Vol. 1, Issue 2

2016-2017

BHARATI VIDYAPEETH PUNE

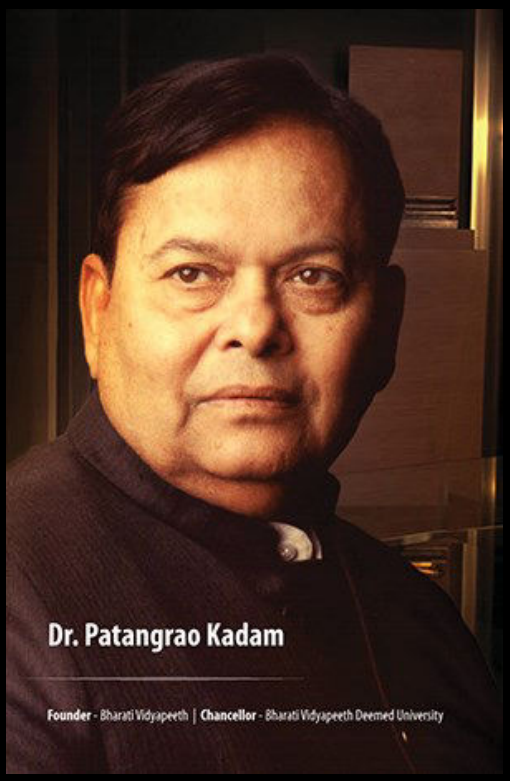
# HAPPENING

# CONTENTS

# BHARATI VIDYAPEETH COLLEGE OF ENGINEERING

Bharati Vidyapeeth is a organization established in the year 1964 by our respected founder Dr. Patangraoji Kadam. It has today created history by establishing 187 educational institutes imparting education from the pre-primary stage to post graduate stage within a short span of 44 years. At Bharati Vidyapeeth our objective has been to contribute to intellectual awakening and social transformation in different spheres such as education, economic, social and cultural fields in India and more particularly in Maharashtra. Our commitment and dedication has been towards catering to needs of Corporate India by providing quality education and to bring about an all-round development of a wider cross section of population including women, tribal and rural people. Always a step ahead, in May 1995 the department of human resources development, Government of India, on the recommendations, of the University Grants Commission accorded the status of Deemed University to 26 institutions of Bharati Vidyapeeth. In the year 2000, three more institutions were accorded the same status. Within such a short span of time, the performance of Bharati Vidyapeeths is accredited to none other than the man himself Dr. Patangrao Kadam.

## *Dr. Patangrao Kadam, Founder Of Bharati Vidyapeeth*




Our mission at Bharati Vidyapeeth is to identify and prepare leaders for the new millennium and also to cope-up with the increasing demand for leaders in the modern society.

Institute of Management is a workshop where today's youths are shaped up as effective managers of tomorrow. Apart from the study of their regular syllabi, the students should get fair and proper opportunities to express their views and ideas, especially in the field of Management, which plays a vital role in the modern era. The youth should be molded and equipped with courage, self-determination, and dedication d must be in a position to overcome any sort of difficulty with introspection.

Keeping this in mind, we should start brainstorming process of management students, because today's youths are building blocks of tomorrows Society. I am sure, "hard work brings surprising results" and we are second to none

## *Dr. Vishwajeet Kadam, Secretary, Bharati Vidyapeeth*

It Is heartening to know that Bharati Vidyapeeth College of Engineering, Navi Mumbai's Department of Computer Engineering is bringing out it's Annual Technical Magazine "HAPPENINIG ". Engineer's play the most vital and important role in nation building. They create new inventions using best engineered technologies to make human life more comfortable, secure and productive.

At the outset I send my greetings to the Editorial Board of "HAPPENINIG ", for working on a Magazine best in all aspects. The magazine should be a good source of guidanee for faculty and coming batches of students in choosing activities of their choice in their future for building their careers.

## *Dr. Vishwajeet Kadam, Director, Bharati Vidyapeeth*

It gives me great pleasure to know that Bharati Vidyapeeth College of Engineering, Navi Mumbai's Department of Computer Engineering is coming up with it's yearbook "HAPPENINIG". Indin has set it's vision to join the committee of the developed nation's by 2020 and this would be achieved if Indians combine their minds with their hearts. We would touch technical heights but we would not compromise with our age old values and traditions. The students have expressed their emotions in the best possible manner and I wish them all the best.

I believe this magazine will provide us the benchmark for continued improvement in overall development of the College and the Student's. I also appreciate the efforts of the Editorial team who have done an excellent job in compiling this magazine.

## *Dr. M.Z.Shaikh, Principal Of BVCOE, Navi Mumbai*

Each issue of our Department magazine is a milestone that marks our growth, unfolds our imagination, and gives life to our thoughts and aspirations. It unleashes a wide spectrum of creative skills ranging from writing to editing and even in designing the magazine.

One of the greatest landmarks of an educational institution is the emancipation of the Annual Magazine and I feel privileged to announce the launching of "Happening", the Annual Technical Magazine of Department of Computer Engineering. It would provide a platform to the budding engineer's to express their technical side of their personalities and " Happening " would go on to become the voice of generations to come.

The essence of Engineering and Management education which has spread in India is a very positive sign not only to cater domestic needs but provide manpower to the entire world and become biggest technically trained community. Bharati Vidyapeeth College of Engineering is a venture contributing to this Endeavour.

## *Dr. D.R.Ingle, Head Of Computer Engineering Department*

New technology is bringing opportunities along with new skill set requirements and challenges. Globalization is bringing competitiveness in every domain. Engineers have to fit into the requirements of companies that recruit across the globe. With the massive, near exponential increases in the amount of data to be processed, we need to completely change our traditional 'sequential instruction execution' way of thinking. The newly refreshed Computer Department Magazine " Happening " makes a gracious attempt at imparting knowledge to students of not only the Computer Department, but any student who may be interested. It provides students with resources to learn and make themselves well versed with current technological developments. It provides them with a perspective of the global advancement that is going on in the computing sector and makes their knowledge technologically rich. Wishing Editorial team the Best of Luck

## *Prof. Nidhi Sharma, Chief Editor, Computer Department*

The world is moving very fast and new technologies are coming up every week. We need to be proactive and enthusiastic in learning about these cutting edge tools and research. Buzz words like Big Data + Data Analytics, Hadoop, Cloud Computing and Parallel Computing are slowly becoming pervasive and are the new revolution. The most important aim of students should be to absorb as much of these new technologies as they can. They must explore, invent and innovate. Read up on algorithms, discuss them, identify points where they can be improved. Research, collaborate and excel. The students are our future and I believe that with students from BVCOE, the future does look bright.

# *Editors Note*


An Engineer is an artist, but the only difference he paints what the world demands. Give him a problem and he gives you a solution, that is what makes an engineer stand out. Computer Engineers take things a step further, the problem remains the same but this time the tool varies. Give him a computer and he solves your problem in a blink of an eye. But who would have thought a century ago that what took an average human being more than a week to do, a device that worked on electricity could end up doing in a matter of hours initially and seconds these days.

Using a computer and electronic media, last year, Prof. Nidhi Sharma with the help of my seniors, came up with the idea of publishing a departmental magazine. The idea was indeed something that gave a platform for students to portray their editorial skills and help them showcase their knowledge in various fields. As we all know, they implemented it and it was indeed appreciated by all.

Now, this year, we need to do it again. But the challenge is in doing the exact same thing yet adding something more to it so that the novelty remains. This year, we proudly present our annual departmental magazine, HAPPENING.

On behalf of our editorial group, I would like to thank Dr. Patangrao Kadam, Dr. Vishwajeet Kadam and Dr. V. J. Kadam for inspiring all of us. They have been motivational figures for all the students and they shall always be an role models.

Dr. M. Z. Shaikh Sir, Respected Principal, encouraged collaboration amongst the students of various years and encouraged us to better what has been previously achieved.

