President, CSI and other dignitaries. The Branch will initially have 100+ members from CSE Branch and expected to grow soon.

CSI Vice President Dr. Anirban Basu inaugurated a CSI Student Branch at KLEIT, Chikodi, Karnataka in presence of Principal Prof. Sidramappa Itti on February 26, 2016 in a colorful function and delivered a talk on “Cloud Computing, IOT and Big Data”.

CSI Education Directorate

Report about workshop on Embedded System Design using ARDUINO

CSI Education Directorate jointly with National Institute of Electronics & Information Technology (NIELIT), Govt. of India has conducted a two days hands-on workshop on Embedded System Design using ARDUINO on 5th & 6th February 2016 at CSIED. Mr Janarthanam, Scientist, NIELIT Chennai has given the introduction about ARDUINO. Mr K Govinda, RVP-VII has also spoke on the occasion.

Mr. Raghuram & Mr. Ajay Nirmal, NIELIT Chennai were the Resource Persons. The two days workshop was conducted as an introduction to embedded systems design and development using ARDUINO platform to allow for easy and fast prototyping. Being able to just hook up I/O peripherals on it in a matter of minutes, instead of hours is just amazingly powerful and convenient when there is an idea and just want to see if it works. Arduino platform gives a lot of pre-wiring and free code libraries that will allow concentrating on testing idea instead of spending time building supporting circuity or writing tons of low level code. On top of the hardware and software advantages, Arduino has a great community of users that can help a lot to testify the ideas.

Key Points of workshop: Introduces the use of open source ARDUINO IDE and freely supported libraries; Dealt elaborately the architecture of platform; Provided coverage of embedded systems, with an emphasis on the practical use of ARDUINO platform; Covered embedded software fundamentals, including software planning, and ARDUINO C-language program development; Included detailed treatment of embedded hardware fundamentals, discussing structure, interfacing and configuration of hardware building blocks; Emphasized examples and exercises that reflect real applications for embedded systems design.

M. Gnanasekaran
Manager (Administration)
Ahmedabad Chapter

In order to promote CSI activities in the region and opening of new CSI student branches, CSI Ahmedabad Chapter Chairman Shri Vijay Shah and Regional Vice President Dr. Vipin Tyagi visited Sabar Institute of Technology for Girls, Ahmedabad and L.J Gandhi BCA College, Modasa on 20 Feb. 2016.

CSI Ahmedabad Chapter and CSI Div-IV organized International Conference on Communications and Networking (ComNet) organized in association with ACM during 20-21 February, 2016 at Ahmedabad Management Association, AMA, Ahmedabad. More than 290 research papers from total 17 states across India were received. Out of these 76 research papers based on peer reviews have been selected for publication with Springer. On the first day Prof. Andrzej Rucinski, Founding Director, Critical Infrastructure Dependability Laboratory, University of New Hampshire, USA gave a talk on “Issues and challenges with IOT Revolution”. The speech was well received by 300+ participant including Research Scholars, Paper Presenters of the conference, IT professionals and entrepreneurs and students of various institutes of Gujarat and India and general public. Mr. Sumit Chowdhury, Global Thought Leader, Smart Cities delivered his key note address on 2nd day on “Smart Cities”. He discussed what exactly a smart city is and what the importance of measurement of various parameters related to the city is. He discussed about protocols, standards, stakeholders, issues and challenges for implementing the concept of smart cities etc. Both the sessions were appreciated by the participants and concluded by unending barrage of interesting questions and answers.

