
INFOLINE
VOLUME VIII ISSUE II
SEPTEMBER 2017
REASON
Lr
CC
DEPARTMENT OF COMPUTER TECHNOLOGY AND INFORMATION TECHNOLOGY
KONGU ARTS AND SCIENCE COLLEGE
(Autonomous)
Affiliated to Bharathiar University, Coimbatore.
Approved by UGC and AICTE and Re-accredited by NAAC
ISO 9001:2015 Certified Institution
Nanjanapuram, Erode – 638 107.
KONGU
Assuring the Best

INFOLINE

EDITORIAL BOARD

CONTENTS

RANSOMWARE VIRUS

Ransomware is a type of cyber attack that locks all digital files and demands payment in order for them to be returned. Computers that are infected with a ransomware virus become unusable save for displaying a ransom note. It is difficult to recover files from a computer that has been infected with ransomware and victims are often advised not to pay the fee. If they do decide to they are advised that their information may not be returned fully and that it has been compromised.

A variant of the Petya ransomware, which has been around for more than a year, was blamed for Tuesday's global attack. Petya is a vicious form of the virus that locks a computer's hard drive as well as individual files stored on it. It is harder to recover information from computers affected by this ransomware, which can also be used to steal sensitive information.

Cyber security experts Kaspersky Lab released a conflicting report that said the ransomware was not related to Petya but was in fact a new program it called NotPetya.

Security experts said the program could have spread in a similar way to the WannaCry attack that hit hundreds of thousands of computers including the NHS earlier this year. Like WannaCry, Petya could have used Eternal Blue, a tool created by the National Security Agency and leaked online by the Shadow Brokers that exploits a problem in Microsoft's software.

The attack hit around 2,000 computers in around a dozen countries including the UK, US, France and Germany. State-run and public organisations were affected, with the global advertising giant WPP and the Ukrainian National Bank both reporting problems.

The most affected country was Ukraine where the Chernobyl nuclear power plant systems were reportedly switched to manual as a precautionary measure.

Computers running the most recent update of Microsoft's software should be safe from the attack. Users are advised to check they have installed the latest version of Windows and refrain from clicking on malicious links.

SRIDHARSHINI R K

II B.Sc. (Information Technology)

GOOGLE APP ENGINE ADDS SUPPORT FOR JAVA 8

Google has made the Java 8 runtime generally available on App Engine, the Google Cloud Platform's development platform service. Google said the upgrade removes performance limitations Java developers had to deal with when using the Java 7 runtime. Java 7 remains a supported option.

"Unfortunately, using Java 7 on App Engine standard environment also required compromises, including limited Java classes, unusual thread execution, and slower performance because of sandboxing overhead," said Amir Rouzrokh, Google product manager.

These limitations are now removed with the move to Java 8. Google App Engine now offers an OpenJDK 8 JVM, the Jetty 9 web server and servlet container, the gRPC framework, and Google Cloud Client Library for Java. The standard App Engine environment also enables use of off-the-shelf frameworks such as Spring Boot and alternative JVM languages such as Kotlin. Support for Java 8 follows Google's addition of support for C#, Node.js, and Ruby on App Engine in March.

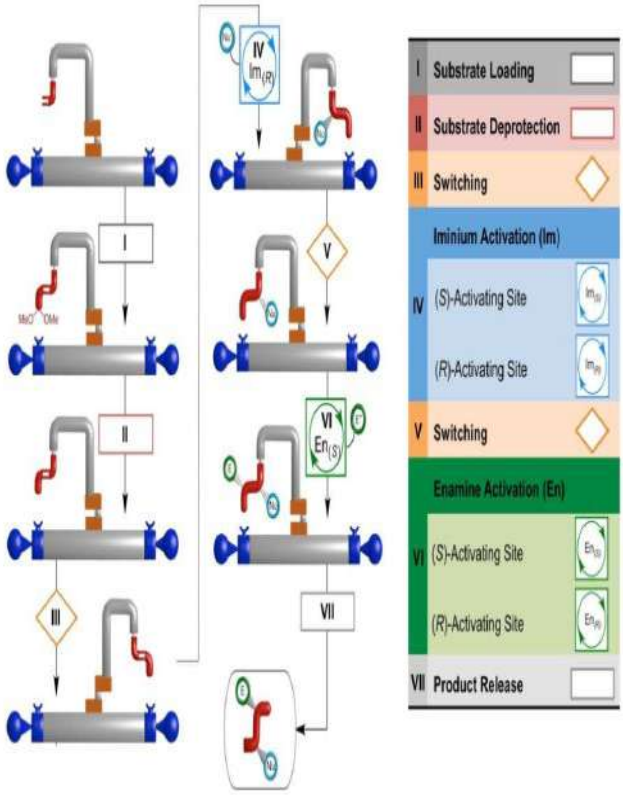
Java 8 had been available on the App Engine standard environment in a beta release since earlier this quarter, with Google using the beta period to improve performance. With the general release, Java 8 is now covered by the App Engine Service Level Agreement, which features a 99.95 percent uptime clause. To migrate to Java 8, users add the java8 line to their appengine-web.xml file and redeploy the application.