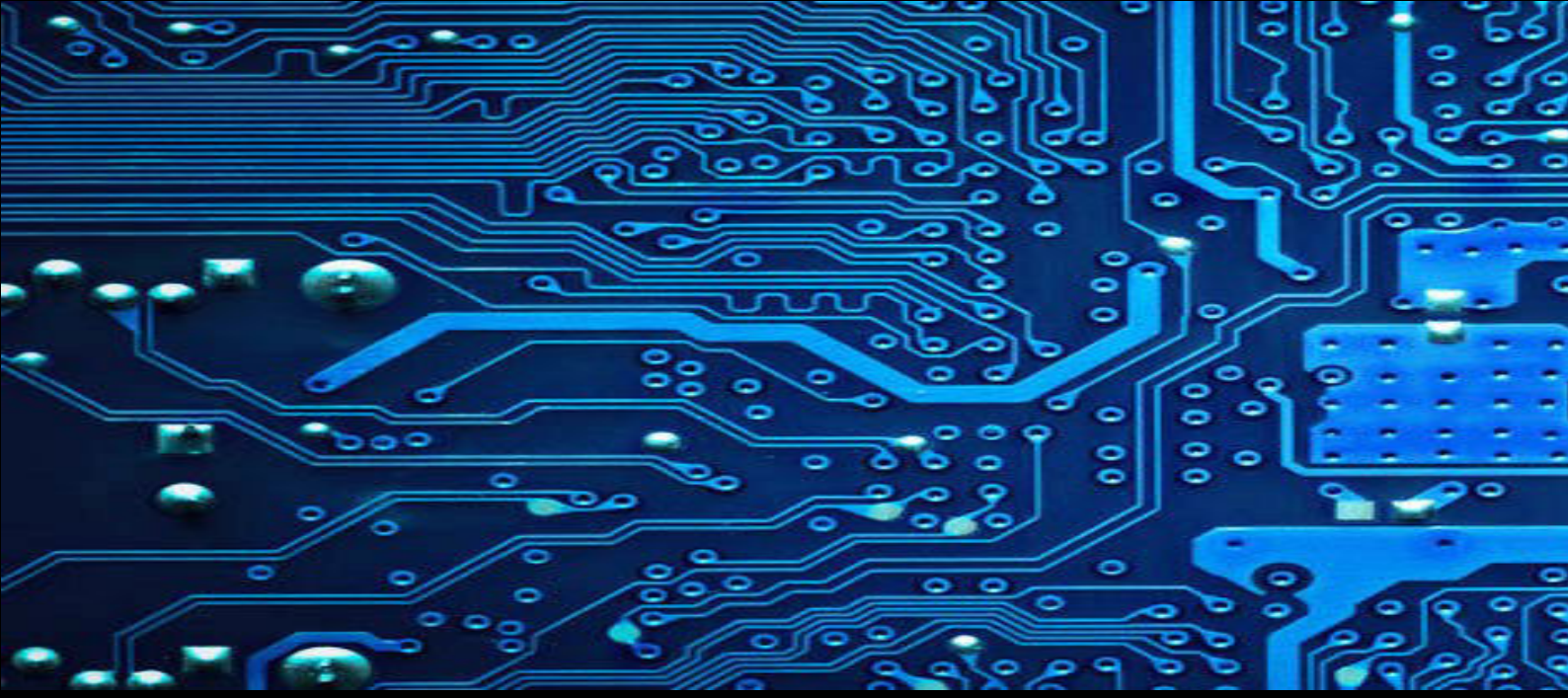
Dr. D. R. Ingle, the head of our department, is the backbone of our computer department. He has encouraged us to think out of the box and guided us since the very first day we joined this institute.

Prof. Nidhi Sharma, she has been the one to co-ordinate the editing and printing. She was there all along making sure all the content was available to the editors and encouraged us to be as creative as possible.

Last, but not the least, a special thanks to our editorial board members, Srina Sinha (S.E), Mrunmayee Dixit (S.E), Sharvil Turbadkar (B.E), Swapnil Velunde (B.E), Tejas Zarekar (B.E) and Kunal Shinde (B.E), Rushabh Wadkar (B.E) and Ankit Agarwal (B.E) who contributed in editing, content writing and printing this issue of our departmental news letter. This wouldn't have been possible without their help.

***-Rohit Vinod Nair,***

***Editorial Head***



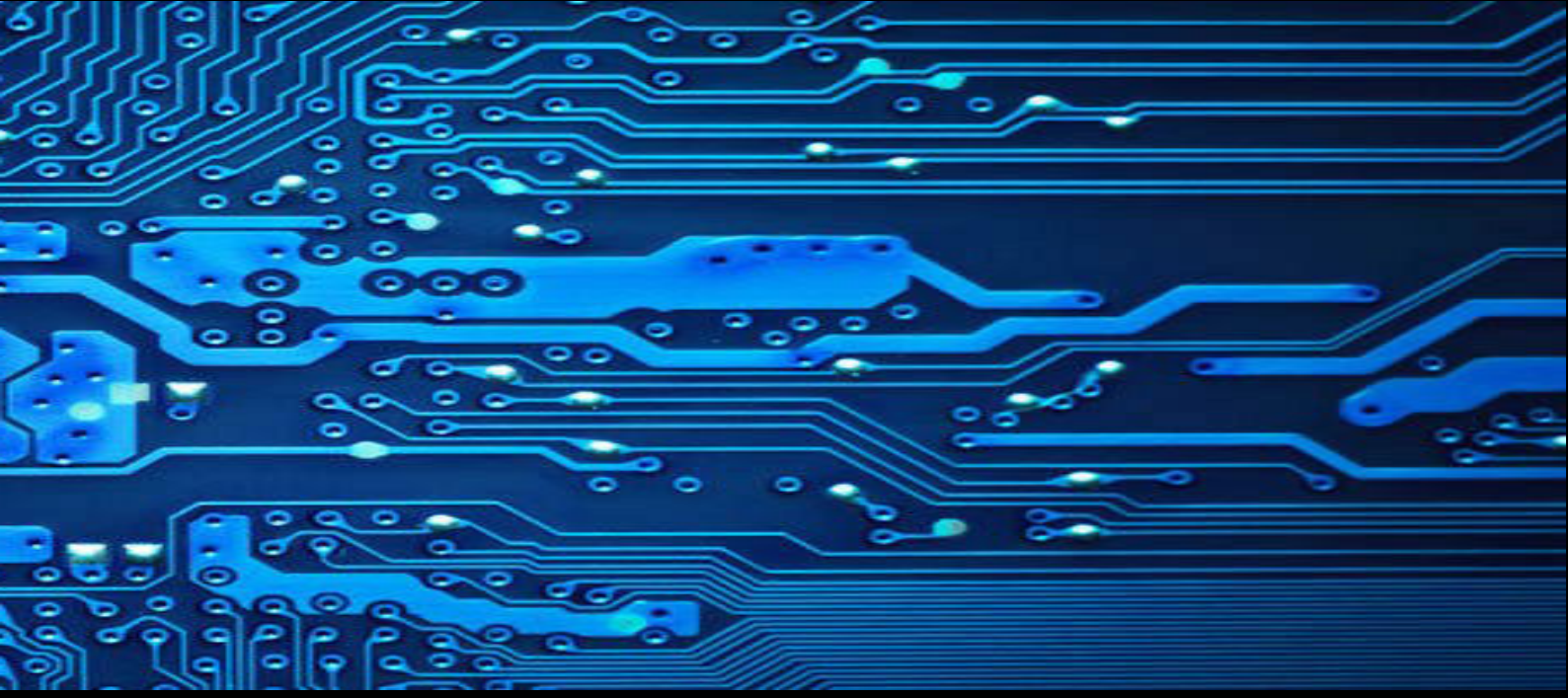
# A Brief History Of Computers

The word "computer" was first recorded as being used in 1613 and originally was used to describe a human who performed calculations or computations. The definition of a computer remained the same until the end of the 19th century, when the industrial revolution gave rise to machines whose primary purpose was calculating.

In 1822, Charles Babbage conceptualized and began developing the Difference Engine, considered to be the first automatic computing machine. The Difference Engine was capable of computing several sets of numbers and making hard copies of the results. Babbage received some help with development of the Difference Engine from Ada Lovelace, considered by many to be the first computer programmer for her work and notes on the Difference Engine. Unfortunately, because of funding, Babbage was never able to complete a full-scale functional version of this machine. In June of 1991, the London Science Museum completed the Difference Engine No 2 for the bicentennial year of Babbage's birth and later completed the printing mechanism in 2000.

In 1837, Charles Babbage proposed the first general mechanical computer, the Analytical Engine. The Analytical Engine contained an Arithmetic Logic Unit (ALU), basic flow control, and integrated memory and is the first general-purpose computer concept. Unfortunately, because of funding issues, this computer was also never built while Charles Babbage was alive. In 1910, Henry Babbage, Charles Babbage's youngest son, was able to complete a portion of this machine and was able to perform basic calculations.

The Turing machine was first proposed by Alan Turing in 1936 and became the foundation for theories about computing and computers. The machine was a device that printed symbols on paper tape in a manner that emulated a person following a series of logical instructions. Without these fundamentals, we wouldn't have the computers we use today. The Turing test is a test, developed by Alan Turing in 1950, of a machine's ability to exhibit intelligent behaviour equivalent to, or indistinguishable from, that of a human. A Turing machine is a hypothetical device that manipulates symbols on a strip of tape according to a table of rules. Despite its simplicity, a Turing machine can be adapted to simulate the logic of any computer algorithm, and is particularly useful in explaining the functions of a CPU inside a computer.



