

8th Edition
March, 2016

The Cyber Time



**Sardar Patel University of Police, Security &
Criminal Justice, Jodhpur**

(Established by Government of Rajasthan)

FACE OF THE EDITION



John McAfee

Software developer, founder of [McAfee](#), Chairman of Future Tense Secure Systems.

John David McAfee (born September 18, 1945) is an American computer programmer, businessman, and 2016 Libertarian Party presidential candidate. He is the developer of the first commercial anti-virus program. This bore the McAfee brand-name for years, until it was bought by Intel and given the Intel name. His wealth peaked at \$100 million, before his investments suffered in the global crisis of 2007. McAfee also has interests in smartphone apps, yoga, and all-natural antibiotics. He resided for a number of years in Belize, but after several disputes with the authorities in Belize and Guatemala, he returned to the United States in 2013.

Ref.: https://en.wikipedia.org/wiki/John_McAfee
<http://www.whoismcafee.com/>

Mar.2016, 8th Edition

The Cyber Time

An initiation towards cyber security...

EDITORIAL

A warm welcome folks.

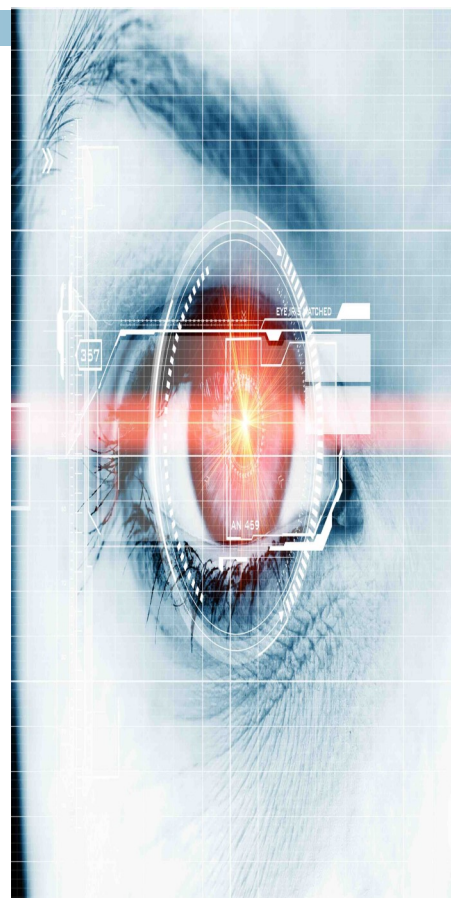
It gives us immense pleasure to publish this newsletter “The Cyber Time” 8th Edition. The purpose of this newsletter is to provide specialized information to a targeted audience. Through this edition readers will come to know about the recent changes in the cyber technology round the globe.

The Newsletter Team is very thankful to Department of Computer Science and Engineering as well as university administration for supporting us. We sincerely hope that this edition makes an interesting read. Please feel free to offer any suggestions for improvement.

Enjoy this edition, and please send your valuable feedback at editors@policeuniversity.ac.in

We wish you a happy and prosperous Holi. On Holi enjoy this edition . :)

All the best, and keep on reading!



Inside cover story:

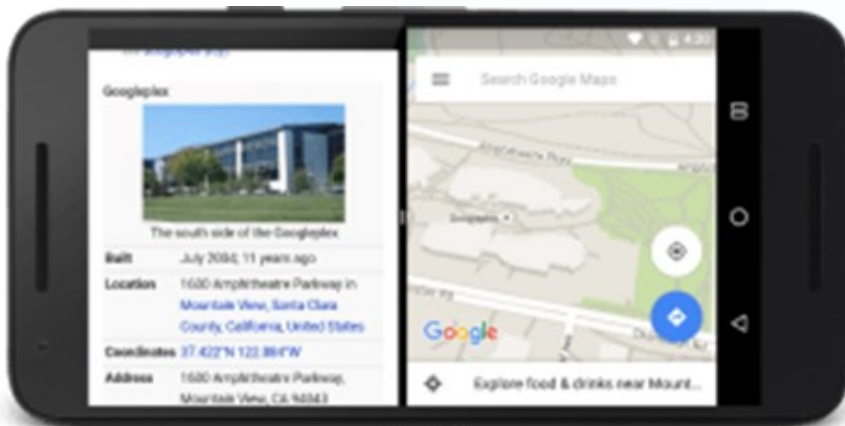
<i>Android N</i>	4
<i>Google as a tool for Hackers and PT</i>	8
<i>Cyber Crime ?</i>	13
<i>Ransomware</i>	16
<i>Big Data</i>	19
<i>News Bulletin</i>	22