Bangalore chapter

CSI Bangalore Chapter and SCI SIG on FM and CSI SIG on IS organized 10th National Conference on IT in Defence in memory of Dr. APJ Abdul Kalam - Former President of India and also Director General of DRDO at Bangalore on 12th and 13th February 2016. The Conference was a grand success with the participation of industry, representatives of armed forces at senior level, academia and top officials of DRDO. As usual DRDO has given full support to this conference by sponsoring it and with Dr. Sateesh Reddy, SA to RM as Chairman of the Advisory Committee. Besides DRDO the conference was supported by the Department of IT, BT & ST, Government of Karnataka, National Technological Research Organization, NTRO a Government of India Organization, and Public Sector Company ECIL of Hyderabad. There were nearly 200 delegates from industry, DRDO, PSU’s and academic institutions. There were 6 sponsors from the industry such as Vmware,
Chekpoint, Stratsys, Beyond Security, Luciad partnered by Ramp Technologies and Cyber Security Privacy Foundation. The conference was inaugurated by Dr. K D Nayak, DG(MED &CoS) of DRDO. Professor Bipin V Mehta was the guest of honor. There was also a panel discussion and valedictory session. Mrs. Bhanumathi KS Organizing Chair ITD 2016 & Convenor SIG FM and Chairperson of Bangalore Chapter delivered the welcome address to the gathering. She welcomed Dr. KD Nayak the Chief guest and Prof Bipin V Mehta President of CSI. She particularly thanked Prof. H N Mahabala, Founder member of CSI and Dr. S Ramani and Mr. M L Ravi who were the former Presidents of CSI. Then she not only welcomed all the delegates but particularly welcomed each one of the Past Chairpersons of CSI- BC who made it convenient to attend. She also welcomed Mr. MVKV Prasad Director of ADE, Mr. MZ Siddique, Director of GTRE and Dr. Bipin Shah, CEO and Chairman of Kovair.

Dr. CR Chakravarthy, Co-Chairman of Advisory Committee spoke on the origin of IT for defence. He mentioned that the first conference was held in 2004 wherein there was very good response with more than 300 delegates participating in this conference. He mentioned that this has become very prestigious conference of CSI. He said that this conference brings on a single platform DRDO, all the three services, PSU’s and academia to discuss the challenges of computing requirements of defence and to evolve solutions for the same. He mentioned that this conference is dedicated to the memory of Dr. APJ Abdul Kalam who was the father of Indian guided missile program. He said the conference has about 6 technical tracks relevant to defence and a panel discussion on “Trusted computing”. He welcomed all the delegates, the Chief Guest, Dr. K D Nayak and Prof Bipin V Mehta.

Dr. R K Ramanathan, Event Chair then elaborated about the event and briefly mentioned the reason behind having the conference in the memory of Dr. A P J Abdul Kalam. He briefly talked about Dr. Abdul Kalam’s life story and his achievements in reaching to the Presidency and his three famous books he wrote before he became the President and how he was an inspiration to the young people and his igniting of minds. His slogan to make the country strong and secure which was the theme of the conference. He recalled his association with Dr. Kalam and Dr. Kalam’s introduction of IT into the President’s office.

Dr. K D Nayak Director General of DRDO was the chief guest. He spoke on the theme of the conference - "Trusted Computing in Defence". Prof. Bipin V Mehta very much praised CSI Bangalore Chapter for holding this conference for the 10th time. He also emphasized on the need for having trusted computing in defence. Mr. Arun Narayanswamy of Vmware briefly explained on the development efforts involved with defence. The 4th technical session was held on Collaborative Engineering. Smt. Sushma Verma from SAG, Mr. Suresh Kumar from ADA, and Dr. Yogananada Jeppu from Honeywell spoke on formal methods pertaining to defence. 5th technical session was on Data Analysis and Security. In this session Dr. Narayan Panigrahi from CAIR, Dr. Sudarsan P. from ABB and Mr. Capt. Rakesh Arora of Indian Air Force. In the first technical session, there were keynote addresses from Mr. V. Ponraj who had worked with Dr. Kalam in the President’s Office and one from each of the sponsors. This session was chaired by Prof. H N Mahabala, Past President of CSI, Fellow and Founder of the CSI. Prof. Mahabala said that he is always happy to come for a seminar organized by CSI. He recalled the time when CSI was founded along with Prof. Narasimhan and Major A Balasubramanian. Major Balasubramanian passed away just about a month ago. Mr. Arun Narayanswamy, of Vmware spoke on “Role of Infrastructure in Trusted Computing”; Mr. Ramandeep Singh Senior consultant of Checkpoint spoke on “Using Cyber Resilience Techniques to defend Corporate Networks”. Mr. Ganesh Babu, from Stratsys India spoke on “3D Printing”. Mr. Ponraj was deputed from ADA to work under Kalam at Raisathapathy Bhavan and was working with him till the time of his death. He described the Pan African Project conceived by Dr. Kalam and executed by him. It consisted of linking some 30 to 40 countries in Africa with Indian Universities for distance Education and also linking a number of superspeciality hospitals in India to provide telemedicine service to various cities and rural centres in Africa.