# The Turing Machine

A Turing machine is an abstract machine that manipulates symbols on a strip of tape according to a table of rules; to be more exact, it is a mathematical model of computation that defines such a device. Despite the model's simplicity, given any computer algorithm, a Turing machine can be constructed that is capable of simulating that algorithm's logic.

The machine operates on an infinite memory tape divided into discrete cells. The machine positions its head over a cell and "reads" (scans) the symbol there. Then, as per the symbol and its present place in a finite table of user-specified instructions, the machine (i) writes a symbol (e.g. a digit or a letter from a finite alphabet) in the cell (some models allowing symbol erasure and/or no writing), then (ii) either moves the tape one cell left or right (some models allow no motion, some models move the head), then (iii) (as determined by the observed symbol and the machine's place in the table) either proceeds to a subsequent instruction or halts the computation.

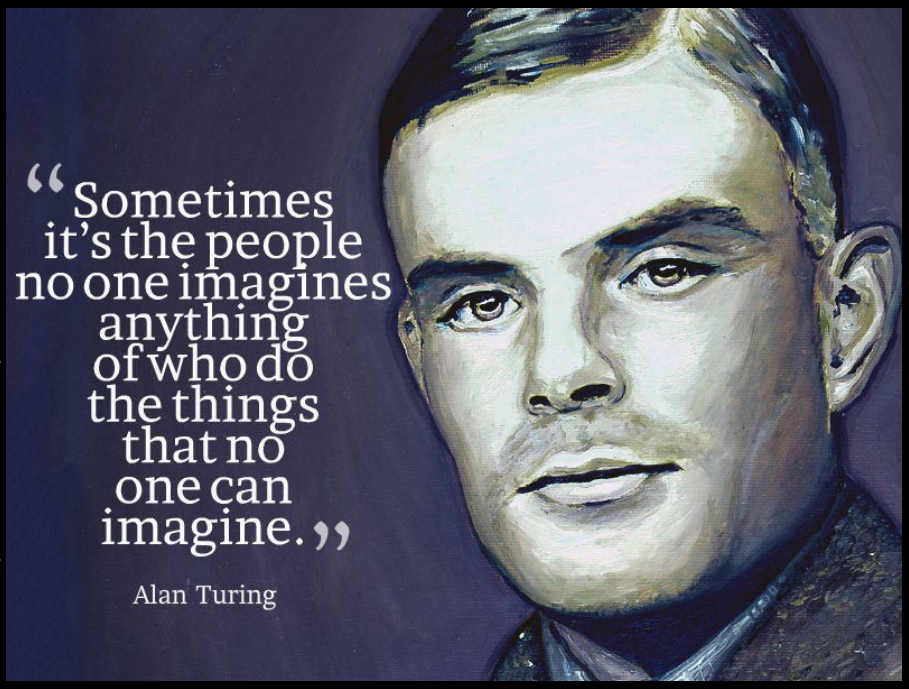
The Turing machine was invented in 1936 by Alan Turing, who called it an a-machine (automatic machine). With this model, Turing was able to answer two questions in the negative: (1) Does a machine exist that can determine whether any arbitrary machine on its tape is "circular" (e.g. freezes, or fails to continue its computational task); similarly, (2) does a machine exist that can determine whether any arbitrary machine on its tape ever prints a given symbol. Thus by providing a mathematical description of a very simple device capable of arbitrary computations, he was able to prove properties of computation in general—and in particular, the uncomputability of the Entscheidungsproblem ("decision problem").

Thus, Turing machines prove fundamental limitations on the power of mechanical computation. While they can express arbitrary computations, their minimalistic design makes them unsuitable for computation in practice: real-world computers are based on different designs that, unlike Turing machines, use random-access memory.

Turing completeness is the ability for a system of instructions to simulate a Turing machine. A programming language that is Turing complete is theoretically capable of expressing all tasks accomplishable by computers; nearly all programming languages are Turing complete if the limitations of finite memory are ignored.

# The Life Of A Legend, Alan Turing

Alan Mathison Turing OBE FRS (23 June 1912 – 7 June 1954) was an English computer scientist, mathematician, logician, cryptanalyst and theoretical biologist. He was highly influential in the development of theoretical computer science, providing a formalisation of the concepts of algorithm and computation with the Turing machine, which can be considered a model of a general purpose computer. Turing is widely considered to be the father of theoretical computer science and artificial intelligence.




During the Second World War, Turing worked for the Government Code and Cypher School (GC&CS) at Bletchley Park, Britain's codebreaking centre that produced Ultra intelligence. For a time he led Hut 8, the section responsible for German naval cryptanalysis. He devised a number of techniques for speeding the breaking of German ciphers, including improvements to the pre-war Polish bombe method, an electromechanical machine that could find settings for the Enigma machine. Turing played a pivotal role in cracking intercepted coded messages that enabled the Allies to defeat the Nazis in many crucial engagements, including the Battle of the Atlantic, and in so doing helped win the war. Counterfactual history is difficult with respect to the effect Ultra intelligence had on the length of the war, but at the upper end it has been estimated that this work shortened the war in Europe by more than two years and saved over fourteen million lives.

After the war, he worked at the National Physical Laboratory, where he designed the ACE, among the first designs for a stored-program computer. In 1948 Turing joined Max Newman's Computing Machine Laboratory at the Victoria University of Manchester, where he helped develop the Manchester computers and became interested in mathematical biology. He wrote a paper on the chemical basis of morphogenesis, and predicted oscillating chemical reactions such as the Belousov–Zhabotinsky reaction, first observed in the 1960s.

Turing was prosecuted in 1952 for homosexual acts, when by the Labouchere Amendment, "gross indecency" was still criminal in the UK. He accepted chemical castration treatment, with DES, as an alternative to prison. Turing died in 1954, 16 days before his 42nd birthday, from cyanide poisoning. An inquest determined his death as suicide, but it has been noted that the known evidence is also consistent with accidental poisoning. In 2009, following an Internet campaign, British Prime Minister Gordon Brown made an official public apology on behalf of the British government for "the appalling way he was treated." Queen Elizabeth II granted him a posthumous pardon in 2013. The Alan Turing law is now an informal term for a 2017 law in the United Kingdom that retroactively pardons men cautioned or convicted under historical legislation that outlawed homosexual acts.

Against the popular belief that he committed suicide , there are people who still believe

that it was not the whole story. He was found dead in his house with an half eaten apple by his side. Though the cause of dead was cyanide poisoning, people claim that the apple was never really tested for cyanide which is not what is expected from the investigating team.

## ALAN TURING

1912-1945

Founder of computer science and cryptography, whose work was key to breaking the war time Enigma Code.

His death may be mysterious, but his legacy continued and all our modern computers wouldn't have existed without his contribution. He saved the lives of millions and Steve Jobs', Apple's CEO, role model was Alan Turing. His company's logo, the half eaten apple, is a

# WhatsApp's end-to-end encryption explained: What is it and does it matter?

-Rushabh Wadkar, B.E

With a single encryption upgrade to Facebook's WhatsApp, a billion users now find themselves confronted with a security technology whose reliability rests on the arcane-sounding end-to-end encryption (e2e) with perfect forward secrecy (PFS).

The firm's official announcement describes it thus: "The idea is simple: when you send a message, the only person who can read it is the person or group chat that you send that message to. No one can see inside that message. Not cybercriminals. Not hackers. Not oppressive regimes."

WhatsApp has been using this security in a more limited way since November 2014 when it adopted the Signal protocol from messaging encryption pioneers Open Whisper Systems. So what has changed? Essentially, it is now offering this security to every single user as a mandatory upgrade across all mobile platforms.

Until now, messages between users were sent via WhatsApp's servers using proprietary technology, which applied and retained the encryption keys used to scramble data. The connection was secure as long as WhatsApp itself didn't decide to peer at the encrypted content, possibly after being served a warrant to do so by a government or police force. The company could also to do this retrospectively on old messages and files as well as future ones.

The proprietary nature of the code meant that the outside world could not study what WhatsApp was doing for weaknesses or backdoors. Replacing this with the highly regarded open source Signal software from Open Whisper Systems means that the underlying technology is open to code review by anyone.

From now on, assuming communicating users have installed the latest version of WhatsApp (post March 31 – the app warns users to upgrade) private keys will be generated and stored on the user's device and will no longer be accessible to WhatsApp. In addition, each message or session uses a different private key (called 'perfect forward secrecy') which means that no single key gives access to all the data sent by someone in the past or future.

The WhatsApp server does of course store a user's public key, which is necessary to build a directory of users so that people can contact each other across the service. In PKI encryption, this public key is useless for accessing encrypted content and is merely a way for two users to communicate with one another without the risky need to send each other a private key, for instance a conventional asymmetric key such as a passcode.

None of the above requires WhatsApp users to configure anything – it's just turned on by default and users who don't upgrade to e2e security will get warning messages. This security can't be turned off or downgraded by using an old version at a later stage.