ANDROID N



Android 7.0 is supposed to be named as Nectar, however others suggest that it could be Nectar, Neapolitan, Nacho or Nougat but not Nugget. Google too hasn't disclosed that what will be its actual name. Google CEO, Sundar Pichai during his visit to India in December suggested that they will conduct online poll, so that users can be able to suggest the name for the Android N. As of now, no official announcement has been made yet.

#1 Split Screen Multi-Tasking Function

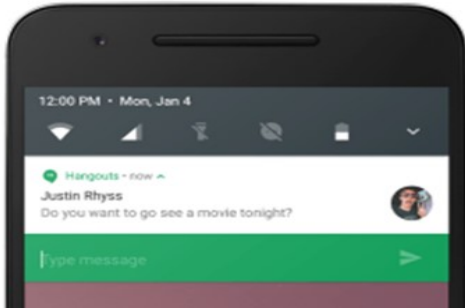


The upcoming android version will come multitasking function, which means you can run two different apps at the same time. When the user will opt for multitasking mode, the screen will show two apps side by side and are separated by a line. User can also adjust the size of the open apps, which means you can make one open app window smaller and other larger or same size. The devices with big screen will be able to choose **"Freeform"** mode which

lets the users to freely re-size each activity.

However, Freeform feature depends on the phone manufacturers whether they will keep this mode in addition to split screen mode.

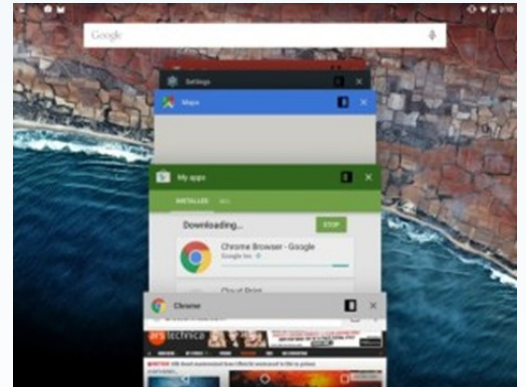
#2 Reply Directly From Notifications



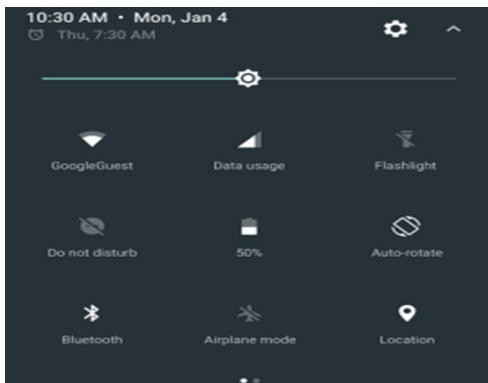
Reply from notifications is also packed in Android 7.0 N, which means you can directly reply to notifications including messages. The new interface will also allow you to see more app information. Google said “When a user replies via keyboard, the system attaches the text response to the intent you had specified for the notification action and sends the intent to your handheld app.”.

#3 Project Svelte | Minimize RAM Usage

Google is working on Project Svelte in order to minimize RAM usage by apps and system in the wide variety of android devices. Svelte is concerned to optimize the apps running manner in the background. Google states “Also, we’re continuing to invest in Project Svelte, an effort to reduce the memory needs of Android so that it can run on a much broader range of devices, in N by making background work more efficient .”



#4 Refurbished and Quick Settings



Google has moved forward to add Quick Settings and have added additional Quick Settings Tiles which can be used by swiping display to left or right. Besides this, Google will also allow the user to set Quick Settings Tiles appearance and location where you want to display them. It also lets the user to add or move tiles by dragging and dropping them.

