



SARDAR PATEL UNIVERSITY OF POLICE,  
SECURITY AND CRIMINAL JUSTICE



9th Edition

# CYBER TIME

What's inside?

- Ransomware
- Bitcoin
- Dark net
- cyberwar
- Artificial intelligence (AI)
- Data as a service .....

2017-18

O  
O  
O  
O  
O

# *Face of edition*

## *Elon musk*

When he was 12 he made his first software sale-of a game he created Blastar.. At age 17, in 1989, he moved to Canada to attend Queen's University and avoid mandatory service in the South African military, but he left in 1992 to study business and physics at the University of Pennsylvania.



After graduating he moved to Stanford University in California to pursue a Ph.D in energy physics. However, his move was timed perfectly with the Internet boom, and he dropped out of Stanford after just two days to become a part of it, launching his first company, Zip2 Corporation.

An online city guide, Zip2 was soon providing content for the new websites of both The New York Times and the Chicago Tribune, and in 1999, a division of Compaq Computer Corporation bought Zip2 for \$307 million in cash and \$34 million in stock options.

Also in 1999, Musk co-founded X.com, an online financial services/payments company.

An X.com acquisition the following year led to the creation of PayPal as it is known today, and in October 2002, PayPal was acquired by eBay for \$1.5 billion in stock.

Before the sale, Musk owned 11 percent of PayPal stock.

<https://www.biography.com/people/elon-musk-20837159>





## *Message from Registrar SPUP*

Our mission is to support the educational goals of the Institution, with an emphasis on creating awareness about growing dynamics of Cyber Security along with the academics. Our purpose is to provide students with services required in the planning and implementation of academics activities.

By publishing The Cyber Time, I hope that students will be aware about recent trends of Cyber Security along with The Cyber Laws associated with it, as this is the expectations and need of today's Community.

Sh. JC Purohit  
IAS, Registrar

# 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” 9th 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*

Preeti Chauhan (M.Tech. 3rd sem.)

Satya Prakash Mehra (M.Tech. 3rd sem.)

# WannaCry a Technical view

## History

Shadow Broker's a hacker's group leaked a load of tools/exploits believed to belong to the National Security Agency(NSA). They were trying to auction the exploit in black market. Auction failed. Now shadow brokers were not able to sell the exploits. So, they leaked the exploit. One such was ETERNAL BLUE.

The tech giant( Microsoft) has called it "MS17-010" and issued a security update

## Eternal Blue:

Its an windows vulnerability. Eternal Blue exploit or Server Message Block(SMB) is the transport protocol used by Windows machines for a wide variety of purposes such as file sharing, printer sharing, and access to remote Windows services. Now this vulnerability was used by some other hackers to create RANSOMWARE called **WANNA CRY** and **PETYA**



Satya Prakash Mehra  
M.Tech. 3rd Sem.

# IT Act 66A



—>What is IT Act 66 A

Section 66A defines the punishment for sending “offensive” messages through a computer or any other communication device like a mobile phone or a tablet. A conviction can fetch a maximum of three years in jail and a fine..

—>Why in news?

This section has been misused by police in various states and innocent person arrested by police for posting comments on social media related to political issues. It was biggest issues to strikes down 66 A by supreme court

—>Case study

The first petition came up in the court following the arrest of two girls in Maharashtra by Thane Police in November 2012 over a Face book post. The girls had made comments on the shutdown of Mumbai for the funeral of Shiv Sena chief Bal Thackeray. The arrests triggered outrage from all quarters over the manner in which the cyber law was used.

Varsha Tak  
M.Tech. 3<sup>rd</sup> sem.



# ANONYMOUS

WE ARE LEGION

WE DO NOT FORGIVE

WE DO NOT FORGET

EXCEPT US

The anonymous group which became the attraction point of the cyber world by its enormous methods to hack against the govt. as well as private agencies. They are not limited to a specific country or area. They have the attention of the whole world.

## Who is Anonymous?

A hacktivist group whose members are not known. There is no information about owner of the group. Anyone who has the potential to do something special in the world of hacking can be a part of it. All he/she has to do to convince the anonymous by his/her skills. Once it gets convinced, one can use the brand name of the group. Anyone can be a member of the group regardless of their nationality. It first came into existence in 2003, when unknown users tagged as Anonymous posted images on 4chan's /b/board. The images were of random things but they gained the popularity soon through the website and by doing some pranks and troll events. This group represent itself by wearing a Guy Fawkes masks in its videos and in public gathering too. The Anonymous members are also known as Anons.

In 2004, they started to use a website named as Encyclopedia Dramatica as a platform for their activities. Through which they got the attention throughout the world as they did some big mass pranks by using this website. They always communicate through the chat groups and if someone they find out with a new idea, they invite the one to the chat group and discuss ideas for further things. The people who support this group, they call its members 'The Freedom Fighters'.

## **What they want?**

As there are no specific goals of this group. Neither they mentioned anywhere that they want to achieve something or want to make the money as generally hacking groups want. Although they have a motto of anti-oppression. They are highly desired about the combat censorship, freedom of speech and the counter government control. They also hit the private agencies who oppress general public in any way.

## **How they do hacking?**

Anonymous known for its enormous methods which they use to crashing web servers, website defacement and leaking of private information. They have their tools and technologies in which maximum of them are not revealed. To carry out hacks it also works with other groups like LulzSec and AntiSec. They are very dedicated to go after its target. They are very keen to taking down the website which copies or spreads the propaganda about the terrorism.

Whenever they do hacking, they never leave a trail and sometimes Anonymous do hacking by giving a warning to the target by some video or some other multimedia messages. They are so efficient in their ways, till date no one is get to know the origin of this group.