The Java 8 JDK (Java Development Kit) was rolled out in March 2014. Oracle just last week introduced JDK 9, which introduces modularity and a host of other features. Rouzrokh notes that Google is "hard at work" to bring OpenJDK 9 support to App Engine.

ANITHA A

II B.Sc. (Computer Technology)

WORLD'S FIRST 'MOLECULAR ROBOT' CAPABLE OF BUILDING MOLECULES



Scientists at The University of Manchester have created the world's first 'molecular robot' that is capable of performing basic tasks including building other molecules. The tiny robots, which are a millionth of a millimetre in size, can be programmed to move and build molecular cargo, using a tiny robotic arm.

Each individual robot is capable of manipulating a single molecule and is made up of just 150 carbon, hydrogen, oxygen and nitrogen atoms. To put that size into context, a billion of these robots piled on top of each other would still only be the same size as a single grain of salt.

The robots operate by carrying out chemical reactions in special solutions which can then be controlled and programmed by scientists to perform the basic tasks. In the future such robots could be used for medical purposes, advanced manufacturing processes and even building molecular factories and assembly lines.

Professor David Leigh, who led the research at University's School of Chemistry, explains: 'All matter is made up of atoms and these are the basic building blocks that form molecules. The robot is literally a molecular robot constructed of atoms just like you can build a very simple robot out of Lego bricks. The robot then responds to a series of simple commands that are programmed with chemical inputs by a scientist.

It is similar to the way robots are used on a car assembly line. Those robots pick up a panel and position it so that it can be riveted in the correct way to build the bodywork of a car. So, just like the robot in the factory, our molecular version can be programmed to position and rivet components in different ways to build different products, just on a much smaller scale at a molecular level.

The benefit of having machinery that is so small is it massively reduces demand for materials, can accelerate and improve drug

discovery, dramatically reduce power requirements and rapidly increase the miniaturisation of other products. Therefore, the potential applications for molecular robots are extremely varied and exciting.

Prof Leigh says: Molecular robotics represents the ultimate in the miniaturisation of machinery. Our aim is to design and make the smallest machines possible. This is just the start but we anticipate that within 10 to 20 years molecular robots will begin to be used to build molecules and materials on assembly lines in molecular factories. Whilst building and operating such tiny machine is extremely complex, the techniques used by the team are based on simple chemical processes.

It is the same sort of process scientists use to make medicines and plastics from simple chemical building blocks. Then, once the nano-robots have been constructed, they are operated by scientists by adding chemical inputs which tell the robots what to do and when, just like a computer program.

KALIKKUMAR V

III B.Sc. (Computer Technology)

SONY TO LAUNCH NEW 'UPDATED' PLAYSTATION VR HEADSET

Japanese electronics giant Sony is set to launch an updated variant of its Playstation VR headset. According to a blog post on its Playstation website, the company will release the updated VR headset in Japan on October 14. The launch date of the headset in US and other markets will be revealed later.

A year after its launch, Sony is updating the design of the PlayStation VR headset, streamlining things a little bit and removing the previous imposition of having to disconnect the unit in order to view HDR content on the PS4 console. The new PlayStation VR headset model is distinguishable by the relocation of its headphone jack from the wire hanging from the headset to the back of the unit, making for a cleaner, more integrated design. There's also a thinner connection cable to the PS4, to go with an upgraded Processor Unit that makes HDR pass through possible with this model.