Man-in-the-middle: WhatsApp offers a third security layer designed to stop the possibility of man-in-the -middle attacks in which someone impersonates the recipient of a message without the sender realising. This involves two people comparing a


unique identifier, either by scanning a QR code or comparing a 60-digit number (which is not an encryption key, just an ID).

Ideally, the users need to be beside each other and the process has to be regenerated if the app is reinstalled. However, the number can be sent remotely using the 'share' button accessible from the app's chat screen and it is also possible to be notified when a contact's security code changes.

The integration of Signal across all of WhatsApp's services marks an important moment for the mass use of secure encryption. At a single stroke, one billion people will start using the sort of security that keeps intelligence services and governments awake at night.

That doesn't mean the implementation of Signal by WhatsApp might not have weaknesses or that a weakness couldn't be found in Signal itself in the future. Seemingly secure encryption has had too many difficult moments in the past two years for anyone to make that brave a prediction.

But amidst a gradual erosion of privacy, there is no doubt that WhatsApp's transition to end-to-end encryption will be remembered a significant tipping of the balance in the opposite direction.

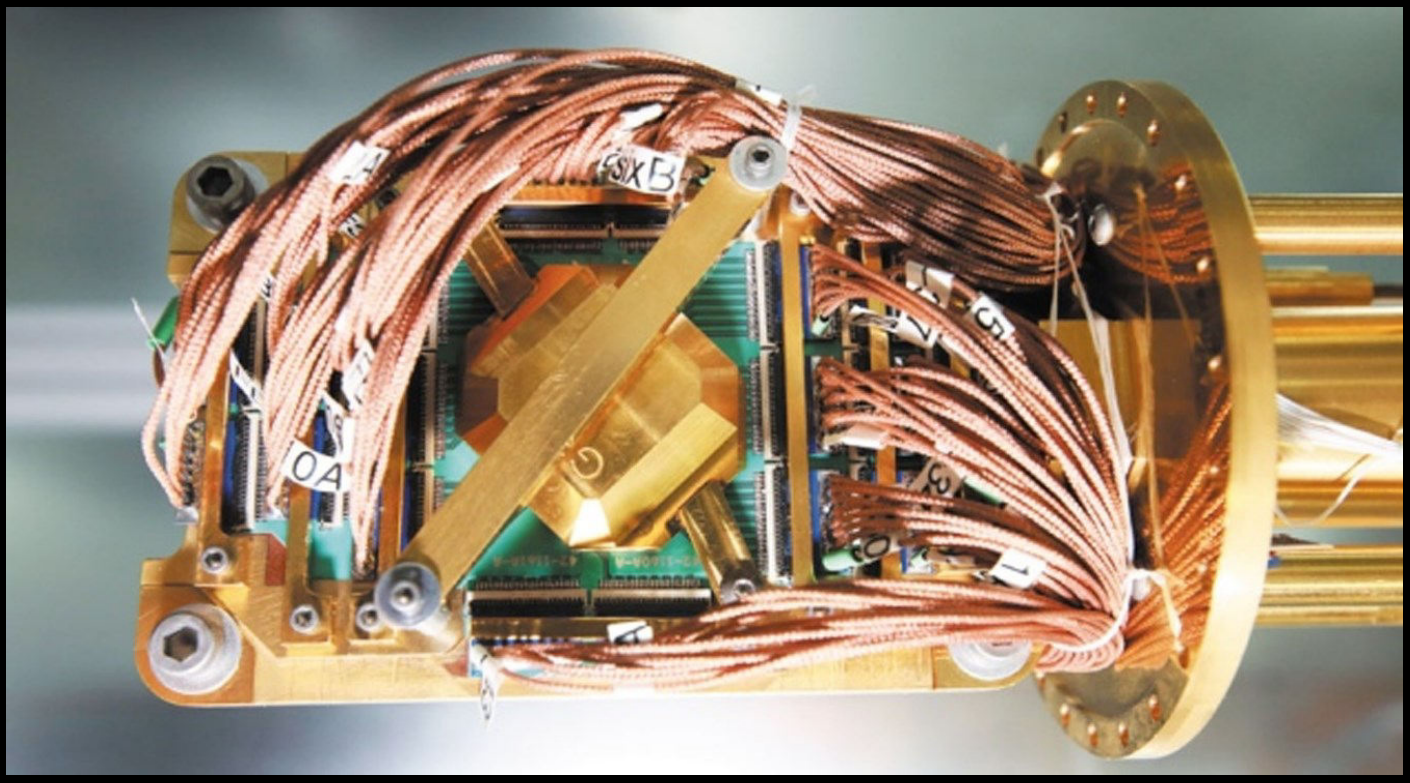
# Quantum Computing: The next generation of computing power.

-Srina Sinha, S.E & Mrunmayee Dixit, S.E

The internet today, relies very heavily on the web search. The only way to allow for fast search on any open web is to pre index. Pre Indexing assumes a fixed static set of data. But it is not a long-term survivable solution. If one does not pre index, there is only one scaling solution, that is, Quantum computing. A quantum computer is a kind of computer that directly leverages the laws of quantum mechanics to do a calculation. The art of quantum computing is to find ways of gaining as much information as possible from the unobservable.

Our desktop PCs, laptops and smart phones can run spreadsheets, stream live video, allow us to chat with people on the other side of the world, and immerse us in realistic 3D environments. But at their core, all digital computers have something in common. They all perform simple arithmetic operations. Their power comes from the immense speed at which they are able to do this. Computers perform billions of operations per second. These operations are performed so quickly that they allow us to run very complex high level applications. Although there are many tasks that conventional computers are very good at, there are still some areas where calculations seem to be exceedingly difficult. Examples of these areas are: Image recognition, and tasks where a computer must learn from experience to become better at a particular task. Even though there has been much effort and research poured into this field over the past few decades, our progress in this area has been slow and the prototypes that we do have working usually require very large supercomputers to run them, consuming a vast quantities of space and power. And here's where the need of Quantum Computer arises.

Quantum Physics tells you that any object that is quantum mechanical, when disturbed, becomes classical. So every quantum computer has its building block, something called as a q-bit, or a quantum bit. A quantum bit is like a digital bit that we have in classical computers that we use today. A classical computer performs calculations using the bits 0 and 1. It uses transistors to process information in the form of zeros and ones. Just like a classical computer uses zeros and ones, these states can be achieved in particles called 'spin'. The spin can either be 'spin up' or 'spin down'. The two states 0 and 1 can be represented using the spin of the particle. Quantum computer gives us the advantage of the particle (in Quantum Physics) being able to exist in multiple states at the same time. This phenomenon is called as superposition, which forms a special characteristic of these computers. Due to this, it can achieve both 0 and 1 states at the same time. Therefore, it has its q-bits, represented by 0 and 1 at the same time, giving us more flexibility in performing complex operations. This allows it to perform one billion or more copies of a computation at the same time. In a way, this is similar to a parallel computer with one billion processors performing different computations at the same time—with one crucial difference. For a parallel computer, we need to have one billion different processors. In a quantum computer, all one billion computations will be running on the same hardware. This is known as quantum



parallelism.

Quantum computers solve some practically important problems much more efficiently. For example, integer factorization can be done in polynomial time on quantum computers what seems to be impossible on classical computers, searching in unordered database can be done provably with less queries on quantum computer.

The process of miniaturization that has made current classical computers so powerful and cheap, has already reached microlevels where quantum effects occur. Chipmakers tend to go to great lengths to suppress those quantum effects, but instead one might also try to make good use of them. Normal computers work, whether there is power going through it or not. What quantum states allow for is much more complex than that because things can be both particle and a wave at the same time and the uncertainty around quantum states allows us to encode more information into a much smaller computer. That's what's breathtaking about quantum computing.

In the past, it was believed that all computers fundamentally did the same thing- may b a little faster than another. However, this is wrong. In the quantum world, if a system, whether an election r a couter can be in a two million different states, it can also be in what we call a superposition of all those states, and gives it much more room to maneuver to try to get from input to output. Making use of quantum effects allows one to speed-up certain computations enormously. It enables some things that are impossible for classical computers.

Quantum computers also utilize an aspect of quantum mechanics known as entanglement. Entanglement means that describing a system of several qubits using ordinary classical information, such as bits or numbers, isn't simply about stringing together the descriptions of the individual qubits. Instead, you need to describe all the correlations between the different qubits. As you increase the number of qubits, the number of those correlations grows exponentially: for n qubits there are 2n correlations. This number quickly explodes: to describe a system of 300 qubits you'd already need more

numbers than there are atoms in the visible Universe. The idea is that, since you can't hope to write down the information contained in system of just a few hundred qubits using classical bits, perhaps a computer running on qubits, rather than classical bits, can perform tasks a classical computer can never hope to achieve.