## **Top hacks of Anonymous-**

Operation Avenge Assange

Project Chanology

Taking down Donald Trump's Towers' website

Charlie Hebdo shootings

Operation KKK (Ku Klux Klan)

OpISIS

2016 US presidential elections

OpNASADrones

OpPayback

Operation Cyber Privacy

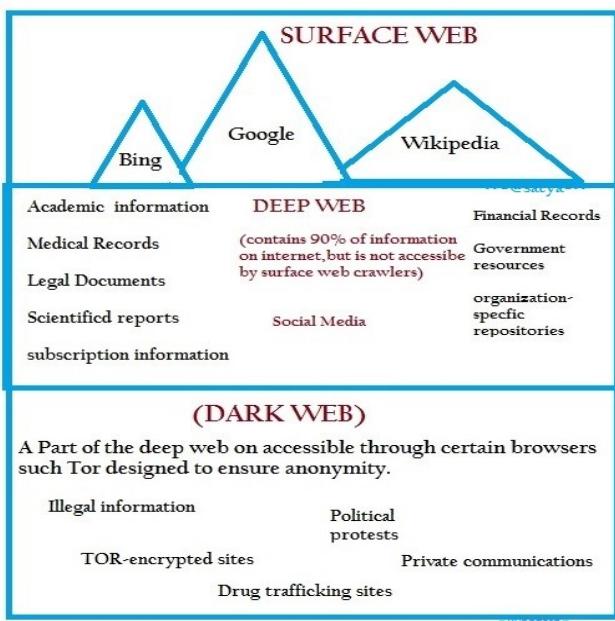
Shivraj Choudhary

M.Tech 3rd Sem.

# What is Deep web, Dark net, TOR?

Deep web is vast and 1000 times larger than the visible internet (such as Google) which is called **SURFACE WEB**. Deep web is not place it's simply an accounts for all of the unindexed data (the data which google not shows) online such as banking data, Administrative code for government, corporations and universities it's like looking under the hood of the internet.

Over the time the deep web became in habitat for all types of people for privacy (such as journalists, criminals, dissidents, whistle blowers, privacy advocates), this hidden area of deep web is called **DARK NET**.



And is accessible by software service called **TOR** originally developed by US military now open source and publically funded while law enforcement and media have painted a picture that TOR and dark net are various tools for criminals it's important to understand that it is largely used for good.nowadays the dark net is misused as it is slowly becoming hub for illegal activities such selling of drugs, pirated products such as movies,

But there is one phase where people use it for good purposes as revealing the truth about the various countries governments and its organization's one such issue is privacy. How the governments and its various agencies spy over its people in the name of security.The US governments runs a mass surveillance program through its agency National Security Agency(NSA) knowns a **PRISM** which collects data from all internet companies.

Some of India Mass surveillance program/monitoring system are following:

- Central monitoring system(**CMS**): the system is designed similar to NSA's PRISM program.
- NATGRID**: it is a centralized agency which stores sensitive personal information on citizens from most agencies to made available for counter terror investigations.

# *Social Media on Cyber Bullying linked to Teen Depression*



## **What is Cyber Bullying?**

The use of electronic devices for communication to bully a person, by sending messages of an intimidating, harassment or threatening in a deliberate and repeated manner is known to be cyber bullying .

***Examples of Cyberbullying*** include text messages or emails, rumours posted on social networking sites,

## **Why is Cyberbullying so harmful?**

Cyberbullying can follow victims wherever they go. Cyber bullies can reach their victims, 24 hours a day, 7 days a week, 365 days a year. They often post hurtful content online, anonymously, so that they cannot be traced or stopped.

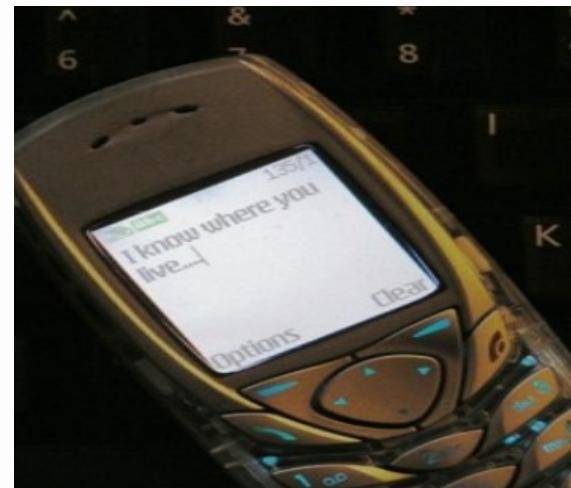
The nature of social media is so quick due to which content posted becomes viral sometimes, and reaches a large audience in the blink of an eye, making it difficult, even impossible for authorities to delete the harmful content before it results to damage.

## **A depressing effect:**

Teens usually take serious decision once they caught into bullying and went into depression condition because Cyberbullying is difficult to locate. Many victims feel helpless and unable to face with it, especially if the bullying is personal and long-drawn. It is no surprise, therefore, that this form of bullying has been known to trigger depression and anxiety in its victims. In many instances, it has also resulted in victims developing

## Safe social media:-

Mobile phones and computers are not to blame for Cyberbullying. Social media websites can be used for good activities like linking kids with their friends and family, helping students with school, and for entertainment. But these tools can also be misused to hurt or harm other people. Whether done by person or through technology, the effects of bullying are similar.



## Ways to fight Cyberbullying:-

1. Don't respond
2. Do Save the evidences
3. handle things with smartness tell the person to stop
4. Reach out for help
5. Use available technology and tools
6. Protect your accounts

## Legal rights against cyber bullying:-

If the cyber cell is not available in your place, you can file an F.I.R. in the local police station else you can also reach out to the commissioner or judicial magistrate of the city if you find any difficulty in filing an F.I.R. Irrespective of the jurisdiction any police station is bound to file an F.I.R.