The 2nd technical session was held on Hardware and software security. In this session Smt. Kamini Malhotra from SAG, Major Meigha Mohanan from Directorate of Information systems in the army and Mr. Prasanna J. of Cyber Security spoke on the latest security threats and attacks. The 3rd technical session was held on IOT. Smt. Subha Easwaran from BEL, Mr. Ravi Prakash A. from Beyond Security spoke on the development efforts involved with defence. The 4th technical session was held on Collaborative Engineering. Smt. Kalam international conference for the 10th time being the Chief Guest.

A panel discussion was held on the theme of the conference “Trusted Computing in Defence”. The moderator was Mr. B.S. Bindhumadhaba Associate director of CDAC. Dr. P. Sudarsan, Gp. Capt. Rakesh Arora and Mr. Viswam from LRDE were the other panelists. The valedictory session was preceded by Dr. C.R. Chakravarthy. Mrs. KS Bhanumathi, Dr. R.K. Ramanathan, Mr. Chander P. Mannar and Mr. B.G. Satish took part. Dr. C.R.
Chakravarthy said the conference was a grand success. He was happy that nearly 200 delegates took part and that conference was well supported by the various sponsors from the industry.

**Bhopal Chapter**

CSI Bhopal Chapter organized the International conference on Advances in Electronics, Computer and Mathematical Sciences from 26-28 Feb 2016 at Sagar Group of Institutions. It was inaugurated by Dr. R. K. Dutta, former President Computer Society of India. In this conference more than 200 research papers were selected for presentation. Eminent Speakers from India and Abroad were invited to deliver the keynote and invited talks. Dr. A. H. Siddiqui from Saudi Arabia delivered the keynote on “Mathematics is the mother of all emerging technologies”, Dr. Sharifuddin from Bangladesh delivered the talk on “Problem and Purpose of vision based GAIT analysis for identification of Individuals ”, Dr. R. Raghvendra from Dubai delivered the talk on “ Partition theory on mathematics”, Dr. N. S. Choudhary, Director, VNIT Nagpur delivered the talk on “Computationally Difficult Problems in Some investigations: P and NP Problem”. Dr. V. H. Pradhan from NIT Surat delivered the talk on “Applications of numerical methods in advance research”, Dr. M. P. S. Chawla from SGSITS Indore delivered the talk on “ Effective methods of teaching”, Dr. R. P. Singh, former director, MANIT Bhopal delivered the talk on “ Wireless and Mobile Communication”, Dr. Vinay Tyagi, Regional Vice President, Computer Society of India for Region-3 from Jaypee University Guna delivered the talk on “Content Based Image retrieval”, Dr. Poonam Sinha from Barkatullah University delivered the talk on “Increased rate of call drop in mobile networks”, Dr. J. C. Bansal from South Asia University also delivered the talk. Apart from these speakers many other well known academician including Dr. Shailendra Singh from NITTTR Bhopal, Dr. Nishchol Mishra from RGPV Bhopal, Dr. R. S. Thakur from MANIT Bhopal, Dr. R. P. Gupta from IETE MP&CG were invited to chair the sessions.

Er. Sanjeev Agrawal Chairman SGI and Dr. Prashant Jain Executive Director SGI congratulated the whole organizing team including conference chair Dr. V. P. Saxena & Dr. Ashish Dutta and the organizing Secretary Prof Rajesh K. Shukla for successful conduction of the conference.

**Goa Chapter**

CSI Goa Chapter in collaboration with Dept. of CSE, Goa University and Saraswat Vidyalaya's Sridora Caculo College of Commerce & Management Studies, Mapusa conducted a one-day workshop on “Course Design and Pedagogy for Introductory Programming” on 6th February 2016 at the Saraswat College under the Continuing Education Programme of IIT Bombay for the benefit of teachers of Higher Secondary, Undergraduate and Post-graduate courses in Computer Science & Engineering.

Prof. Abhiram Ranade, IIT-Bombay was the resource person. Prof. Ranade provided insights into the pedagogical approach adopted at IIT Bombay and other premier engineering institutions in teaching introductory computer programming. He conducted a hands-on session on Simplecpp, a graphics package.