A hardware update to PlayStation VR is being prepared. The new version, model

number CUH-ZVR2, features an updated design that enables the stereo headphone cables to be integrated with the VR headset and a slimmer, streamlined connection cable. There's also an updated Processor Unit that supports HDR pass through, enabling users to enjoy HDR-compatible PS4 content on a TV without having to disconnect the Processor Unit in between the TV and the PS4 system. This function can be used only when the VR headset is turned off.

The company has also changed the packaging of the new model. The previous PS VR's model number is CUH-ZVR1, and the new PS VR's model number is CUH-ZVR2. Also, the product image on the packaging will be updated to show changes on the new model, like the integrated headphones on the VR headset, said Sony on the blog.

Sony India gave a price cut to the PS VR headset. The VR headset was launched earlier this year at Rs 41,990 but is now available for Rs 37,990. The Playstation VR headset bundles comes in with the headset, cables, demo disc and the PS4 camera needed for VR. Along with the headset, Playstation VR games also got a price cut. Some of the games whose prices have have been slashed include Battlezone, RIGS and Eve Valkyrie.

MYTHILI T

III B.Sc. (Information Technology)

NEW TECHNOLOGY TURNS ANY OBJECT INTO TV REMOTE

Scientists have developed a technology that can turn everyday objects - such as teacups or toy cars - into remote controls for televisions. Researchers from Lancaster University in the UK show a novel technique that allows body movement, or movement of objects, to be used to interact with screens.

The Matchpoint technology, which only requires a simple webcam, works by displaying moving targets that orbit a small circular widget in the corner of the screen. These targets correspond to different functions - such as volume, changing channel or viewing a menu. The user synchronises the direction of movement of the target, with their hand, head or an object, to achieve what researchers call spontaneous spatial coupling, which activates to the desired function.

Unlike existing gesture control technology, the software does not look for a specific body part it has been trained to identify - such as a hand. The technology looks for rotating movement so it does not require calibration, or the software to have prior knowledge of objects. This provides much more flexibility and ease for the user as it works even while hands are full, and while stood or slouching on the sofa.

Users also do not need to learn specific commands to activate different functions, as is the case with some gesture controlled televisions on the market, and the user is able to decouple at will.
When selecting volume adjustment or channel selection, sliders appear. The user moves their hand, head, or object, in the required direction indicated by the slider to change the volume or to find the desired channel.

As well as televisions, the technology can also be used with other screens. For example, YouTube tutorials, such as mending bikes or baking cakes, could be easily paused and rewound on tablet computers without users having to put down tools or mixing bowls.

Multiple pointers can be created to allow more than one user to point at drawings or pictures on interactive whiteboards simultaneously. Matchpoint also allows users to manipulate images on whiteboards by using two hands to zoom in and out, and rotate images.

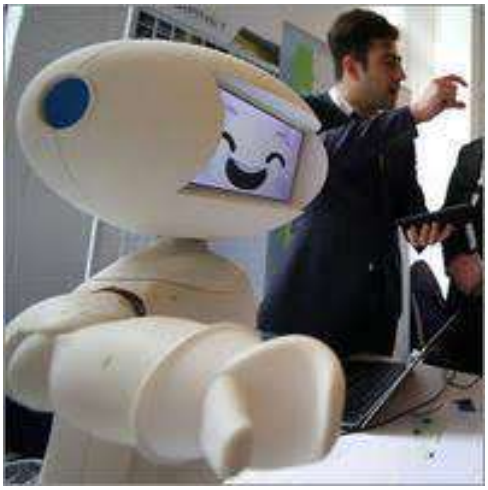
In addition to short-term couplings, users can also link stationary objects to controls, which even when left for prolonged periods will retain their control function.

VARSHA R

I B.Sc. (Information Technology)

SOCIAL ROBOTS: PROGRAMMABLE BY EVERYONE

The business model of LuxAI is developing and constructing so-called social robots. Such robots can be used, for example, in the educational or health system, where they would support trainers and therapists in their work. The robots can be programmed to practice vocabulary with children or to make rehabilitation exercises with stroke patients.