Sl.No	offences	Section Under IT Act
1.	Publishing or transmitting obscene material in electronic form	Sec .67
2.	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Sec. 67A
3.	Word, gesture or act intended to insult the modesty of a woman	Sec. 509 IPC
4.	Sending defamatory messages by e-mail	Sec. 499 IPC
5.	Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail	Sec. 292A IPC
6.	Commits the offence of stalking	Sec. 354 D
7.	Making sexually colored remarks, guilty of the offence of sexual harassment.	Sec 354 A
8.	Punishment for violation of privacy	Sec. 66E
9.	Criminal intimidation by an anonymous communication.	Sec. 507
This is not a comprehensive list.		

Vishrant Ojha  
M.Tech. 3rd Sem.

# *Bitcoin: The currency of cyber world*



In the cyber world a bitcoin is become more valuable than anything else even more after the ransomware attacks which are happening all around the world and hackers are demanding bitcoins as in payment.

## **What is Bitcoin?**

Bitcoin is a digital token invented under the name of Satoshi Nakamoto in 2009. Bitcoin is accepted worldwide and based on decentralised network. There is no third party in between and transactions take place from one user to another user anonymously. Experts differentiate, Bitcoin(capitalized) as the digital currency and bitcoin(lowercase) as the network through which this digital currency moves. The network is designed in a special way to create the currency and the financial network so that there is no control of any government or any company. There is no central authority to run Bitcoin so no one can force the users to reveal their identities. One can buy anything electronically using Bitcoin.

## **How to buy Bitcoin?**

There are many companies such as Coinbase, BitPay, BitPesa in different countries which sell Bitcoin in the exchange of the local currency i.e. Dollar, Euro etc. To buy Bitcoin you have to open an account with the respective company which is same as when you open a bank account with a lots of verification details. They take the traditional money from you and in exchange they provide you the coin. One Bitcoin is worth \$3147 or 197711.19 Indian Rupee and this value is constantly changing in Bitcoin exchanges world like the stock market. Some people who don't want to reveal their identities, there are services like Local Bitcoins that connects local people to sell or buy Bitcoin for cash without any requirement of verification. To exchange Bitcoin is as easy as to sending an email. All you have to create a Bitcoin address.

## **Bitcoin Importance in the hacking world**

Bitcoin is completely a digital currency and exchange take place anonymously worldwide. Hackers are using this currency for demand ransom without getting caught by anyone. They don't have to reveal their identity for the transactions and then they use that Bitcoins for the real cash. As Bitcoin value fluctuates and risen quickly, they sell these Bitcoins in higher values and earn more and more cash.

## **Tracking of Criminals using Bitcoin: Possible or not?**

The Bitcoin transactions are recorded on the network's public ledger, known as the block chain. Some law enforcement agencies or financial authorities can sometimes use the block chain to track transactions among criminals. But it is not as simple as it seems to track them. Authorities can see the payments but it's tough to know who owns the wallet and criminals can wash the coins to throw off tracking using services called 'tumblers', that make a lot of trades back and forth with Bitcoins from lots of different sources. That means it's become hard to track the movement of the coins over the bitcoin network. Generally, the criminals who don't provide any identity with their Bitcoin address they are tough to trace.

Atul Kumar Gupta  
M.Tech 3rd Sem .

# DATA AS A SERVICE: what you can expect?



**DAAS** is a distribution model which provide data such as text, images, audio and video made available to customers over a network using internet. The concept of data-as-a-service (DaaS) is based on the view that with the emergence of service-oriented architecture (SOA), which includes standardized processes for accessing data "where it lives" the actual platform on which the data resides doesn't matter. With data-as-a-service, any business process can access data irrespective of where it resides. Data as a service is a cloud strategy used to provide the accessibility of enterprise-critical data in a well-timed, protected and affordable manner. DaaS depends on the principle that specifies, useful data can be supplied to users on demand anytime, irrespective of any organizational or geographical separation between consumers and providers.

The idea behind the DaaS model is all about offloading the risks and burdens of Data Management to a third-party Cloud-based provider. Traditionally, companies manage their own data within a self-contained storage system. The problem with this traditional model is that as data becomes more complex it can be increasingly difficult and expensive to maintain whereas with the DaaS Cloud computing model, data is readily accessible through a Cloud-based platform. Simply DaaS is a new way of accessing enterprise-critical data within an existing data center. In the DaaS environment information can be delivered to a user regardless of organizational or geographical barriers.

A few DaaS providers are Urban Mapping, a geography data service, provides data for customers to embed into their own websites and applications. Xignite is a company that makes financial data available to customers.

## **Benefits of Data-as-a-Service**

**Agility:** As the DaaS providers are based on service oriented architecture(SOA) we get more flexibility.

**High Quality Data:** we get improved data quality which is largely due to the fact that the primarily data is controlled by the data service itself, this adds another layer of security and improves the overall quality.

**Cost Effectiveness:** Just like other cloud applications, Daas providers can deploy their applications in such a way that it reduces overall cost..

Preeti Chauhan  
M.Tech. 3rd sem.

# *Can artificial intelligence is safe?*



Artificial Intelligence (AI) is coming soon to a network near you. Limited forms of AI are already in use and much more powerful applications are in queue of development. That means there is no better time to start thinking about the suggestions of AI on cyber security.