Another interesting quantum phenomenon that quantum computers exploit is quantum interference. For example, we can device quantum algorithms such that all the possible ways to get to the wrong answer interfere with themselves and cancel each other out., while leaving only the possibility of getting the right answer. These are also called as amplitudes.

Quantum algorithms combine the effects of parallelism and interference . Quantum parallelism is used to perform a large number of computations at the same time, and quantum interference is used to combine their results into something that is both meaningful and can be measured according to the laws of quantum mechanics.

As miniaturization of computing devices continues we are rapidly approaching the microscopic level where the laws of the quantum world dominate. Thus not only scientific curiosity and challenges but also technological progress requires that the resources and potentials of quantum computing be fully explored. Quantum computing is a potential. There are already results convincingly demonstrating that for some important practical problems quantum computers are theoretically exponentially more powerful than classical computers. In addition, the laws of quantum world harvested through quantum cryptography can improve the view of our current knowledge unconditional security of communication unachievable by classical means.

Finally the development of quantum computing is a drive and gives new impetus to explore in more detail and from new points of view concepts potentials laws and limitations of the quantum world and to improve our knowledge of the natural world The study of information processing laws limitations and potentials is nowadays in general a powerful methodology to extend our knowledge and this seems to be particularly true for quantum mechanics.

Quantum computers could one day replace silicon chips, just like the transistor once replaced the vacuum tube. But for now, the technology required to develop such a quantum computer is beyond our reach. Most research in quantum computing is still very theoretical.The most advanced quantum computers have not gone beyond manipulating more than 16 qubits, meaning that they are a far cry from practical application. However, the potential remains that quantum computers one day could perform, quickly and easily, calculations that are incredibly time-consuming on conventional computer. Quantum computing could lead to significant developments in artificial intelligence and allow for search or analysis of much more data than can be handled by today’s most powerful machines.

# Psychologists enlist machine learning to help diagnose depression

-Ankit Agarwal, B.E

Depression affects more than 15 million American adults, or about 6.7 percent of the U.S. population, each year. It is the leading cause of disability for those between the ages of 15 and 44.

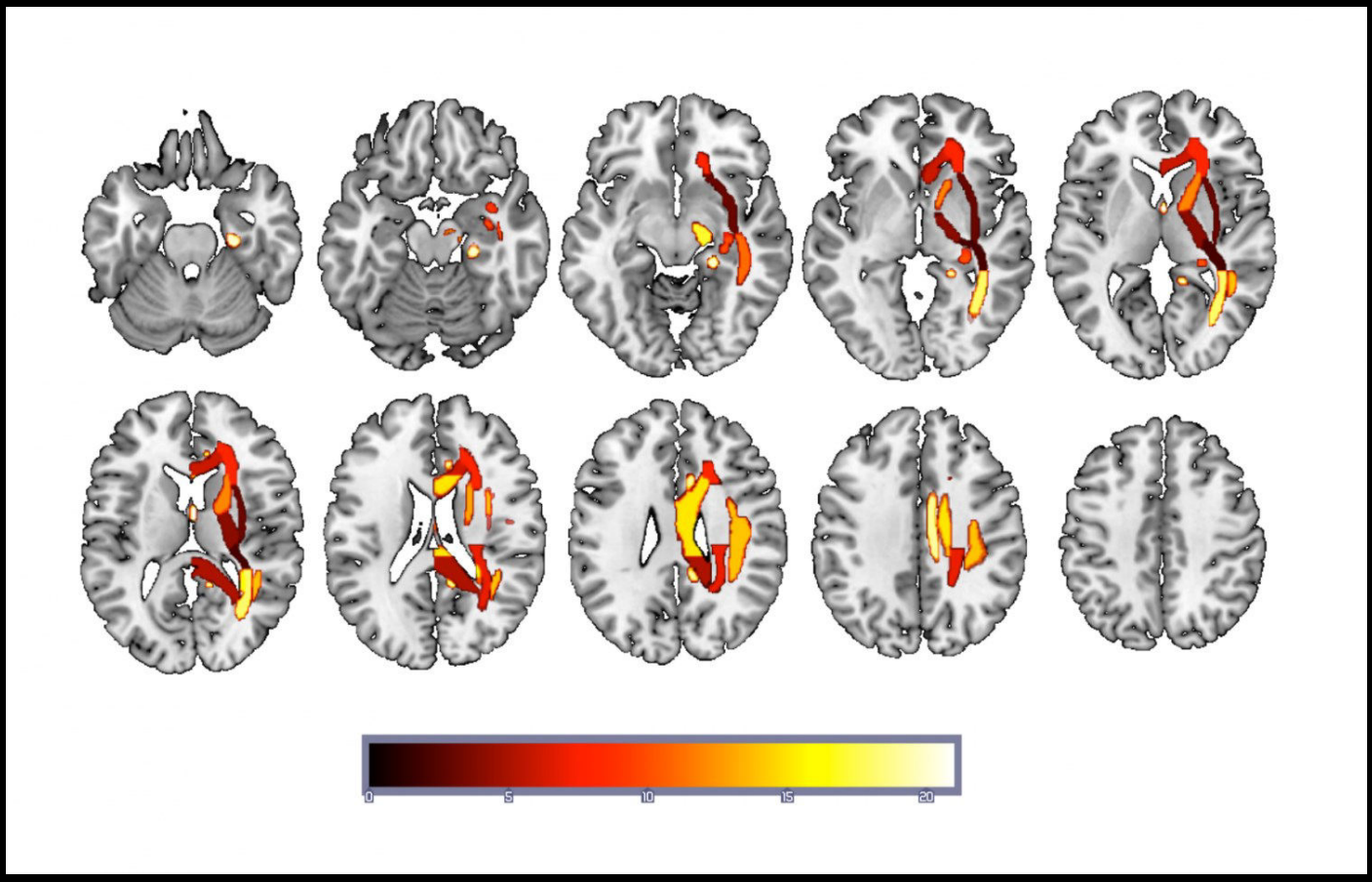
Is it possible to detect who might be vulnerable to the illness before its onset using brain imaging?

David Schnyer, a cognitive neuroscientist and professor of psychology at The University of Texas at Austin, believes it may be. But identifying its tell-tale signs is no simpler matter. He is using the Stampede supercomputer at the Texas Advanced Computing Center (TACC) to train a machine learning algorithm that can identify commonalities among hundreds of patients using Magnetic Resonance Imaging (MRI) brain scans, genomics data and other relevant factors, to provide accurate predictions of risk for those with depression and anxiety.

Researchers have long studied mental disorders by examining the relationship between brain function and structure in neuroimaging data.

"One difficulty with that work is that it's primarily descriptive. The brain networks may appear to differ between two groups, but it doesn't tell us about what patterns actually predict which group you will fall into," Schnyer says. "We're looking for diagnostic measures that are predictive for outcomes like vulnerability to depression or dementia."

In 2017, Schnyer, working with Peter



Clasen (University of Washington School of Medicine), Christopher Gonzalez (University of California, San Diego) and Christopher Beevers (UT Austin), completed their analysis of a proof-of-concept study that used a machine learning approach to classify individuals with major depressive disorder with roughly 75 percent accuracy.

Machine learning is a subfield of computer science that involves the construction of algorithms that can "learn" by building a model from sample data inputs, and then make independent predictions on new data.

The type of machine learning that Schnyer and his team tested is called Support Vector Machine Learning. The researchers provided a set of training examples, each marked as belonging to either healthy individuals or those who have been diagnosed with depression. Schnyer and his team labelled features in their data that were meaningful, and these examples were used to train the system. A computer then scanned the data, found subtle connections between disparate parts, and built a model that assigns new examples to one category or the other.

In the study, Schnyer analyzed brain data from 52 treatment-seeking participants with depression, and 45 heathy control participants. To compare the groups, they matched a subset of depressed participants with healthy individuals based on age and gender, bringing the sample size to 50.

Participants received diffusion tensor imaging (DTI) MRI scans, which tag water molecules to determine the extent to which those molecules are microscopically diffused in the brain over time. By measuring this diffusion in multiple spatial directions, vectors are generated for each voxel (three-dimensional cubes that represent either structure or neural activity throughout the brain) to quantify the dominant fiber orientation. These measurements are then translated into metrics that indicate the integrity of white matter pathways within the cerebral cortex.

One common parameter used to characterize DTI is fractional anisotropy: the extent to which diffusion is highly directional (high fractional anisotropy) or unrestricted (low fractional anisotropy).