#5 Now control the Pile of Notifications Mess

Are you getting piles of notifications? If yes, then upcoming android version will help you to sort out that mess. Android N is coming with a new feature called “Bundled Notifications”, which allows the user to combine notifications together from every app which means if you are receiving many notifications from Facebook App, you will see all notifications of it at one place, so your device won’t be flooded with notifications from same app.

Moreover, user need to tap the bundle in order to receive individual alerts. Bundled Notifications is quite similar to Notifications Stack present in Android Wearable Devices.

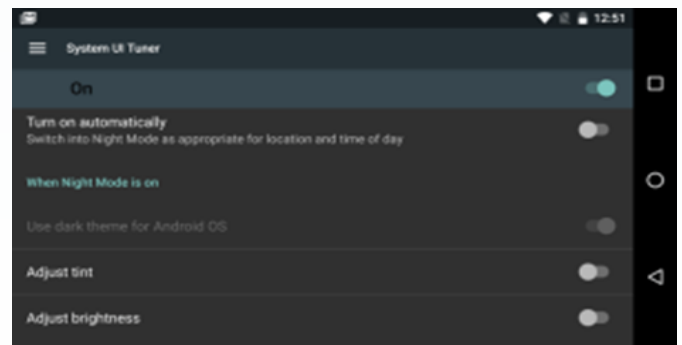
#6 Improved Battery efficiency



Android N is expected to come with improved battery efficiency. The current latest version of Android which is 6.0 Marshmallow came with “Doze” feature which puts the device in sleep mode when left idle. If your device’s screen is off, doze mode will also work.

#7 Night Mode

Are you waiting eagerly for Night Mode Feature in Android? If yes, Android N is also coming with this feature This feature will automatically activate the night mode depending upon time or location where you reside. Apple’s iOS is having the similar feature which it calls “Night Shift”.



#8 Better Java 8 Language Support



Google stated that Android N will also come with Java 8 Language features. This feature will let the users to use Java 8 Language features, Lambdas and much more on Android Versions as far back as Gingerbread.

Android N is coming with enticing features and there are still few months left for the launch of Android 7.0 N. If you have more to add, you are welcomed to add it in the comment section.

-SHIVAM SINGH
(M.Tech. Cyber Security — 1st Year)

GOOGLE AS A TOOL FOR HACKERS AND PENETRATION TESTERS

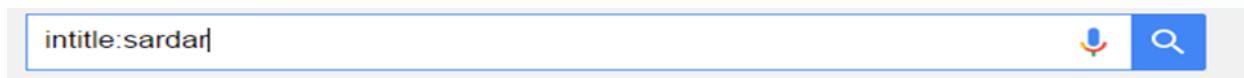


Google.com is popular and most used web based search engine on the internet, it provide easy, nice look and feel interface which is copyright protected, but most of the people do not know about Google is that how powerful is Google's interface is. So what behind this simple interface makes Google a powerful tool? Let start from its operators because these are powerful component of Google.

#Google Operator's

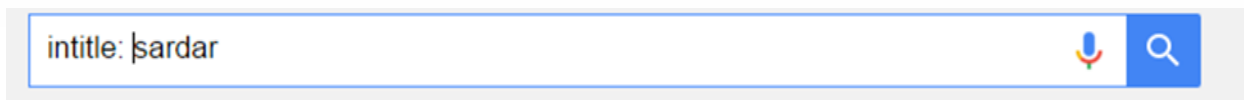
Google provide advanced operators to perform more advanced queries, using these operator's you can find exact results in less time. Before discussing about these operators, we will discuss right syntax to use them. Let we have an operator "intitle" which search a word or string in title of webpage (Note: Type in Google search box as in image)

operator:search_term >> Right syntax



The query is "Intitle:sardar" this will search "sardar" in all Google cache pages and print results according to page rank. Look at the results, it will show all Webpages which have "sardar" in their title. You can also use it like intitle:"sardar patel" this will search "sardar patel" whole string together and intitle:sardar.patel both will work same but time taken by these two are different, so it's about choice which one you prefer.