## **AI working History:**

Speculation about AI in the form of robots has been popular for generations. Initially speculations were about the dangers that might be posed by malicious or mistaken robots. But for now with AI become more reality, its potential risks and benefits are no longer mere speculations. In past era, when people started thinking about artificial intelligence, they had only one point of reference to go by HUMAN INTELLIGENCE. Whether the robots were made to be look like more or less human. They were also imagined to do the things in the same way as human do, including both behavior and feeling part. But AI in real life has developed in an entirely different fashion. For example: it was once assumed that any computer which is able to play champion level chess would need to think in the same way as humans do. In fact, we still do not able to understand that how top players play so well and computers still beat them anyway. They use the brute force capability of testing millions of possible moves, something no human can do to, find the best option. So at present AIs are not subject to emotions or motivations of any sort.

They do what they learn from their tasks and experiments having a bar on emotions and motivations.

## **Matching Human Intelligence or concentrating human intelligence?**

Instead of matching the human intelligence it could be said that real world AI concentrates on human intelligence in the same way as a lever concentrated the user's strength onto the desired task. In fact, AI has a lot of things in common with institutional intelligence. Like an organization it can and does perform intelligent behavior, expressed by characteristics such as institutional memory and institutional learning so AI of tomorrow will be a sort of automated organization. Works on composite human machine learning is already focusing on network security issues. MIT researchers are working on a system AI2 which combines AI with human analyst intuition looks for patterns which it then represents to its human partners for evaluation and it is assumed that it would predict the 85% of cyber-attacks using input from human experts. Those human insights improve the machine's ability to ignore nonthreat patterns while still warning of potentially dangerous ones.

## **A Whole New Meaning of ‘Trusted Users’**

Once human social learning is added to the AI mix, a new and subtle security challenge emerges. Now a day's one of the leading security threats is social engineering such as spear phishing, which tricks users into making security mistakes. Social learning for AIs introduces the risk that malicious teachers could trick the AI or even subvert it into helping attackers. Designers need to ensure that only trusted teachers have access to the AI, particularly in the critical initial stages of learning before the AI has been taught to be wary of suspicious lessons. The risks can come not only from deliberately malicious users, but also from careless ones who could inadvertently teach the wrong lessons. If the AI resembles AI2 in being designed for security tasks, the challenge of identifying is even more critical.

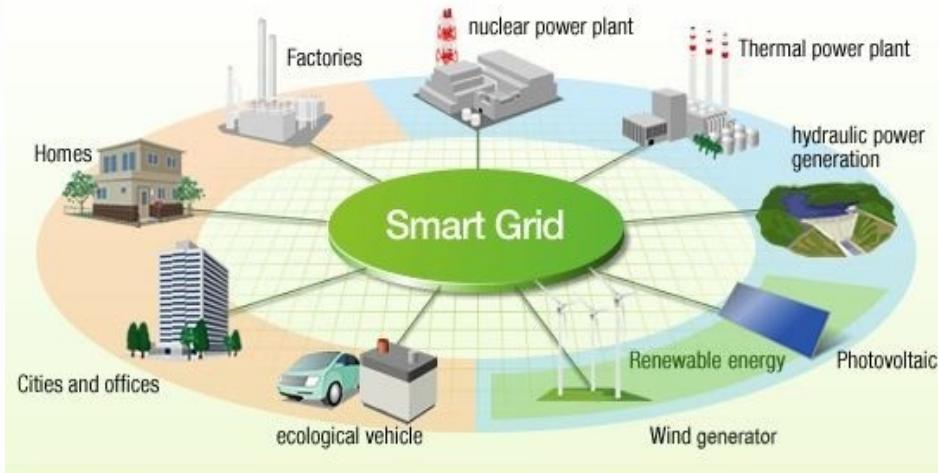
Can we achieve this level of user security? As applied to AI, the challenge is a new one, but it is really the oldest security challenge of all —as the Latin proverb asks, “*Quis custodiet ipsos custodes?*” Who will guard the guards themselves?

All security is ultimately about human trust. This will not change, even as we enlist AIs to be our security partners.

Atul Kumar Gupta  
M.Tech. 3rd sem.

# Risks Encircling Internet of Things (IoT) in Cyber Space

The Internet of Things is a giant collection of things connected to the network. These ‘Things’ comprises of anything ranging from physical devices, cellphones, sensors, coffee machines, refrigerators, buildings, wearables to automobiles. The main concept behind the IoT is to link all the physical assets to the network so as to compose an intelligent automated system where devices work in combination with each other to complete a specific task without requiring any human to human or human to computer interaction.



**SOURCE:** <https://goo.gl/LCG8xq>

**Fig1. A Smart Grid is an example of Internet of Things**

The fig1 illustrates a smart grid system where all the resources whether generating electricity or consuming electricity are together connected to a network. By collecting and analyzing data about production and consumption of electricity, the system could be made more efficient and fulfil electricity demand in a sustainable, reliable and economic manner. Thus we can expect a greener and more efficient electricity delivery system based on IoT. IoT describes a new & vast generation of cyber space where just about anything can be connected and communicate in a “smart mode” by combining simple data to produce usable intelligence. IoT has the potential to change the way we work in our daily lives

## **IoT Security:**

Internet of things agenda describes iot security as “**IoT security is the area of endeavor concerned with safeguarding connected devices and networks in the Internet of things.**”

Whenever we talk about network security we have a notion of thinking in terms of smartphones & Computers only. The reason behind this is that the concept of connecting entities to a network is relatively new and major portion of the world is unaware about it.

Till now two incidents have been reported where IoT threat became real:

**Stuxnet attack** where a malicious program “Stuxnet” was developed to disrupt Iran’s nuclear program. Stuxnet targeted Iranian programmable logical controllers (PLC’s) by collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart.

**Chrysler Jeep Hack**, where key systems such as engine management and braking systems were shown to be accessible using an external cellular connection.