The "AI" in LuxAI stands for Artificial Intelligence. Robots that are supposed to interact with humans have to process a great deal of information very quickly, and adapt their behaviours according to the interaction, says the CEO of LuxAI, Dr. Pouyan Ziafati. Ziafati wrote his doctoral thesis on artificial intelligence and robotics at the SnT and founded LuxAI based on it. Our robot is the first social robot to come out of Luxembourg, says Ziafati: We have already run the prototype through practical tests. It received

excellent scores for its social expressiveness, emotionality and ease of use.

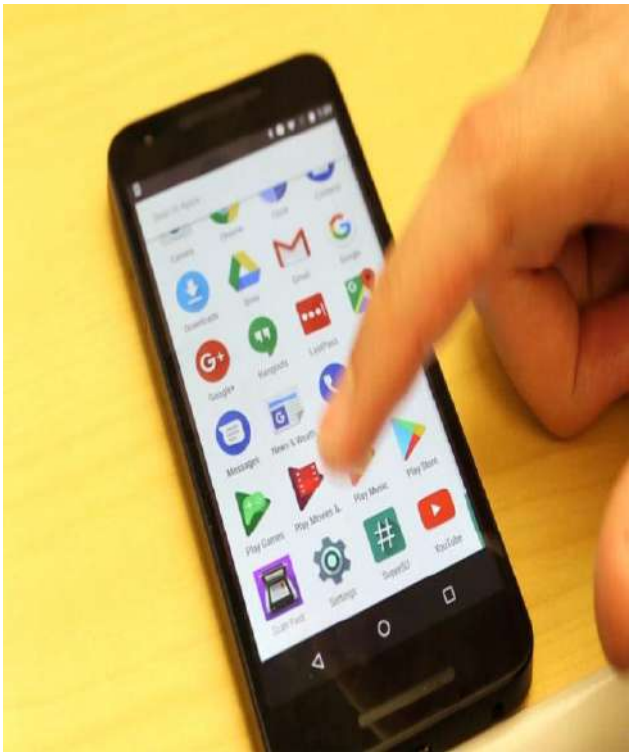
The heart of every robot is its programming the software. LuxAI's social robot is based on a so-called Robot Agent Programming Language, which Ziafati designed for his doctorate and adapted to the needs of social robots. Such programming, however, is only accessible to IT experts. Practitioners who want to teach a robot how to train stroke patients, for example, can't learn their way into it, says Ziafati. "They need an interface by which they can program the robot intuitively and naturally"

LuxAI in cooperation with the Autonomous Robot Lab of the Computer Science and Communications Research Unit (CSC) of the University of Luxembourg has developed this interface. It is based on the same Android platform as is widespread on smartphones, and can make social robots suitable for the mass market, as Ziafati assures. "Non-IT-expert people have made the first tests with our robots. They were able to program the robots for their purpose within 20 minutes. Our software lets anyone do it. Ziafati sees possibilities for many fields of application: as learning support for autistic children, in schools, in the entertainment industry or in geriatric care.

Social robots will never replace qualified personnel but they can support them, since they have unlimited time and can take over routine tasks, Luxembourg and three departments in the University of Luxembourg on developing applications for autism therapy and behavioural regulation, geriatric medicine and teaching foreign languages to children in kindergardens.

VISHNUVARDHAN A
I B.Sc. (Computer Technology)

COMBINATION OF FEATURES PRODUCES NEW ANDROID VULNERABILITY



A new vulnerability affecting Android mobile devices results not from a traditional bug, but from the malicious combination of two legitimate permissions that power desirable and commonly-used features in popular apps.

The combination could result in a new class of attacks, which has been dubbed "Cloak and Dagger."

The vulnerability, which was identified and tested in closed environments by computer scientists at the Georgia Institute of Technology, would allow attackers to silently take control of a mobile device, overlaying the graphical interface with false information to hide malicious activities being performed underneath -- such as capturing passwords or extracting the user's contacts. A successful attack would require the user to first install a type of malware that could be hidden in a pirated game or other app.

Georgia Tech researchers have disclosed the potential attack to Google, maker of the Android system, and details of the vulnerability will be presented at the 38th IEEE Symposium on Security and Privacy in San Jose, California. But because it involves two common features that can be misused even when they behave as intended, the issue could be more difficult to resolve than ordinary operating system bugs.