operator: search_term >> Wrong Syntax



S.N	Operator	Functionality	Example
1	intitle	Search word or string in title of the page	Intitle: "sardar"
2	allintitle	Search more than one word in title of the page	allintitle: sardar patel university
3	inurl	Search word or string in URL	Inurl:policeuniversity
4	allinurl	Search more than one word in URL of the page	allinurl: police university jodhpur
5	site	Search word and string in given site, if no search query is supplied or only site is mentioned then it will return all possible links on that site.	site:policeuniversity.ac.in Results (will search "Results" at policeuniversity.ac.in and give you Results page of policeuniversity.ac.in)
6	intext	Search word or string in text of pages (Look at the example you can use one and more operators together with +,-, as AND, NOT, OR respectively)	<i>intext:Mongolia</i> <i>+site:policeuniversity.ac.in</i>
7	allintext	Same as allintitle and allinurl but this will search words in text area only.	<i>allintext:Workshop and seminar</i> <i>police university</i>
8	filetypeE	Search for only specific file extension	<i>filetype:pdf</i> <i>+site:policeuniversity.ac.in</i> (will list all available PDF files available on site)
9	cache	Use to list cache page of a site stored by Google cache	<i>cache:policeuniversity.ac.in</i> (Show list of cache copy of the site)

Table No.1: Google Operators

Note: allintitle, allinurl, allintext works alone, do not use these operators with another operator. These are the most useful operators of Google, it provide more operators you can take a look [Here](http://libguides.mit.edu/c.php?g=176061&p=1159512). (<http://libguides.mit.edu/c.php?g=176061&p=1159512>)

Now you will say what the big deal in this, I can search this query's directly typing my string in Google search box. But look table No 2 and try these queries

S. No.	Query	Operation
1	<i>intitle:"Live View / - AXIS" inurl:view/view.sht</i>	This will print all open Axis web camera available on internet. Hacker can use it for social engineering or break the authentication system to gain full access or he can try Default passwords to access these cameras.
2	<i>inurl:"sap-system-login"</i>	Gives list of login portals of SAP systems.
3	<i>inurl:"ViewerFrame?Mode="</i>	Panasonic Network cameras
4	<i>inurl:aboutprinter.shtml</i>	Network printers (if found one break the authentication and gain access the printed document)

Table No.2: Usefulness of Google operators

For more Databases [Google Hack DB](#).

(<https://www.exploit-db.com/google-hacking-database>)

2. Use Google.com to crawl a website

Google.com continuously crawl sites available on World Wide Web and stores in Google cache, so later user can browse cache pages, if websites goes down. Now what is useful in that, the answer is you can crawl entire webpage without sending a single packet to original web-server.

So how to use Google cache? How to crawl websites? Simple you know more about Google operator now use it, type this in Google search box:

cache:policeuniversity.ac.in

This will show cache page of given URL. Do not click any link otherwise it will redirect you to main site, Just copy URL of the link and open in cache only like

cache:URL

The Cyber Time:

To verify that we are not sending request to website. First open this side to view your public IP www.whatismyip.com

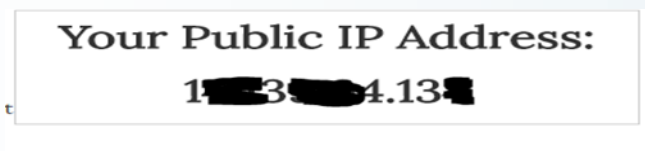


image 1: My public IP 1xx.x3xx.x4.1x

Then open cache page of this website by typing this on Google search box *cache:* www.whatismyip.com

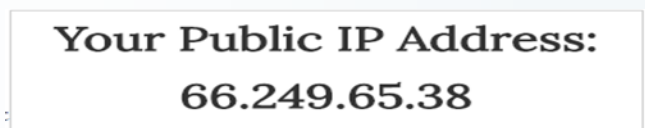


Image-2: My Public IP in Google cache page, showing that this page is crawl by 66.249.65.38, not from Gateways IP Address

Note: Use Google operators wisely, do not create more requests at once otherwise Google will block your IP.