## **Vulnerabilities in IoT:**

- Privacy: Raised privacy concerns regarding collection of data such as e-mail address, Date of Birth, Contacts, Photos/Media Files, Location and credit card credentials.
- Authorization: Failure to create passwords with strong strength and complexity with most devices allowing passwords such as “1234”, “abc”.
- Web Interface: Raised security concerns with user interfaces such as persistent Cross-Site Scripting (XSS), poor session management and credentials being transferred in clear text.
- Software: 60% users do not use encryption when downloading software updates, some downloads can be intercepted and extracted allowing the full code to be viewed or modified.
- Encryption: Critical security issues such as unencrypted communication to the cloud, key loss during communication which makes it impossible for data to be decrypted back and super users with broad privileges can potentially disable encryption.

Under such circumstances IoT Security is going to pose a big challenge in upcoming time. More connected devices mean more possibilities for hackers to target. While security experts are making constant efforts to secure IoT in cyber space but they aren't enough to ensure that we can leverage the full power of this new technology in a secure environment .

Divam lehri  
M.Tech. 3rd sem.



# Digital DNA

Imagine if everything you ever did lasted forever, your own version of immortality. Well in the digital world you already are immortal because as you chat with friends, listen to music, go shopping, buy concert ticket, organize parties in fact do almost everything in digital world and you're leaving behind your digital footprint and in most cases it lasts forever. In our everyday life , millions bytes of data procreates in a single minite. Generally it takes HDDs, PDs, cloud storage, or other electronic devises to store theis large amount of data. Don't you think , these electronic devices have some limitations?

"In data centres, no one trusts a hard disk after three years, No one trusts a tape after at most ten years. Where you want a copy safe for more than that, you need something more powerful tool and the 'thing ' is 'DIGITAL DNA'. Once we can get those written on DNA, and forget about it until you want to read it." The world is generating huge amounts of digital data, and scientists see DNA as an effective way of not only dealing with the volumes produced, but as a secure method of preservation. In the face of nuclear explosions, radiation exposure or extreme temperature fluctuation some bacteria can continue to exist -- data centers will not.

The latest experiment signals that interest in using DNA as a storage medium is surging far beyond genomics: the whole world is facing a data crunch. Counting everything from astronomical images and journal articles to YouTube videos, the global digital archive will hit an estimated 44 trillion gigabytes (GB) by 2020, a tenfold increase over 2017. By 2040, if everything were stored for instant access in, say, the flash memory chips used in memory sticks, the archive would consume 10–100 times the expected supply of microchip-grade silicon.

The idea of encoding data in DNA started out as a joke by Nick Goldman, but it was a tube light moment. DNA storage would be pathetically slow compared with the microsecond timescale for reading or writing bits in silicon memory chip. But with DNA, a whole human genome fits into a cell that is invisible to the naked eye. The researcher's biggest worry was that DNA synthesis and sequencing made mistakes as after as 1 in every 100 nucleotides. After several years of research, they got success in there mission.

## EVOLUTION

The first person to map the ones and zeroes of digital data onto the four base pairs of DNA was artist Joe Davis, in a 1988 collaboration with researchers from Harvard. The DNA sequence, which they inserted into *E. coli*, encoded just 35 bits. When organized into a  $5 \times 7$  matrix, with ones corresponding to dark pixels and zeroes corresponding to light pixels, they formed a picture of an ancient Germanic rune representing life and the Earth.

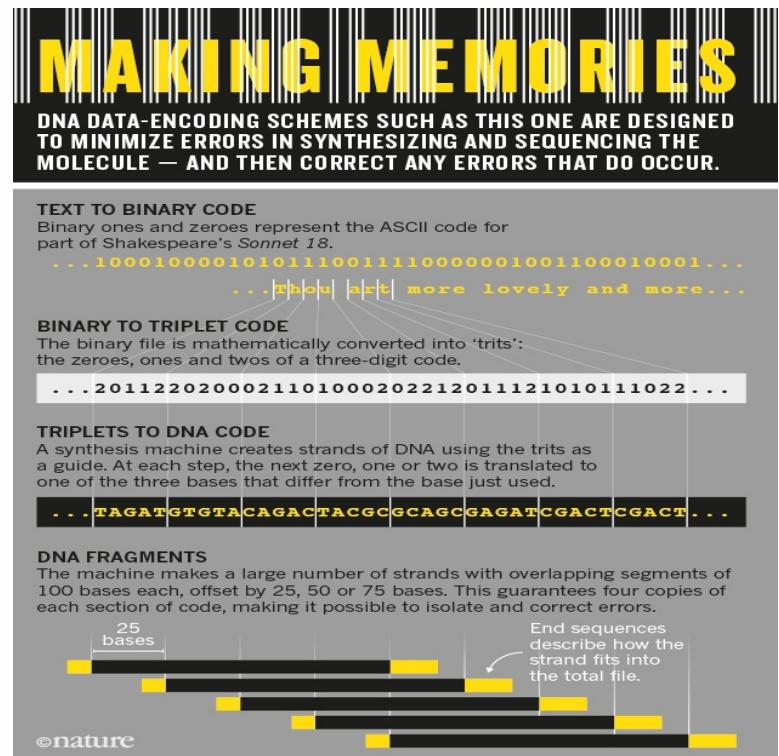
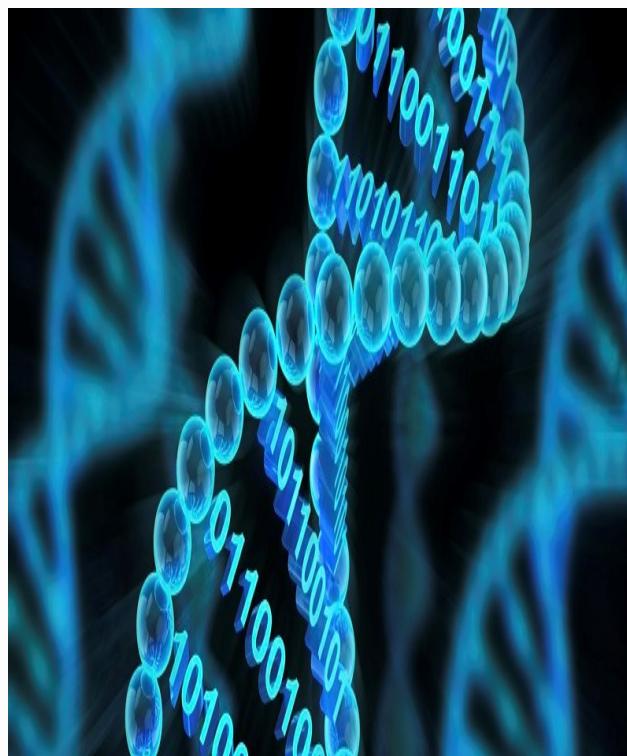
In 2013, the team used many short DNA strings to encode a 659-kB version of a book. Meanwhile, the other team were also using many strings of DNA to encode their 739-kB data store, which included an image, ASCII text, audio files and a PDF. Part of each string was an address that specified how the pieces should be ordered after sequencing, with the remainder containing the data. A binary zero could be encoded by the bases adenine or cytosine, and a binary one could be represented by guanine or thymine. That flexibility helped the group to design sequences that avoided reading problems, which can occur with regions containing lots of guanine and cytosine, repeated sections, or stretches that bind to one another and make the strings fold up. They didn't have error correction in the strict sense, instead relying on the redundancy provided by having many copies of each individual string. Consequently, after sequencing the strings, they found 22 errors — far too many for reliable data storage.