**Nagpur Chapter**

CSI Nagpur Chapter organized a two days National level Technical Symposium “POLARIS-2k16” with Computer Science & Engineering Department of Shri. Ramdeo Baba College of Engg & Management, Nagpur on 29th and 30th Jan 2016. The chief guest of the event was Mr. Amit Kale Director Engineering, GlobalLogic India Pvt. Ltd. Total 1200 people participated from all over the region. Highlighting Events were Project Competition, Coding Contest, Password cracking competition, Personality contest and two days pre workshops from 27th to 28th Jan 2016 on Android, Sales force- mobile and Cloud, Fun with MATLAB for UG and PG students.

**Rourkela Chapter**

CSI Rourkela Chapter conducted a technical talk on “High performance computing, Grid, Cluster and Cloud: an Overview” on 12th May 2015. Talk was given by Prof. L. M. Patnaik who is a senior scientist and Honorary Professor of IIISC, Bangalore. He covered various aspects of subject covering grid computing, cluster computing and cloud computing. He had discussed basics, uses of these technologies and its industry integration. Covering the various aspects of these technologies he had explained uses of these technologies in steel industry particularly in SAIL and how SAIL can get benefit out of it. Members of CSI Rourkela Chapter from OCL Rajgangpur, NIT Rourkela and
CSI Rourkela Chapter organised a technical talk on “Privacy Preserving Data Publishing” at C & IT Conference Hall of Rourkela Steel Plant on 8th Aug 2015. Dr. Sathya Babu of NIT Rourkela delivered the talk. He covered various aspects of subject like data privacy, data security, biometric Industry and genetic privacy, algorithms of data privacy and publishing. He explained how data is being collected from various sources and its vulnerability during publishing of data. He has explained how data can be published with maintaining privacy of data.

Members of CSI Rourkela Chapter from OCL Rajangpur, NIT Rourkela and RSP attended the talk. Mr. Sanjoy Mohanty, Chairman CSI Rourkela welcomed the gathering and Mr. Sanjay Gautam gave vote of thanks. Mr. Biswajit Mandal coordinated the event.

CSI, Rourkela Chapter is instrumental in spreading computer awareness amongst the people in and around Rourkela for the last 3 decades. Upholding the above tradition, the Chapter conducted a written quiz competition for the students of Class IX and X on 29th November 2015 at St. Paul’s School, Rourkela. The topics covered are Computer Hardware, Programming Basics, Networking, Database and Who is Who in Computer Industry. A total of 240 Students from 17 schools participated in the competition. To encourage Computer awareness amongst the students, the Examination was held in On-Line mode (paperless) using student response system. This was widely appreciated by students as well as the teachers of the participating schools.

The topic for the elocution competition was “Is online shopping a pain or gain”. A total of 24 Students from 17 schools participated in the competition. To encourage Computer awareness amongst the students, the elocution was of very high standard, which speaks the volume of the debating quality of Rourkela students. The result was declared by the judges on the spot.

CSI-Vadodara Chapter

CSI-Vadodara Chapter celebrated “The Computer Day” on 31st January, 2016 in collaboration with Department of CSE, The M. S. University of Baroda. Following the mission of Computer Society of India, under the pretext of integrating new entrants into the IT field, the CSI – Vadodara Chapter, organizes several CS/IT related technical competitions for School & University students, during this Technical Fiesta.

The CDC-2016 comprised of 17 competitions, wherein total 266 participants from 13 schools & 10 colleges participated. The total number of participants from schools were 132 & from colleges 134, thus providing opportunity to students of every age group to participate in CS/IT competitions. Total of 63 prizes were distributed, amounting to Rs. 27,000/- which were covered entirely from Participation Fees and Sponsorship.

Dr. S.K. Vij, Veteran & Ex-Chairman, CSI, Vadodara Chapter, Shri D.O. Shah, Chairman CSI, Vadodara Chapter and Mr. Chetanbhau Shah, VC inaugurated the event. The Jury Members for College Competitions were Senior IT Officials from Industries like Linde Engg. India, L&T Technologies, Reliance IPCL, ONGC etc and the School Competitions Jury were University Professors and Senior CSI Professionals. The Prize Distribution Ceremony was conducted in auspices of Dr. S.K. Vij, Shri Anjan Thakur, Senior Veteran CSI, Mr. Maulik Bhansali, ED, CEQ, Netweb S/w, Mrs. Vibha Naik, GM (IT), Linde Engineering, India.