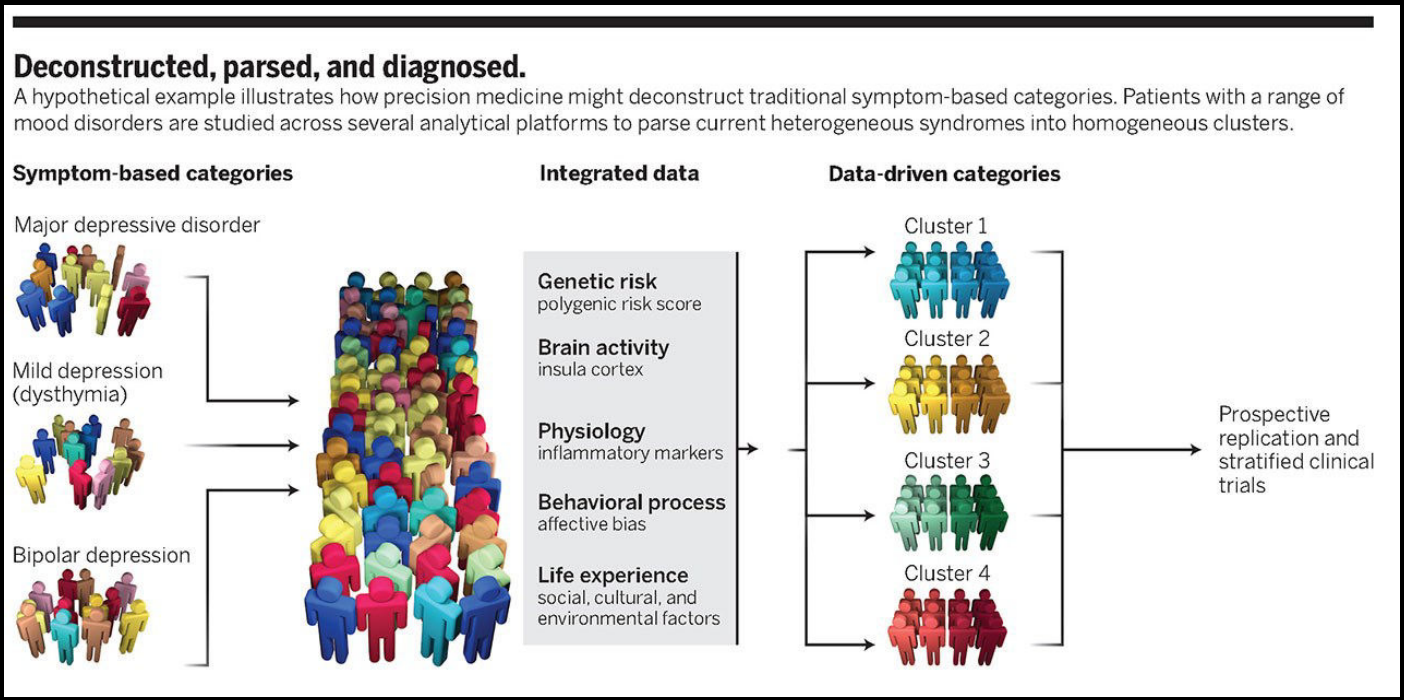
They compared these fractional anisotropy measurements between the two groups and found statistically significant differences. They then reduced the number of voxels involved to a subset that was most relevant for classification and carried out the classification and prediction using the machine learning approach.

"We feed in whole brain data or a subset and predict disease classifications or any potential behavioral measure such as measures of negative information bias," he says.

The study revealed that DTI-derived fractional anisotropy maps can accurately classify depressed or vulnerable individuals versus healthy controls. It also showed that predictive information is distributed across brain networks rather than being highly localized.

"Not only are were learning that we can classify depressed versus non-depressed people using DTI data, we are also learning something about how depression is represented within the brain," said Beevers, a professor of psychology and director of the Institute for Mental Health Research at UT Austin. "Rather than trying to find the area that is disrupted in depression, we are learning that alterations across a number of networks contribute to the classification of depression."

The scale and complexity of the problem




necessitates a machine learning approach. Each brain is represented by roughly 175,000 voxels and detecting complex relationship among such a large number of components by looking at the scans is practically impossible. For that reason, the team uses machine learning to automate the discovery process.

"This is the wave of the future," Schnyer says. "We're seeing increasing numbers of articles and presentations at conference on the application of machine learning to solve difficult problems in neuroscience."

The results are promising, but not yet clear-cut enough to be used as a clinical metric. However, Schnyer believes that by adding more data -- related not only to MRI scans but also from genomics and other classifiers -- the system can do much better.

"One of the benefits of machine learning, compared to more traditional approaches, is that machine learning should increase the likelihood that what we observe in our study will apply to new and independent datasets. That is, it should generalize to new data," Beevers said. "This is a critical question that we are really excited to test in future studies."

Beevers and Schnyer will expand their study to include data from several hundred volunteers from the Austin community who have been diagnosed with depression, anxiety or a related condition. Stampede 2 -- TACC's newest supercomputer which will come online later in 2017 and will be twice as powerful as the current system -- will provide the increased computer processing power required to incorporate more data and achieve greater accuracy.

"This approach, and also the movement towards open science and large databases like the human connectome project, mean that facilities like TACC are absolutely essential," Schnyer says. "You just can't do this work on desktops. It's going to become more and more important to have an established relationship with an advanced computing center."

# How predictive analytics helps Indian police fight crime.

-Ankit Agarwa, B.E

Imagine a world in which we could predict crime and police officers would be sent to the incident spot as the crime is happening, or even before it happened. This could be achieved by predicting situations based on data trends in crimes.

According to the National Judicial Data reports, on an average, out of every 100 people worldwide, 12 people are affected by crime-related activities. In India alone, more than 3.7 crores cases were pending in courts as of 2014. In the wake of increasing crime rate in India, the police forces are increasingly turning to data analytics.

Big data and predictive analytics the cornerstones of analysing multiple data types and data sources to predict and even prevent crimes from happening. As a result of the ever-increasing shortage of police force to sift through the growing volumes of data including physical records, digital feeds, social media data and others, it is paramount for law enforcement agencies in the country to use advanced analytical tools. This move can save costs, and more importantly save time and the effort in crime investigation and prevention.

Data analytics, helpful for larger enterprises to make business decisions, can now be used to help police officers find the proverbial needle in massive haystacks, agreed analysts.

According to Ehtisham Zaidi, senior research analyst at Gartner, the Indian Police force has started taking an increasing interest in crime analytics using big data, which involves storing and analyzing huge volume and variety of data in real time, to predict and inference patterns and trends especially relating to human interactions and behavior.

“The police force now has access to mature big data storage platforms such as Hadoop, NoSQL etcetera, which allows them to store years’ worth of structured digital content and unstructured data within the same platform, and analyze them along with the incoming real time data to understand crime patterns within their jurisdictions,” he says.

He further adds that the Indian police force also uses predictive analytics to develop models using machine learning to know which areas are most prone to crime, and which individuals to keep on its watch list.

The Indian police force has started taking an increasing interest in crime analytics using big data, which involves storing and analyzing huge volume and variety of data in real time.Delhi police have recently partnered with the ISRO to develop an analytical system—Crime Mapping, Analytics and Predictive System (CMAPS). CMAPS helps Delhi police to ensure internal security, controlling crime, and maintaining law and order through analysis of data and patterns.According to a senior official in Delhi police, “Each one in the force will be equipped with Personal Digital Assistant device, which will be connected to a central system, and will contain records of more than two lakh criminals.”

Similarly, the Jharkhand police force is trying to implement an analytical system, with

the help of IIM Ranchi, which would evaluate criminal records, date and time of crime occurrences, and location to predict crime-prone zones. The system is built on sophisticated algorithms and behavioral science, which will accumulate crime related data from all over the country.

From public records to social media information to informant tips, Indian police force has access to an expansive amount of data, which is spread over its legacy systems. Therefore, it becomes extremely important for Indian police across different states to adopt easy-to-operate analytical tools to utilize this vast intelligence.

According to Pankaj Kapoor, president at ACSG Corporate, several state police departments of the country are working with newer technologies to collect, analyze and predict data streams in real time to keep citizens safe. “They use live camera feeds, communications, reports and other sources, by applying facial recognition and voice analytics,” says Kapoor.

Several other companies like IBM, Oracle, SAS, Microsoft, SAP, EMC, HP, and DELL are aggressively working towards the same agenda. Advanced analytic capabilities have now been integrated into several CCTV systems of the country to improve response times to crime incidents.

Alok Kumar, additional commissioner of Police (Law and Order), mentioned in an interview with ET, that the key is data mining and it is very important.

The Bangalore police with the help of IBM is now training officers on the better usage of data analytics software.

Another separate agency, National Crime Records Bureau (NCRB) collects a huge amount of data and acts as clearing house information on national and international criminals. They use geographic information -based analytical systems to predict and curb the crime rates in the country.

Although criminals always try to be ahead of the law, deployment of big data and predictive analytics in Indian police agencies will help the police force to enhance the effectiveness of their work, making our country safer.

# Predpol: The future of policing.

-Tejaz Zarekar, B.E


PredPol’s mission is to provide a crime prevention platform to keep communities safer. Their secure, cloud-based technology places public safety officers at the right time and location to give them the best chance of preventing crime.