Conclusion:

The Google.com is not only for searching stuffs, but it is a good tool for Hackers, Researchers and Students who are digging information on the internet, simple Google queries help them but if they have knowledge of Google's operators, then they can discover more knowledge in less time. Google.com is also useful for penetration tester to find what kind of information of client is publicly available on Internet, and to find possible targets on the internet. And of course it is fun to find more useful and interesting information available on WWW. Google is also a great social engineering tool which provide lot of information which is available online, and if you have doubt on capabilities of social engineering hit this on Google search box "*intitle:guccifer intext:social.engineering*".

The Cyber Time:

References:-

- 1) www.google.com
- 2) <https://www.exploit-db.com/google-hacking-database>
- 3) Johnny Long Presentation In: Google Hacking for penetration testers, available at https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf

-NARENDRA PAWANR
(M.Tech. Cyber Security — 2nd Year)

CYBER CRIME ?



What Is Cyber Crime?

“The intelligence of any Machine /Device is uses for making control on another device (non-intelligent/intelligent) or there is intentionally doing that work, is comes under Cyber Crime.”

Non-Intelligent:-Less Secure machines (very few security mechanism are uses)

Intelligent:-High level security mechanism uses.

Source of making crime:-

1. Network level Cyber Crime
2. Host level Cyber Crime

Network level Cyber Crime:-The whole network is compromised by Hacker/Attacker and the network is uses as a Botnet for making Crime or accessing valuable data from the network.

Host level Cyber Crime:-Any Particular system is compromised and digital data are theft or making control on that machine.

Botnet:-Spreading Malware automatically, treat like a robot.

Some Possible Attacks on Sources:-

Attack	Description	Recently happened
Trojans	A malicious programme which itself ensnare to a victim to install it.	September 2105: Trojan “Shifu” affected at least 14 banks in Japan.“Shifu” is capable of stealing data from smart cards if it discovers a smart card reader attached to the compromised endpoint. It can search for steal from crypto-currency wallets on infected system.
Distributed Denial of Service (DDoS)	Works by bringing down or disable individual websites, computer or network, it is flooding them with data’s.	May 2015: An International hacker group hacker launched DDoS attacks on BOCHK and the Bank of east Asia Demanding payment in Bitcoin.
Viruses and Worms	These can be attach itself to another programme in order to reproduce.	October 2015: A Virus “Tyupkin” that causes ATMs to bounce out cash by plugging in a USB drive or rebooting the ATM after taking of the side or back panel
Zero-day attacks	Zero-day vulnerability refers to a hole in software that is unknown to the vendor. It allows the infiltration of Malware, spyware or unwanted access to user information.	October 2015: A zero-day attack place the Magento e-commerce platform. Attackers used a few IP addresses to scan for vulnerability versions of “Magmi”, an open source database client that imports data on to Magento

The Cyber Time:

Some Effective methods acting against Cyber Crime:-

1. IDS/IPS Technologies:-

Intrusion detection is the process of monitoring the activity occurring on the network or a computer system, and these activity analyzing for signs of possible incidents. Intrusion detection system (IDS) is software that automates the intrusion detection process. Intrusion prevention system (IPS) is a software which also attempt to stop possible incident. IDPSs basically focused on identifying possible incidents, IDPSs detect when attacker has successfully compromised a system by any vulnerabilities in the system.

2. Firewall:-

Is a network security system, it can be either hardware or software based works on defined rules. The defined traffic only allowed onto the network, and it defined in the firewall policy. Firewall are placed at different levels in a network. Two or more firewall in a network make a “Network Firewall Hierarchy”. If a firewall at the organizational level are known as “Root Level Firewall”. The Root level firewall act as gateway, that control the traffic.

Amazing things which are all over internet:-

- Hack the Pentagon — US Government Challenges Hackers to Break its Security.
- Russian Cyber crime Rule No. 1: Don't Hack Russians.
- The highest numbers of Cyber crime victims are located in Russia, China and South Africa.
 1. Russia:- 92%
 2. China:- 84%
 3. South Africa:- 80%
- Facebook's Vice President Arrested in Brazil for Refusing to Share WhatsApp Data

-VIKASH Kr. SAINI

(M.Tech. Cyber Security — 2nd Year)

RANSOMWARE



Hello folks, let me tell you a story. One day you wake up and see your smartphone with sleepy eyes. Instead of your Dearest message, your smartphone welcome with a red screen, alerting you, that all your important and lovely data on your phone will be deleted, if you don't pay \$150 to an unknown account within next 48-hours. Yes...this is Ransomware. One of the easiest ways for cyber criminals to extract money from victims.