On July 2017, researchers describe using a Crispr system to insert bits of DNA encoded with photos and a GIF of a galloping horse into live bacteria. When the scientists retrieved and reconstructed the images by sequencing the bacterial genomes, they got back the same images they put in with about 90 percent accuracy.

Up till now, most of the research that was conducted into using DNA for storage involved synthetic DNA made by scientists. And this horse GIF, which is just a tiny  $36 \times 26$  pixels in size, represents a relatively small amount of information compared to what scientists have so far been able to encode in synthetic DNA. However, it is essential to understand that it is way more challenging to upload information into living cells than synthesized DNA, because live cells are constantly moving, changing, dividing, and dying off..

Although, interestingly, the benefit of hosting data in living cells like bacteria, they tend to offer better protection. For instance, some bacteria still thrive after nuclear explosions, radiation exposure, or extremely high temperatures.

Beside storing digital information as a use case scenario of this experiment, another researcher who was involved in the study says he wants to use the technique to make “living sensors” that can record what is happening inside a cell or in its environment.



Madhura  
M.Tech 1st sem.

# **Bigdata**

In the era of digital information BigData has emerged as a research area when it comes to deal with large amount of data. Big data is an evolving term that describes any voluminous amount of structured, semi structured and unstructured data that has the potential to be mined for information Although big data is not equal to any specific volume of data, the term is often used to describe terabytes, petabytes and even Exabyte's of data captured over time.

## **History**

BigData is new term, there is no years of history associated with it, but the act of gathering and storing data is something different. The concept of BigData come into momentum in the early 2000 when the analyst Doug Laney summarized the BigData in 3v's

The *volume* of data: The name 'Big Data' itself is related to a size which is enormous.

The wide *variety* of data: Variety refers to heterogeneous and distributed sources and the nature of data, both structured and unstructured. During earlier days, spreadsheets and databases were the only sources of data considered by most of the applications. Now days, data in the form of emails, photos, videos, PDFs, audio, etc. is also being considered in the analysis applications.

and the *velocity*: The term 'velocity' refers to the speed of generation of data. How fast the data is generated and processed to meet the demands, determines real potential in the data.

## **Benefits of Big Data Processing**

Ability to process 'Big Data' brings in multiple benefits, such as-

1. Access to social data from search engines and sites like Facebook, twitter are enabling organizations to fine tune their business strategies.
2. Traditional customer feedback systems are getting replaced by new systems designed with 'Big Data' technologies.
3. Early identification of risk to the product/services if exists any.
4. 'Big Data' technologies can be used for creating staging area or landing zone for new data before identifying what data should be moved to the data warehouse. In addition, such integration of 'Big Data' technologies and data warehouse helps organization to offload infrequently accessed data.

## **Who uses it?**

Banking, healthcare, government, education are few sectors .

## **How it works?**

The Primary sources for big data fall into three categories:

- Streaming data: This category includes the data which is reached to your system from a network of connected device, once it is arrived we can analyse and make decision on what data to keep, what not to keep and what requires further analysis
- Social media data: The data on social media is usually set of information regarding marketing, sales and support functions. It can be unstructured or semi structured forms therefore usually it's a challenge when it comes to analyse it properly.
- Publicly available sources: There is large amount of data which is available through open sources like the US government's data.gov, the CIA World Fact book or the European Union Open Data Portal hence they come under it.

Once we have identified the sources of data, we need to gather

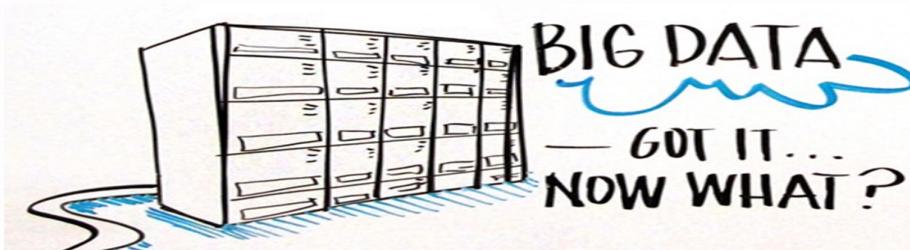
How to store and manage it?