Dr. Mamta C. Padole, Co-ordinator, Mr. Kshitij Gupte, Co-Coordinator and the Students Committee from CSE, Dept. The M.S. University of Baroda organized the event, under the aegis of Ex-Chairman CSI (VC) Prof. B.S. Parekh.

CSI Vellore Chapter

CSI Vellore Chapter organized a one day guest lecturer in “Research directions in Internet of Things and Big Data Analytics” on 04-02-2016 at VIT University.

Mr. Ravi B, CEO, Vishal Telecommunications Pvt. Ltd, Bangalore covered Introduction IOT and big data and discussed about the research issues in internet of things and big data above topics round 45 faculty members attended, organized by Prof. G. Jagadeesh and Prof. K. Govinda.

CSI Vellore Chapter organized a guest lecturer in “Applications of Sensors in IOT” on 11-02-2016 at VIT University. Prof. Narayanamoorthy, Assistant Professor (SG), VIT University, Vellore covered Introduction session on IOT, explained different types of sensors and their applications, demonstrated the wearable sensors used in healthcare domain 45 students attended the workshop, organized by Prof. G. Jagadeesh and Prof. K. Govinda.
<table>
<thead>
<tr>
<th>REGION - II</th>
<th>REGION - III</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOVT COLLEGE OF ENGINEERING &amp; CERAMIC TECHNOLOGY, KOLKATA</td>
<td>G H PATEL COLLEGE OF ENGINEERING &amp; TECHNOLOGY, VALLABH VIDYANAGAR</td>
</tr>
<tr>
<td>21 &amp; 22-1-2016 – during Two days Workshop on Programming in Java</td>
<td>15-2-2016 – during One day National Symposium on Internet of Things</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGION - III</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES INSTITUTE OF COMPUTER STUDIES, AHMEDABAD</td>
</tr>
<tr>
<td>5-2-2016 – during experts session on Innovation and Career Opportunities in Open Source Technologies</td>
</tr>
<tr>
<td>AES INSTITUTE OF COMPUTER STUDIES, AHMEDABAD</td>
</tr>
<tr>
<td>30-1-2016 - during experts session on Sales Force Technologies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGION - III</th>
</tr>
</thead>
<tbody>
<tr>
<td>THE LNM INSTITUTE OF INFORMATION TECHNOLOGY, JAIPUR</td>
</tr>
<tr>
<td>8 &amp; 9-2-2016 – during two-day lecture series on GIT and Github</td>
</tr>
<tr>
<td>GYAN GANGA INSTITUTE OF TECHNOLOGY AND SCIENCE, JABALPUR</td>
</tr>
<tr>
<td>during industrial visit at Nainital scheduled from 12th Feb 2016 to 17th Feb 2016.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGION-IV</th>
<th>REGION-V</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAKIR MOHAN UNIVERSITY, BALASORE</td>
<td>GIT - GITAM UNIVERSITY, VISAKHAPATNAM</td>
</tr>
<tr>
<td>17-2-2016 – during Study tour programme and Experimental Establishment (PXE) at DRDO Lab</td>
<td>27 to 29-01-2016 - during three days workshop on Python Programming</td>
</tr>
</tbody>
</table>
### FROM STUDENT BRANCHES

| REGION-V |
|-----------------|-----------------|
| **SRINIVAS INSTITUTE OF TECHNOLOGY, MANGALORE** |
| 3-2-2016 – Mr. Shashidar & Mr. Alwyn during one day workshop on Android Application development using Phonegap |
| **SRINIVAS INSTITUTE OF TECHNOLOGY, MANGALORE** |
| 4-2-2016 - Mr. Aravind Naik & Mr. Manjesh during one day workshop on Image processing using MAT Lab |