As growing Internet of Things, Cyber Criminals interested in this field. Maybe you are feeling proud having smartwatch, a smart TV, an internet-enabled Car, and the concept of connected homes. Then I think you must be next target of Ransomware. All these Internet of Things (IoT), which are operated with Android and iOS based devices, all are targeted by new generation Ransomware.

So here I tell you something about this dangerous threat and how you protect your data from it.


Ransomware: it is type of malware that take over your device and encrypt your data to prevent you from accessing it. This type of malware ask user to pay the ransom money in form of Bitcoin. It is very hard to decrypt it back. Interesting fact even FBI suggest a Ransomware victim – just pay the Ransom Money.

Your files are encrypted.
To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **20/01/15 - 16:13** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**
Prior to increasing the amount left:
167h 59m 00s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted 2860 files.

Refresh Payment FAQ Decrypt 1 file for FREE Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

 **bitcoin**

1. You should register Bitcon wallet ([click here for more information with pictures](#))
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union

First Ransomware found in 1989, name is AIDS Trojan (Aids Info Disk) which hide directories and encrypt the bootable partition of device after 90 days and ask to user to renew the license, cost of \$189. Different type of Ransomware will do different things, but one thing is common that is to extort money from user.

Letter found that a crypto Trojan or virus, in which they encrypt the victim's data using their public key and victim must pay to decryption key. In 2015, Ransomware-as-a-service (RaaS) hosted on the Tox and making use of virtual currency for payment purpose. Some new techniques involved in ransomware and make it strong. Like Tor network, virtual Money, Smartphone, Large storage device. Involving Tor network criminal hide their server's location which store victims decryption key. Using Tor network criminal maintain their network for long time.

Virtual Money: Cyber Criminal ask money in the form of bitcoin, because its transfer cannot be traced. According to a report in 2014, First ransomware found to encrypt data on android smartphone by using AES encryption, encrypt the data on the Smartphones.

The Cyber Time:

How to protect your data:

- Keep backups all your important data that you do not want to lose.
- Try to use online data storage space.
- Make sure you run an active and updated antivirus.
- Think before clicking on unknown emails attachments.
- Don't use outdated tools like internet explorer.

In 2016 first Ransomware “Ransom32” spotted, which is written in JavaScript to infect Mac, Windows or Linux Computers.

Good News: in January, 2016 one of ransomware which target Linux based websites and servers by encrypting MySQL, Apache, and root directories of the targeted site and ask for \$453.99 to decrypt those important files. But it is very easily get rid of it.

Always browse the internet safely.

-VIKAS YADAV

(M.Tech Cyber Security — 2nd Year)

BIG DATA



A word or a term Big Data defines a very wide area or volume of data .
It is in two basic types: *structured and unstructured.*

Big Data is basically collection or a group of data ,it is very large and complex to use and handle. we use database management tools for use it . There are many hurdles to capture it , to visualize it ,to manage it , in searching , in analysing and sharing it. We can also say that big data management is a work by intelligence to storing managing and analysing the data to make it usable .There is a huge amount of data which is created and stored on a global level.

Characteristics:

We can define big data characteristics in form of V's : Variety ,Volume, Velocity, Veracity, Variability and Complexity

Variety : It contain all types of data and in any form of data ,like audio, video structured ,unstructured , text file ,transaction file ,document file etc. We can say that it defines variety or a nature of data ,which help us to effectively analyse it. stored and generated data quantity.

The Cyber Time:

Velocity: It contain all those data which based in assumptions, on theory, and it contain data which use to save or handle the real time problems .We can say that it describe , the speed at which the data is generated and processed to meet the demands.And also defines the challenges that lie in the path of growth and development.