How much of it is to analyse?

How to use any insights you uncover?

The final step in making big data work for business is to research the technologies that help you make the most of big data and big data analytics.

- Cheap, abundant storage.
- Faster processors.
- Affordable open source, distributed big data platforms, such as Hadoop.
- Parallel processing, clustering, MPP, virtualization, large grid environments, high connectivity and high throughputs.



Preeti Chauhan

M.Tech 3rd sem

# All-new Hacker's Search Engine "Censys"



By the end of last year, researchers from SEC Consult found that the manufacturers which are providing large number of home routers and Internet of Things devices are re-using the same set of hard-coded cryptographic keys and left around 3 millions of devices open for mass hijacking.

## **But how did the researchers get this number?**

Researchers got to know all this by using censys, it's a new search engine that scans the internet for vulnerable devices on daily basis.

## **Censys Maintains Complete Database of Everything on the Internet**

Censys is somewhat similar to hacker's search engine **Shodan**, which is designed specifically to get location of any devices that have been carelessly plugged into the Internet although all the security concerns to prevent unauthorized access is provided. However, Censys consists of more advanced method to find vulnerabilities in the devices and make the Internet a safer place.

**Censys is a free search engine that was originally released by researchers from the University of Michigan and is powered by the world's biggest search engine Google.**

Censys is an open source project that aims in maintaining a database of everything on the internet which includes how hosts and websites are configured, therefore it allows researchers to query the data through a search UI, report builder, and SQL engine helping researchers and companies unwrap Online security mishaps and vulnerabilities in products and services.

.

## **How Does Censys Work?**

Censys collects all information on hosts and websites via daily scans of the IPv4(internet protocol version 4 address space) that routes the majority of the Internet traffic. It consists of two tools:

**ZMap** is an open source network scanner

**ZGrab** is an application layer scanner

ZMap scans IP addresses on the Internet and collects new information every day. It also helps in determining whether the machines on the internet have security vulnerabilities or not and if yes than that should be fixed before being exploited by the hackers

Annu Choudhary  
M.Tech. 3rd sem.

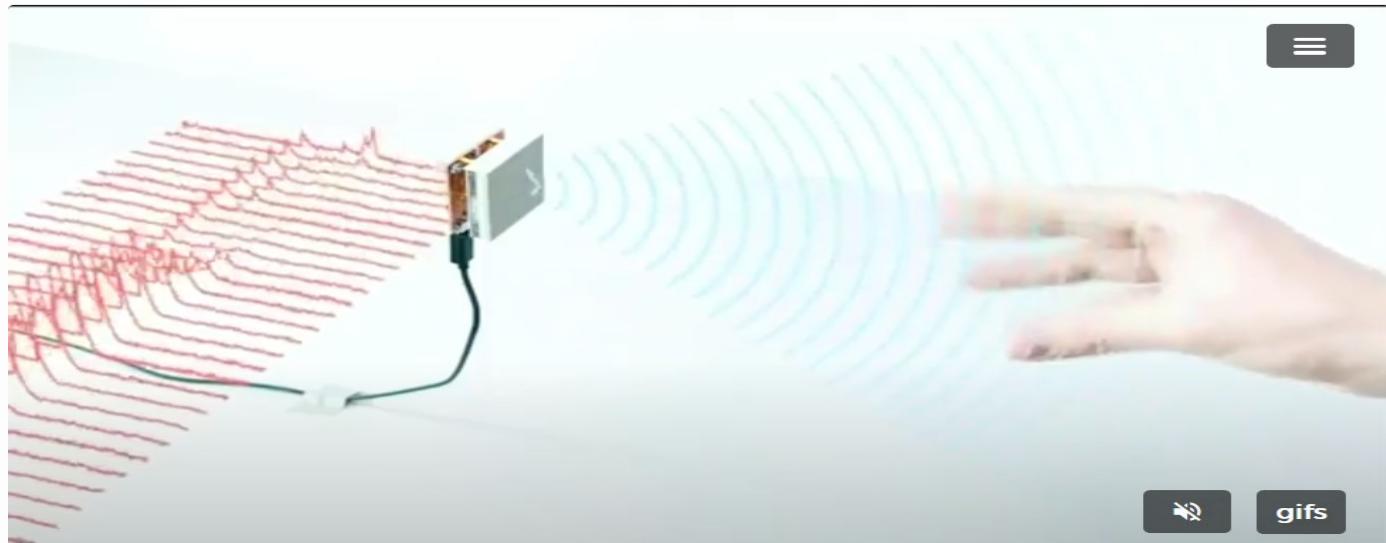
# The Tiny Radar Chip Revolutionizing Gesture Recognition: Project Soli

There are many new technologies that have helped mankind to make their task simpler. Amongst all these technologies a new technology has been emerged in recent times "PROJECT SOLI". "PROJECT SOLI" states that "Your hands are the only interface you'll need". "PROJECT SOLI" had a great impact on last year's GOOGLE I/O 2016 conference. Google's Advanced Technologies and Projects group has developed these project which completely works on mobile hardware technology. The founder of this project is "Ivan Pouer". The main concept of this project is to introduce "SMART TOUCH" into real world in which we do not need to touch (touchless interaction) the particular device to control it, we can use gesture instead. They have proposed a universal set of gestures which only will able to control a particular device such as button, dial & slider.



Previous inventions includes stereo cameras (which have difficulty understanding the overlap of fingers) and capacitive touch sensing (which struggles to interpret motion in a 3D context). "PROJECT SOLI" introduced the concept of the Soli sensor which uses radars when it comes to gesture-recognition technology. Radar is capable of interpreting objects position and motion even through other objects, making it perfect for developing a sensor that can be used in different kinds of devices like smartphones, smartwatch, smart tv. The difficulty was that radar hardware is too large for wearable applications.