PredPol grew out of a research project between the Los Angeles Police Department and UCLA. The chief at the time, Bill Bratton, wanted to find a way to use CompStat data for more than just historical purposes.

The goal was to understand if this data could provide any forward-looking recommendations as to where and when additional crimes could occur. Being able to anticipate these crime locations and times could allow officers to pre-emptively deploy and help prevent these crimes.

Working with mathematicians and behavioral scientists from UCLA and Santa Clara University, the team evaluated a wide variety of data types and behavioral and forecasting models. The models were further refined with crime analysts and officers from LAPD and the Santa Cruz Police Department. They ultimately determined that the three most objective data points collected by police departments provided the best input data for forecasting: Crime type, Crime location, Crime date and time.

PredPol uses only three data points in making predictions: past type of crime, place of crime and time of crime. It uses no personal information about individuals or groups of individuals, eliminating any personal liberties and profiling concerns.

For many jurisdictions, predictive policing strategy encourages patrol officers to work as partners with communities in the locations where crime is most likely to occur. PredPol is one of the tools to guide location -based strategies in which law enforcement officers communicate and build relationships with residents to engage them in community crime watch efforts.

Using only three data points – crime type, crime location and crime date/time – PredPol's powerful software provides each law enforcement agency with customized crime predictions for the places and times that crimes are most likely to occur. PredPol pinpoints small areas, depicted in 500 feet by 500 feet boxes on maps – that are automatically generated for each shift of each day.

The algorithms used by PredPol have been published and discussed publicly in peer-reviewed papers. They are based on the observation that certain crime types tend to cluster in time and space. PredPol uses self-exciting point process models to replicate this behavior (Click Self-Exciting Point Process Modeling of Crime).

PredPol takes a feed from each department's Records Management System (RMS) to collect crime type, location and date/time. This data is collected at least daily and feeds our prediction engine, which is run once a day to create predictions for each beat, shift and mission type.

They initially process several years of data to lay down a "background" level of crime patterns and to understand how crimes propagate throughout the city. This is done using an Epidemic Type Aftershock Sequence (ETAS) Model, which is a self-learning algorithm.

As new crimes come in, they are mapped against existing patterns and events in the city. Based on the propagation patterns uncovered by the initial analysis of the data, we predict when and where similar crimes related to these crimes are most likely to occur.

Every 6 months, we force a "re-learning" of the patterns using all historical and recent crime data. This ensures that new patterns of behavior are picked up by the system as well.

# How that bluelight in gadgets affects your health.

-Rushabh Wadkar, B.E

Technology and Light from technology, have entered our living and sleeping spaces in a big way in recent years. While the benefits of electricity, in the form of bulbs, tubelights and entertainment devices, have made it easier for people to continue their work and entertainment whenever they want, the light from gadgets has started affecting our health. A big source of concern is the 'blue light'.

The light spectrum includes ultraviolet, infrared and visible rays. Blue light is a part of visible rays and has the highest energy wavelength.

Blue light is a part of our daily requirement from sunlight that helps us stay alert, assists memory and elevates mood. Psychologists are known to prescribe 'sun therapy' to their patients for the same reason.

While we have always been exposed to blue light from the sun, experts have started to worry about an increase in exposure from electronic devices. "In present times, humans are getting exposed to many other sources of blue light such as LEDs, CFLs, tablets, televisions and computer screens. There is no doubt that the exposure of blue light is on the rise. This cumulative exposure over time has the potential to damage the photoreceptors in our retina — the light-sensitive part of the eyes — which in turn slowly leads to blindness," says Dr Santhosh Chidangil, professor and head of department of Atomic and Molecular Physics at Manipal University.

Not just eyesight, long-term exposure to blue light can also potentially cause other issues. "Researchers have shown that light influences humans physically by affecting hormone secretion, heart rate, alertness, sleep propensity, body temperature and even the gene expression. In certain other experiments, it has been shown that blue light can potentially elevate body temperature, heart rate and reduce sleepiness," says Chidangil. Dr Rajesh R, who works as a consultant for vitreo and ocular oncology for Sankara Eye Hospital, Bengaluru, says that apart from blue light, one should also be aware of ultraviolet rays that have the potential to damage your eyes. "Ultraviolet light can have harmful effects on the cornea, lens and retina. It can lead to light sensitivity, progression of cataract and retinal damage," he says.

In present times, it may be difficult to keep oneself away from devices that emit blue light, as most are required for our daily work and entertainment. However, there are ways to limit its exposure. "There are many apps on phones and protective devices for desktop and computer screens that allow you to limit your exposure to blue light. The apps remove blue light from the screen, giving it an almost sepia look. But more importantly, it is necessary for people to switch off and not use devices at least two hours before going to sleep," says Dr Janaki Chopra, a general physician practising in Hyderabad.

# Soon, charge your smartphone using sunlight, heat.

-Rushabh Wadkar, B.E

Sunlight, heat in a room and even movements may soon power your portable and wearable gadgets such as smartphones, thanks to a material identified by scientists that can extract energy from multiple sources at the same time.

Researchers from the University of Oulu in Finland have found that a mineral with the perovskite crystal structure has the right properties to extract energy from many forms of energy that surround us and is normally wasted. Perovskites are a family of minerals, many of which have shown promise for harvesting one or two types of energy at a time - but not simultaneously.

One member may be good for solar cells, while other may be good at harnessing energy from changes in temperature and pressure.

Yang Bai and his colleagues studied a specific type of perovskite called KBNNO, which may be able to harness many forms of energy.

Like all perovskites, KBNNO is a ferroelectric material, filled with tiny electric dipoles analogous to tiny compass needles in a magnet.

When ferroelectric materials like KBNNO undergo changes in temperature, their dipoles misalign, which induces an electric current. Electric charge also accumulates according to the direction the dipoles point. Deforming the material causes certain regions to attract or repel charges, again generating a current. Previous researchers have studied KBNNO's photovoltaic and general ferroelectric properties, but they did so at temperatures a couple hundred degrees below freezing, and they did not focus on properties related to temperature or pressure. The new study represents the first time anyone has evaluated all of these properties at once above room temperature, said Bai. The experiments showed that while KBNNO is reasonably good at generating electricity from heat and pressure, it is not quite as good as other perovskites.

Within the next year, Bai said, he hopes to build a prototype multi-energy-harvesting

device. The fabrication process is straightforward, so commercialization could come in just a few years once researchers identify the best material.

"This will push the development of the Internet of Things and smart cities, where power-consuming sensors and devices can be energy sustainable," he said. This kind of material would likely supplement the batteries on your devices, improving energy efficiency and reducing how often you need to recharge. The research was published in the journal Applied Physics Letters.

# Google Achieves First-Ever Successful SHA-1 Collision Attack.

-Rushabh Wadkar, B.E

SHA-1, Secure Hash Algorithm 1, a very popular cryptographic hashing function designed in 1995 by the NSA, is officially dead after a team of researchers from Google and the CWI Institute in Amsterdam announced today submitted the first ever successful SHA-1 collision attack.