In Cloak and Dagger, identified two different Android features that when combined, allow an attacker to read, change or capture the data entered into popular mobile apps. The two features involved are very useful in mapping, chat or password manager apps, so preventing their misuse will require users to trade convenience for security.

The first permission feature involved in the attack, known as "BIND_ACCESSIBILITY_SERVICE," supports the use of devices by disabled persons, allowing inputs such as user name and password to be made by voice command, and allowing outputs such as a screen reader to help the disabled view content. The second permission, known as "SYSTEM_ALERT_WINDOW," is an overlay or "draw on top" feature that produces a window on top of the device's usual screen to display bubbles for a chat program or maps for a ride-sharing app.

When combined in a malicious way, "SYSTEM_ALERT_WINDOW" acts as a cloak, while "BIND_ACCESSIBILITY_SERVICE" serves as the dagger. The two could allow attackers to draw a window that fools users into believing they are interacting with legitimate features of the app. The malicious program, operating as the overlay, would then capture the user's credentials for the malware author, while the accessibility permission would enter the credentials into the real app hidden beneath, allowing it to operate as expected, leaving the user with no clue that anything is awry.

The researchers tested a simulated attack on 20 users of Android mobile devices

and found that none of them noticed the attack. Of most concern to Georgia Tech's researchers is that these permissions may be automatically included in legitimate apps from the Google Play store, meaning users do not need to explicitly grant permissions for the attack to succeed.

This is a design flaw that some might say allows the app functionality to work as intended, but our research shows that it can be misused. Once the phone is compromised, there may be no way for the user to understand what has happened?

Nearly 10 percent of the top 5,000 Android apps use the overlay feature and many are downloaded with the accessibility feature enabled. Creating vulnerabilities when permissions are combined may be a reality that system developers will have to consider more seriously in the future. Changing a feature is not like fixing a bug. System designers will now have to think more about how seemingly unrelated features could interact. Features do not operate separately on the device.

Android versions up to and including the current 7.1.2 are vulnerable to this attack. The researchers caution that it may be difficult to determine the status of the settings required for the attack.

There are two key precautions one is to avoid downloading apps from providers other than branded outlets such as the Google Play store. A second step is to check the permission requests that apps make before allowing them to operate.

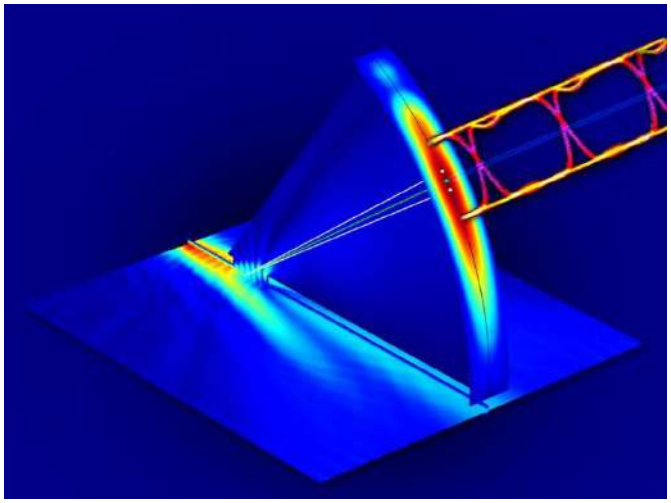
Users need to be careful about the permissions that new apps request. If there are very broad permissions, or the permissions don't seem to match what the app is promising to do, you need to be sure you really need that app.

The researchers have produced a video that shows the attack and how to check these permissions, which are in different locations depending on the mobile operating system version.

Apps from name-brand sources such as Facebook, Uber and Skype should be okay. But with a random game or free versions of paid apps that you might download, you should be very careful. These features are very powerful and can be abused to do anything you could do as a user without you knowing.

SELVA BHARATHI A
I B.Sc. (Computer Technology)

FIRST DATA TRANSMISSION THROUGH TERAHERTZ MULTIPLEXER



Multiplexing, the ability to send multiple signals through a single channel is a fundamental feature of any voice or data communication system. An international research team has demonstrated for the first time a method for multiplexing data carried on terahertz waves, high-frequency radiation that may enable the next generation of ultra-high bandwidth wireless networks.