Even the early prototypes developed were about the size of a briefcase. However, after several iterations, the current model is only 8mm x 10mm: smaller than a dime. And that's including the antenna array. This change has been done in a span of ten months. For comparison, evaluating normal radar information often requires the use of a supercomputer. The Soli evaluation board, itself, has two transmit antennas and four receive antennas. So when it comes to taking Soli to its possible applications, the board is easy to develop with.

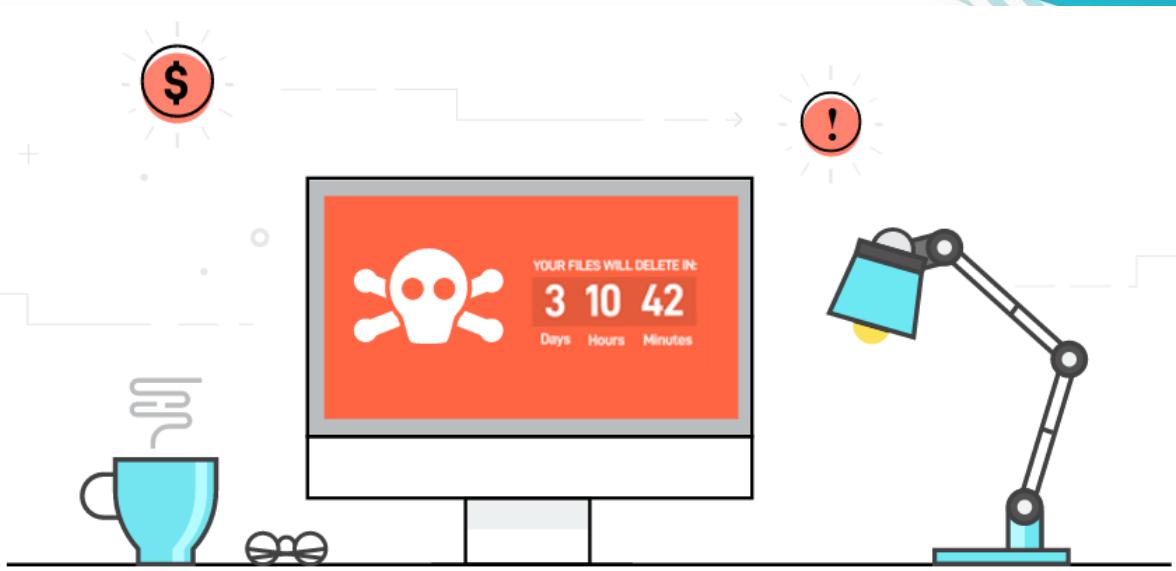


Motion signals detected by the radar chip are transformed into multiple representations, including range Doppler, which helps map the location of a hand by its velocity and distance from the sensor. From these representations, engineers can extract features, such as "range Doppler distance". The features are then passed to machine learning algorithms, which interpret them and approximate hand motions based on the signals received. The "PROJECT SOLI" team have proposed this technology to help mankind to make their tasks simpler. This project is about to be introduced into the real world within a very short time. We are hoping that this project would be a great success and more technologies like this would emerge in a similar manner.

Saurabh kumar

M.Tech. 1st sem.

# Global Bulletin



## Game of Thrones stars

**Release** – August 8, 2017

Origin - Hackers of US television network HBO

Target- released personal phone numbers of Game of Thrones actors, emails and the hackers claim to have taken 1.5TB of data

## Wannacry ransomware

**Release** - May 2017

Origin -North Korea

Target- Windows's vulnerability

Effectected country- U.K. , Spain, into Russia, Taiwan, France, Japan, and dozens ,India and more countries.

## Petya ransomware

**Release** – June 27, 2017

Origin – Ukraine via Tainted Accounting Software

Target- Microsoft Windows-based systems

Effectected country- Belgium, Hungary, Ukraine, US, Russia, France, UK, Germany, India, china, Japan, Canada, Australia, Italy, Span, Poland, Africa, Korea.

## **Massive malware attack**

**Release – June 28, 2017**

Origin – Theft of ‘cyber weapons’ from the NSA

Target- Microsoft Windows-based systems

Effectected country- U.S., Ukraine, Russia, U.K., France, Germany, Denmark, India, Australia

## **WikiLeaks CIA Vault7**

**Release – March 7, 2017**

Origin - U.S. Central Intelligence Agency.

Target - iPhone, Android, smart TVs, Windows, OSx, Linux, routers.

Effectected country - Middle East, Europe, Asia, and Africa.

## **Cloud bleed**

**Release - February 17, 2017**

Origin -. US internet Infrastructure Company Cloud flare

Target- The internet infrastructure company Cloud flare announced that a bug in its platform caused random leakage of potentially sensitive customer data

## **Macron Campaign Hack**

**Release – May, 2017**

Target- Hackers Hit Macron with Huge Email Leak Ahead of French Election

Effectected country – French

## **A Bad Batch**

**Release – May, 2017**

Origin - England

Target- Encrypting the data on the hard drive

Effectected country – London and Northern England

Varsha Tak  
M.Tech. 3rd sem.

# 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.

**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

**Preeti Chauhan (M.Tech. 3rd sem.)**

**spu16cs18@policeuniversity.ac.in**

**Satya Prakash Mehra (M.Tech. 3rd sem.)**

**spu16cs20@policeuniversity.ac.in**

Valediction ceremony of "2 Years Training Program in Cyber Security" of Mongolian Officers by Centre for Cyber Security Training.



Meet with The Former Hon'ble President of India