| REGION-V |
|-----------------|-----------------|
| **SILICON INSTITUTE OF TECHNOLOGY, BHUBANESWAR** |
| 15 & 16-1-2016 – during two days Workshop on Wireless Sensor Networks with Internet of Things and Cloud Computing (WICC-2016) |
| **NBKR INSTITUTE OF SCIENCE AND TECHNOLOGY, NELLORE** |
| 19-2-2016 - during Brain Drain Event for II and III Year CSI Student Members |

| REGION-V |
|-----------------|-----------------|
| **G. PULLIAH COLLEGE OF ENGINEERING & TECHNOLOGY, KURNOOL** |
| 20-2-2016 – during a seminar on Importance of Technology, Database and Communication |
| **VASAVI COLLEGE OF ENGINEERING, HYDERABAD** |
| 6-2-2016 - during guest lecture on Need For Programming Languages and Agile |

| REGION-VI |
|-----------------|-----------------|
| **UNIVERSAL COLLEGE OF ENGINEERING, VASAI** |
| 29-1-2016 – Prof. Kanchan Dabre delivering lecture during one day Windows Movie Maker Workshop |
| **SHARAD INSTITUTE OF TECHNOLOGY COLLEGE OF ENGINEERING, YADRAV** |
| 16-1-2016 – during Student Branch Inauguration |
#REGION-VI

<table>
<thead>
<tr>
<th>SHARAD INSTITUTE OF TECHNOLOGY COLLEGE OF ENGINEERING, YADRAV</th>
<th>KAVIKULGURU INSTITUTE OF TECHNOLOGY &amp; SCIENCE (KITS), NAGPUR</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 &amp; 17-1-2016 - during two days university level hands-on workshop on Hibernate and Spring</td>
<td>19-1-2016 - Mr. Venkateswara Rao during Expert lecture on Virtualization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KAVIKULGURU INSTITUTE OF TECHNOLOGY &amp; SCIENCE (KITS), NAGPUR</th>
<th>K. K. WAGH INSTITUTE OF ENGINEERING EDUCATION &amp; RESEARCH, NASHIK</th>
</tr>
</thead>
<tbody>
<tr>
<td>13-1-2016 - Mr. Muni Shekhar Reddy during one day seminar on Industry Perception-Cloud Computing</td>
<td>11-2-2016 - Student participants appearing for the C / C++ Quiz Competition</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNIVERSAL COLLEGE OF ENGINEERING, VASAI</th>
<th>LATE G. N. SAPKAL COLLEGE OF ENGINEERING, NASHIK</th>
</tr>
</thead>
<tbody>
<tr>
<td>29-1-2016 - Mr. Sridhar Iyer delivering a Technical Talk on Digital Forensics</td>
<td>19 &amp; 20-1-2016 - Prof. Wankhade with Mr. Anand Shirsat during Two days workshop on Android Application Development</td>
</tr>
</tbody>
</table>