The transmission of two real-time video signals through a terahertz multiplexer at an aggregate data rate of 50 gigabits per second, approximately 100 times the optimal data rate of today's fastest cellular network. To transmit separate data streams on terahertz waves at very high speeds and with very low error rates. This is the first time anybody has characterized a terahertz multiplexing system using actual data.

Current voice and data networks use microwaves to carry signals wirelessly. But the demand for data transmission is quickly becoming more than microwave networks can handle. Terahertz waves have higher frequencies than microwaves and therefore a much larger capacity to carry data. However, scientists have only just begun experimenting with terahertz frequencies, and many of the basic components necessary for terahertz communication.

A system for multiplexing and demultiplexing (also known as mux/demux) is one of those basic components. It's the technology that allows one cable to carry multiple TV channels or hundreds of users to access a wireless Wi-Fi network.

The mux/demux approach Mittleman and his colleagues developed uses two metal plates placed parallel to each other to form a waveguide. One of the plates has a slit cut into it. When terahertz waves travel through the waveguide, some of the radiation leaks out of the slit. The angle at which radiation beams escape is dependent upon the frequency of the wave.

There are several waves at several different frequencies each of them carrying a data stream into the waveguide, and they won't interfere with each other because they're different frequencies that's multiplexing, Mittleman said. Each of those frequencies leaks

out of the slit at a different angle, separating the data stream that's demultiplexing.

Because of the nature of terahertz waves, signals in terahertz communications networks will propagate as directional beams, not directional broadcasts like in existing wireless systems. This directional relationship between propagation angle and frequency is the key to enabling mux/demux in terahertz systems. A user at a particular location (and therefore at a particular angle from the multiplexing system) will communicate on a particular frequency.

In 2015, Mittleman's lab first published a paper describing their waveguide concept. For that initial work, the team used a broadband terahertz light source to confirm that different frequencies did indeed emerge from the device at different angles. While that was an effective proof of concept, Mittleman said, this latest work took the critical step of testing the device with real data.

Working with Guillaume Ducournau at Institut d'Electronique de Microélectronique et de Nanotechnologie, CNRS/University of Lille, in France, the researchers encoded two high-definition television broadcasts onto terahertz waves of two different frequencies: 264.7 GHz and 322.5 GHz. They beamed both frequencies together into the multiplexer system, with a television receiver set to detect the signals as they emerged from the device. When the researchers aligned their receiver to the angle from which 264.7 GHz waves were emitted, they saw the first channel. When they aligned with 322.5 GHz, they saw the second.

Further experiments showed that transmissions were error-free up to 10 gigabits per second, which is much faster than today's standard Wi-Fi speeds. Error rates increased somewhat when the speed was boosted to 50 gigabits per second (25 gigabits per channel), but were still well within the range that can be fixed using forward error correction, which is commonly used in today's communications networks.

In addition to demonstrating that the device worked, Mittleman says the research revealed some surprising details about transmitting data on terahertz waves. When a terahertz wave is modulated to encode data turned on and off to make zeros and ones the main wave is accompanied by sideband frequencies that also must be detected by a receiver in order to transmit all the data. The research showed that the angle of the detector with respect to the sidebands is important to keeping the error rate down.

Detecting the full power of the signal, but we're receiving one sideband a little better than the other, which increases the error rate. Mittleman explained. So it is important to have the angle right.

The researchers plan to continue developing this and other terahertz components. Mittleman recently received a license from the FCC to perform outdoor tests at terahertz frequencies on the Brown University campus.

IYSWARIYA R
I B.Sc. (Information Technology)

QUANTUM COMPUTER

A quantum computer is any device for computation that makes direct use of distinctively quantum mechanical phenomena, such as superposition and entanglement to perform operations on data.

In a classical (or conventional) computer, information is stored as bits in a quantum computer it is stored as qubits (quantum bits). The basic principle of quantum computation is that the quantum properties can be used to represent and structure data, and that quantum mechanisms can be devised and built to perform operations with this data.

Although quantum computing is still in its infancy, experiments have been carried out in which quantum computational operations were executed on a very small number of qubits.