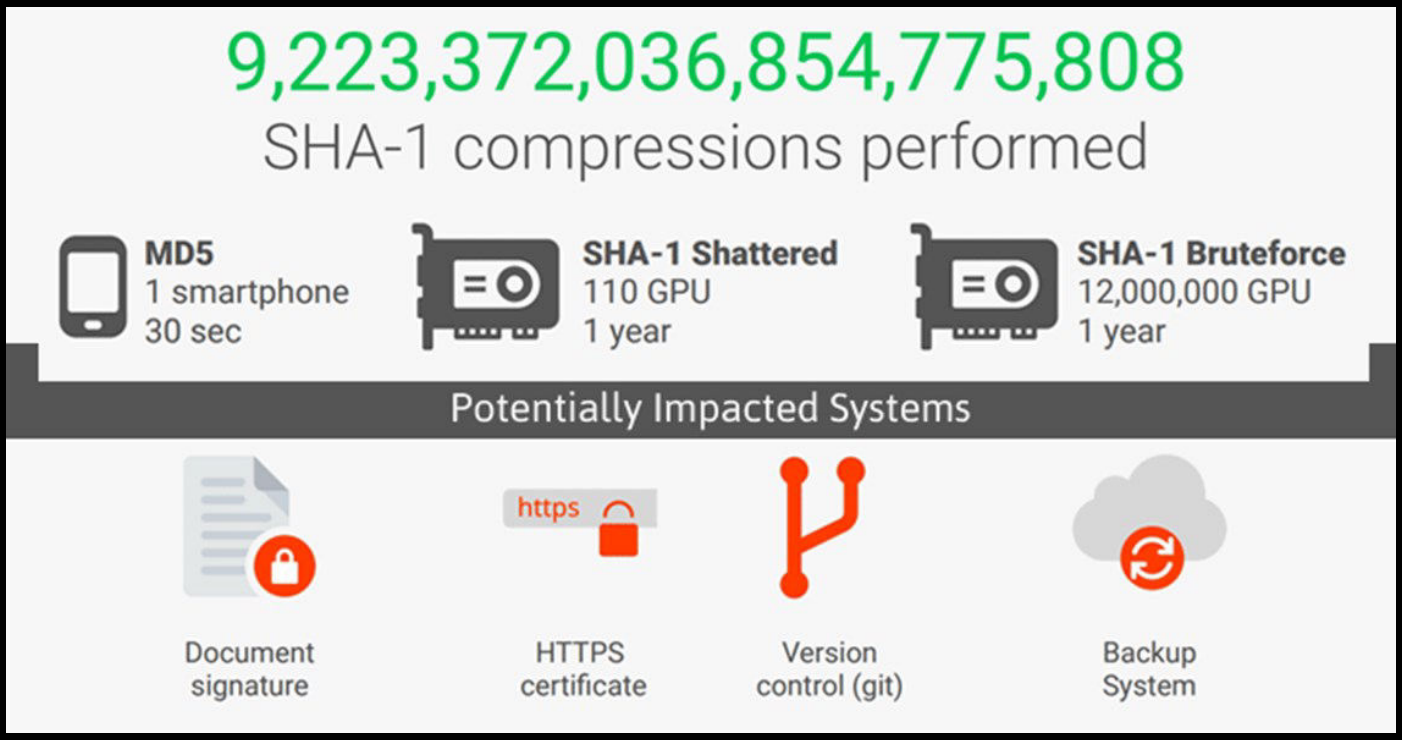
SHA-1 was designed in 1995 by the National Security Agency (NSA) as a part of the Digital Signature Algorithm. Like other hashes, SHA-1 also converts any input message to a long string of numbers and letters that serve as a cryptographic fingerprint for that particular message.

Collision attacks appear when the same hash value (fingerprint) is produced for two different messages, which then can be exploited to forge digital signatures, allowing attackers to break communications encoded with SHA-1.

The explanation is technologically tricky, but you can think of it as attackers who surgically alter their fingerprints in order to match yours, and then uses that to unlock. The researchers have been warning about the lack of security of SHA1 from over a decade ago, but the hash function remains widely used.

In October 2015, a team of researchers headed by Marc Stevens from the Centrum Wiskunde & Informatica (CWI) in the Netherlands had published a paper that outlined a practical approach to creating a SHA-1 collision attack – Freestart Collision. our Smartphone.

The researchers have been warning about the lack of security of SHA1 from over a decade ago, but the hash function remains




widely used.

In October 2015, a team of researchers headed by Marc Stevens from the Centrum Wiskunde & Informatica (CWI) in the Netherlands had published a paper that outlined a practical approach to creating a SHA-1 collision attack – Freestart Collision.

The Google approached the same group of researchers, worked with them and today published new research detailing a successful SHA1 collision attack, which they dubbed SHAttered and costs just $110,000 to carry out on Amazon's cloud computing platform.

According to researchers, the SHAttered attack is 100,000 faster than the brute force attack.

"This attack required over 9,223,372,036,854,775,808 SHA1 computations. This took the equivalent processing power as 6,500 years of single-CPU computations and 110 years of single-GPU computations," the researcher explains.

"While those numbers seem very large, the SHA-1 shattered attack is still more than 100,000 times faster than a brute force attack which remains impractical."

Despite declared insecure by researchers over a decade ago and Microsoft in November 2013, announcing it would not accept SHA1 certificates after 2016, SHA1 has widely been used over the Internet.

So, it's high time to migrate to safer cryptographic hashes such as SHA-256 and SHA-3. Google is planning to release the proof-of-concept (PoC) code in 90 days, which the company used for the collision attack, meaning anyone can create a pair of PDFs that hash to the same SHA-1 sum given two distinct images with some pre-conditions.

Therefore, an unknown number of widely used services that still rely on the insecure SHA1 algorithm have three months to replace it with the more secure one.

Meanwhile, Google and researchers have released a free detection tool that detects if files are part of a collision attack. You can find both the tool and much more information about the first collision attack at shattered.io.

# How big data analytics helped decode the Panama Papers.

-Swapnil Veunde, B.E

ICIJ turned to Nuix to help unravel the secrets of offshore banking scandal. Nuix Pty Ltd is an Australian company that produces a software platform for indexing, searching, analyzing and extracting knowledge from unstructured data, with applications that include digital investigation, cyber security, information governance, e-Discovery, email migration and privacy. The software platform is used by organizations in more than 45 countries.

The sheer variety and volume of this data rendered manually going through it all was impractical, if not impossible, as was the use of traditional analytics and search software. Consequently, the ICIJ called in big data analytics firm Nuix to help make sense of the vast amount of information it had received.

"We take in lots of different sorts of information - it could be email, databases, images, PDFs, all those different file formats - and extract all of the text and all of the metadata (information about the file itself). Once it has been indexed we can do some great analytical things, such as bringing out people's names or credit card information if necessary. We can also see who is connected to whom, so if we find a person's name in an email, maybe we want to find that person's name in other documentation and other things like that as well," Carl Barron, Nuix's senior solutions consultant explained.

Nuix and the ICIJ have been working together for over four years, but this is the largest data analysis that has ever been done before on leaked information - 10 times that seen in the Offshore Leaks documents in 2013.

However, for Nuix's software this wasn't an extraordinary volume of data, being described by Barron as "quite routine".

The information released in the Panama Papers has discovered alleged cases of money laundering, involvement with organized crime, bribery and corruption at the highest levels of global government.

While Süddeutsche Zeitung has only gone so far as to say it received the information from an anonymous source, Mossack Fonseca, the subject of the leak, has claimed the data was extracted through a hack on its email servers.

# Alan Turing

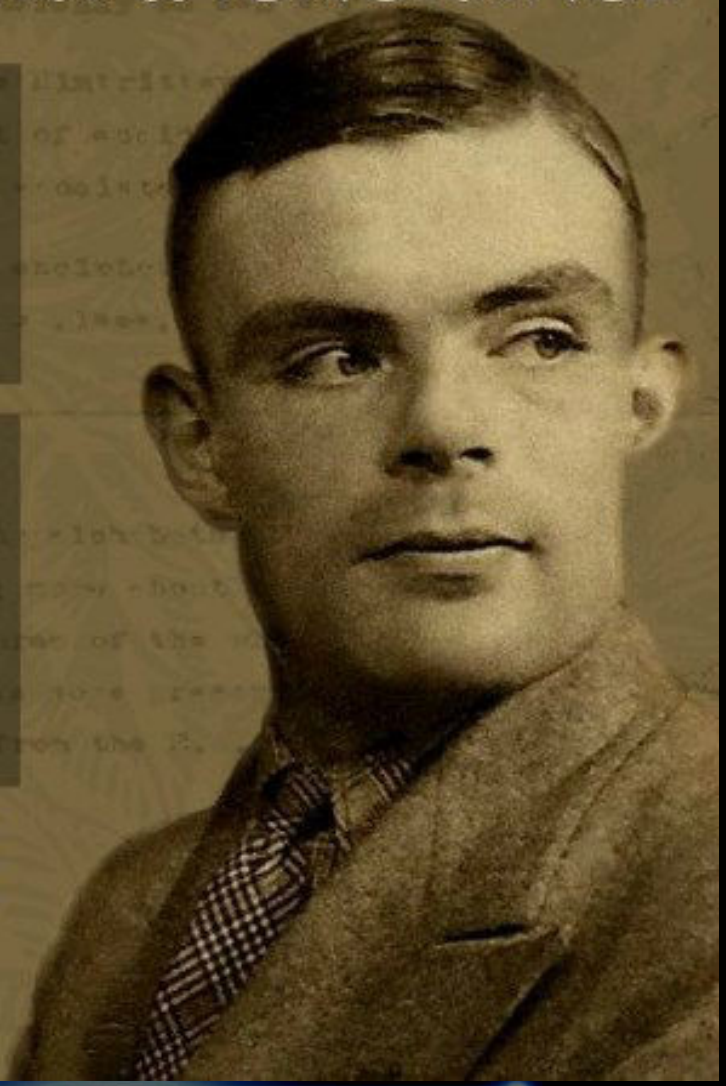
## FATHER OF MODERN COMPUTING

## CASUALTY OF BIGOTRY & IGNORANCE

In addition to basically saving the world during World War II by helping crack the 'impenetrable' Enigma code used by the Nazis, Alan Turing's elaborate thought experiments became the precursor on which modern computers were built.

Despite his invaluable contributions to science, Turing was also a homosexual male, which was still a crime in the UK in the 1950's. Given the choice between chemical castration and imprisonment, he chose the former.

He killed himself 2 years later.



*It is harder to crack a prejudice than an atom.*