#REGION-VII

<table>
<thead>
<tr>
<th>EINSTEIN COLLEGE OF ENGINEERING, TIRUNELVELI</th>
<th>SRM UNIVERSITY, KATTANKULATHUR</th>
</tr>
</thead>
<tbody>
<tr>
<td>25-01-2016 - Dr. Ramar, Ms. Subha, Prof. Suresh Thangakrishnan &amp; Mr. Ravikumar during Quiz competition</td>
<td>4-2-2016 - Mr. H. R. Mohan, Immediate past president, CSI inaugurated the CSI Student Branch</td>
</tr>
<tr>
<td>REGION-VII</td>
<td>REGION-VII</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>SKR ENGINEERING COLLEGE, CHENNAI</strong></td>
<td><strong>SKR ENGINEERING COLLEGE, CHENNAI</strong></td>
</tr>
<tr>
<td>6-1-2016 – Dr Senthil Kumar, Mr Karthick, Dr Senthil Kumar, Mr Prem, Mr Satish, Dr Divya Satish &amp; Dr Suguna during FDP on Mobile Application Development on Android</td>
<td>8 &amp; 9-1-2016 – Ms Kanmani, Dr Suguna, Mr Gowtham, Mr Rathish Babu &amp; Mr Sivakumar during two days workshop on Cloud computing</td>
</tr>
<tr>
<td><strong>SCAD COLLEGE OF ENGINEERING AND TECHNOLOGY, CHERANMAHADEVI</strong></td>
<td><strong>SCAD COLLEGE OF ENGINEERING AND TECHNOLOGY, CHERANMAHADEVI</strong></td>
</tr>
<tr>
<td>7-12-2015 to 13-12-2015 – Mr. Harold Robinson, Dr. Suresh, Dr. Jessiah Selval, Mr. Daniel Prakash, &amp; Mr. Balaji during FDP on Compiler Design</td>
<td>5-1-2016 to 11-1-2016 – during one week FDP on MS- Access and Outlook</td>
</tr>
<tr>
<td><strong>KONGU ENGINEERING COLLEGE, PERUNDURAI</strong></td>
<td><strong>NANDHA COLLEGE OF TECHNOLOGY, ERODE</strong></td>
</tr>
<tr>
<td>15-2-2016 – during Tamil Nadu State Level CSI Student Convention</td>
<td>27-1-2016 – Dr. Thamarai Selvi, MIT, Chennai delivers lecture during Academic Seminar on Cloud Computing</td>
</tr>
<tr>
<td><strong>VIT, VELLORE</strong></td>
<td><strong>NATIONAL ENGINEERING COLLEGE, KOVILPATTI</strong></td>
</tr>
<tr>
<td>27-1-2016 to 29-1-2016 Prof. Govinda, RVP-VII &amp; Prof. Karthikeyan distributing prizes to the winners during three days workshop on Riddler</td>
<td>27-10-2015 – Mr. Jerart Julus, SBC delivers lecture during one day Seminar on Preventive Vigilance as a tool of Good Governance</td>
</tr>
<tr>
<td>Date</td>
<td>Event Details &amp; Contact Information</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4 March 2016</td>
<td>National Round of CSI YITP awards at Freedom Fighter M P Baya Hall - The Institution of Engineers (INDIA), Udaipur Local Centre, Hiran Magri Sector-11 Udaipur- 313002</td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Dr Nilesh K Modi : +919662640500, Mr Amit Joshi : +919904632888 128,</td>
</tr>
<tr>
<td>9 March 2016</td>
<td>State Level Student Convention Organized by CSI Raipur Chapter Division IV on Communication in Association with Department of Computer Science and Engineering &amp; Information Technology S S I P M T Raipur</td>
</tr>
<tr>
<td></td>
<td><strong>Venue:</strong> Academic Block SSIPMT Raipur <a href="http://www.scipmt.com">www.ssipmt.com</a></td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Dr. J P Patra <a href="mailto:patra.jyotiprakash@gmail.com">patra.jyotiprakash@gmail.com</a>, 8305665004</td>
</tr>
<tr>
<td>4-11 March 2016</td>
<td>First International Conference on Data Engineering and Communication Technology-ICDECT at LAVASA, Pune <a href="http://www.icdect.com">www.icdect.com</a></td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Prof Suresh Limkar <a href="mailto:icdect2016@gmail.com">icdect2016@gmail.com</a> 9823328686</td>
</tr>
<tr>
<td>12-13 March 2016</td>
<td>CSI Golden Jubilee National Student Convention Organized by CSI GLA University Student Branch, GLA University, Mathura, UP, in association with CSI Mathura Chapter, Region-I &amp; Div-I, <a href="http://www.gla.ac.in/CSIINSC">www.gla.ac.in/CSIINSC</a></td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Mr. Keshav Goyal, <a href="mailto:keshav.goyal_c12@glu.ac.in">keshav.goyal_c12@glu.ac.in</a>, Mob. - 9837002003</td>
</tr>
<tr>
<td>14-15 March 2016</td>