Veracity: It analyze the quality of data which is captured can vary greatly and affecting accurate analysis.

Variability: It contain increasing velocities and different varieties of data , data flows can be highly incompatible or inconsistent with periodic peak daily, weekly ,monthly ,yearly ,seasonal and event-triggered peak or important data loads can be challenging to manage. Even more challenging with unstructured data.

Complexity: Today's data can be come from different sources, it is very difficult or challenging to linked it, correlated it ,match it and connected it and transform the data across the system. It's necessary to connect, match and correlate relationships, hierarchies and linkages of multiple data or your data can quickly spiral out of control.

Importance of Big Data:

The general question arise in our mind is that - Why Is Big Data Important?

It is important for these aspects :

- To reduce the cost
- For smart decision making,
- To new product develop and optimizing,
- For time reduction,
- Increase usability,
- Finding root causes of failures, determining issues of failure and defects in near-real time

The Cyber Time:

- Recalculating and analyzing entire risk portfolios in minutes .
- Detecting fraudulent behavior which affects your organization.
- Increase development of next generation product.
- Increase innovation.
- Increase customer satisfaction.
- Sharpen competitive advantages.

Limitations to the use of big data:

- 1) **Prioritizing correlations:** Data analysts use big data to tease out correlation
- 2) **Security:** As with many technological endeavors, big data analytics is prone to data breach. The information that you provide a third party could get leaked to customers or competitor
- 3) **Transferability:** Because much of the data you need analyzed lies behind a firewall or on a private cloud.
- 4) **Inconsistency in data collection:** Sometimes the tools we use to gather big data sets are imprecise

-NEELIMA BAWA

(M.Tech. Cyber Security — 1st Year)



RAJASTHAN: [Govt. Promises Use of Technology for Crime Control](#)

Rajasthan Home Minister Gulab Chand Kataria today said the government will use high technology for crime control and management in the state. Replying to the debate on demands for grant for the home department in the assembly, Kataria said the police establishment is taking control of hardcore criminals and claimed that crime rate in the state has reduced as compared to the previous year. He also announced that the government would raise various allowances for the police, jail and civil defence departments.

INDIA: [India, Malaysia, Singapore And Japan Sign Pacts For Cyber Security](#)

NEW DELHI: The Indian Computer Emergency Response Team (CERT-In) and its counterparts in Malaysia, Singapore and Japan have signed three pacts for cooperation in cyber security. The pacts aim at promoting exchange of knowledge and experience in detection, resolution and prevention of security related incidents between India and these countries, said the Ministry of Communications and Information and Technology. The Cabinet chaired by Prime Minister Narendra Modi was today apprised of the MoUs (Memorandums of Understanding), said the ministry in a statement.

WORLD: [Security Researcher Goes Missing, Who Investigated Bangladesh Bank Hack](#)

Tanvir Hassan Zoha, a 34-year-old security researcher, who spoke to media on the \$81 Million Bangladesh Bank cyber theft, has gone missing since Wednesday night, just days after accusing Bangladesh's central bank officials of negligence. Zoha was investigating a recent cyber attack on Bangladesh's central bank that let hackers stole \$81 Million from the banks' Federal Reserve bank account.

CALL FOR ARTICLES

Students/Readers/Researchers are invited to get involved in the TechNewsletter activities by providing articles and other related materials. Suggestions and feedbacks for the improvement of the newsletter are most welcome and contributions are invited from the faculty and students of the department. Contributions can be from any of the whole gamut of activities in the department like any special achievement, an admirable project, a publication, and Cyber Crime case, Quiz, puzzles or even the fun section material like jokes, cartoons, interesting facts or poems. You can also report any interesting workshops or talks taking place in the department.

You can send your articles on: - ***editors@policeuniversity.ac.in***

Disclaimer: - If any of the article is found to be copied, the writer himself/herself will be responsible for copyright issues. Editor or University will not be liable for any issue.

Members of Newsletter



Janardan Kumhar

Shivam Singh

Sakshi Sharma

Neelima Bawa

Amar Verma



**Brought out by the Department of Computer Science & Cyber Security
Sardar Patel University of Police, Security & Criminal Justice, Jodhpur**