<td>CSI AP State Student Convention Venue : NBKR Institute of Science and Technology, Vidyanagar, Nellore, Andhra Pradesh,</td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Dr. S. Maruthuperumal, Professor, CSE, SBC-CSI, NBKRIST 9848772088</td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Prof. M. N. Hoda, <a href="mailto:Conference@bvicam.ac.in">Conference@bvicam.ac.in</a>, <a href="mailto:indiacom2016@gmail.com">indiacom2016@gmail.com</a></td>
</tr>
<tr>
<td>18-19 March 2016</td>
<td>National Seminar on “Assemblage of Digital Era -2016” Venue: The Bhopal School of Social Sciences, Bhopal</td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Jincy Renjiy Thomas, Email-IId: <a href="mailto:jincyrenjay78@gmail.com">jincyrenjay78@gmail.com</a></td>
</tr>
<tr>
<td>28-29 March 2016</td>
<td>Workshop on research Methodology and Research Opportunities, AES Institute of Computer Studies, Ahmedabad University, Ahmedabad. <a href="http://www.aeics.ac.in">www.aeics.ac.in</a></td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Dr. Sandeep Vasant, <a href="mailto:sandip.vasant@gmail.com">sandip.vasant@gmail.com</a></td>
</tr>
<tr>
<td>23 April 2016</td>
<td>International Conference on “Advances in Information Technology and Computer Science and Engineering” at Uttarakhand University, Dehradun</td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Mr. Sumit Chaudhary, Mob: 09917155889, <a href="mailto:iiimtsmit@gmail.com">iiimtsmit@gmail.com</a></td>
</tr>
<tr>
<td>10-11 May 2016</td>
<td>National Conference on Recent Trends in Computer and Communication Technology (RTCCT 2016) at Sarvajanik College of Engineering and Technology, Surat, Gujrat. <a href="http://www.rtcct2016.scet.ac.in">www.rtcct2016.scet.ac.in</a></td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> info <a href="mailto:rtcct16@scet.ac.in">rtcct16@scet.ac.in</a>, Phone: 0261-2240145-158</td>
</tr>
<tr>
<td>28-30 May 2016</td>
<td>International Conference on Computational Intelligence and Informatics (ICCII-2016) by Dept. of CSE, JNTUH College of Engineering, Hyderabad <a href="http://www.iccii.net">www.iccii.net</a></td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> 7680995513, <a href="mailto:convener.iccii2016@jntuh.ac.in">convener.iccii2016@jntuh.ac.in</a></td>
</tr>
<tr>
<td>18-19 August 2016</td>
<td>International Conference on “Internet of Things” Venue : APS College of Engineering, Bangalore <a href="mailto:hodcse.apsce@gmail.com">hodcse.apsce@gmail.com</a></td>
</tr>
<tr>
<td>16-17 Sept. 2016</td>
<td>2016 International Conference on Frontiers of Intelligent Computing: Theory and applications (FICTA), KIIT University, Bhubaneswar. <a href="http://www.ficta.in">www.ficta.in</a></td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> <a href="mailto:fictaconf@gmail.com">fictaconf@gmail.com</a></td>
</tr>
<tr>
<td>8-10 Dec. 2016</td>
<td>CSI-2016 Computer Society of India’s 51st Annual Convention on Digital Connectivity - Social Impact Organized by CSI - Coimbatore Chapter</td>
</tr>
<tr>
<td></td>
<td><strong>Contact:</strong> Mr. Ranga Rajagopal, Convener, 9442631004 <a href="mailto:office@csi-cbe.org">office@csi-cbe.org</a></td>
</tr>
</tbody>
</table>
FORM IV
(Rule No. 8)

Statement about ownership and other particulars of the ‘CSI Communications’

1. Place of Publication
   Computer Society of India
   Unit No. 3, 4th Floor, Samruddhi Venture Park,
   Marol MIDC Area, Andheri (E). Mumbai 400 093.

2. Periodicity of its Publication
   Monthly

3. Printers Name
   Mr. Sanjay Mohapatra
   Indian
   Computer Society of India
   Unit No. 3, 4th Floor, Samruddhi Venture Park,
   Marol MIDC Area, Andheri (E). Mumbai 400 093.

4. Publishers Name
   Mr. Sanjay Mohapatra
   Indian
   Computer Society of India
   Unit No. 3, 4th Floor, Samruddhi Venture Park,
   Marol MIDC Area, Andheri (E). Mumbai 400 093.

5. Editor’s Name
   Dr. A. K. Nayak
   Indian
   Computer Society of India
   Unit No. 3, 4th Floor, Samruddhi Venture Park,
   Marol MIDC Area, Andheri (E). Mumbai 400 093.

6. Names and Address of Individuals who own the newspaper and partners or shareholders holding more than one percent of the total capital

I, Sanjay Mohapatra, hereby declare that the particulars given above are true to my knowledge and belief.

1st March, 2016