Research in both theoretical and practical areas continues at a frantic pace, and many national government and military funding agencies support quantum computing research to develop quantum computers for both civilian and national security purposes, such as cryptanalysis.

If large-scale quantum computers can be built, they will be able to solve certain problems exponentially faster than any of our current classical computers (for example Shor's algorithm). Quantum computers are different from other computers such as DNA computers and traditional computers based on transistors.

Some computing architectures such as optical computers may use classical superposition of electromagnetic waves, but without some specifically quantum mechanical resources such as entanglement, they have less potential for computational speed-up than quantum computers.

The power of quantum computers Integer factorization is believed to be computationally infeasible with an ordinary computer for large integers that are the product of only a few prime numbers (e.g., products of two 300-digit primes). By comparison, a quantum computer could solve this problem more efficiently than a classical computer using Shor's algorithm to find its factors.

This ability would allow a quantum computer to "break" many of the cryptographic systems in use today, in the sense that there would be a polynomial time (in the number of

bits of the integer) algorithm for solving the problem. In particular, most of the popular public key ciphers are based on the difficulty of factoring integers, including forms of RSA.

These are used to protect secure Web pages, encrypted email, and many other types of data. Breaking these would have significant ramifications for electronic privacy and security.

The only way to increase the security of an algorithm like RSA would be to increase the key size and hope that an adversary does not have the resources to build and use a powerful enough quantum computer. It seems plausible that it will always be possible to build classical computers that have more bits than the number of qubits in the largest quantum computer.

KEERTHANA R
II B.Sc. (Computer Technology)

THE DATA MANAGEMENT CHALLENGES OF TOP CLOUD PROVIDERS

Seagate's engineers have worked closely with the world's largest cloud providers and OEMs to gain a deeper understanding of the data management challenges they face. This insight led the engineering team to implement several new firmware and hardware innovations to the helium-filled hard drives, resulting in the following key improvements:

- Highly scalable hard drive storage that is rapidly deployable for maximum performance and energy efficiency for Open Compute Project (OCP) platforms.
- 50 percent higher capacity, which enables hyperscale customers to deploy over 10PB of high performance storage in a single 42U rack for the first time – maintaining current space, weight, and power consumption profiles.
- 21 percent increase in IOPs performance/watt perfect for next generation eco-friendly infrastructures.
- 20 percent increase in enhanced caching performance, which results in faster access to unstructured data.

These innovations enable customers to gain more control over unstructured data, store vastly more information and retrieve it more quickly than ever before without expanding the storage footprint in the data center. By offering the lowest power consumption and lowest weight in the industry, the drop-in upgrade 12TB drive translates to a groundbreaking TCO for hyper scale customers.

Data storage innovations have led to dramatically improved business results. For example, Cloud companies are storing massive amounts of videos and images in hyperscale

infrastructures for search and social applications. Our 12TB drive helps solve the proliferation of data both enterprise and cloud service customers must manage and move, while improving response times.

Seagate's new 12TB high density, enterprise-class hard drive will be a great addition to our OCP-compliant storage product family. As a major OCP solution provider, it's important to ensure compatibility of this innovative, high density hard drive with our OCP solutions that meet the needs of this growing market.

PRADEEP RAJAN R
III B.Sc. (Computer Technology)

CRYPTOCURRENCIES

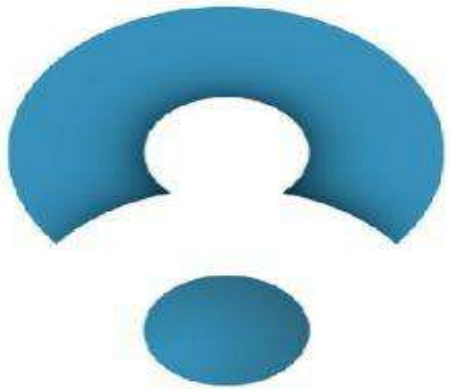
Investment opportunities in digital cryptocurrencies have been constantly rising over the past few years. These blockchain-based financial instruments have been giving back good returns ever since bitcoin was first introduced. Many countries, including India, have thus seen the growth of exchange platforms for assisting investors through the complexities of digital currency trading. There are seven major exchange platforms in India that one can effectively use for bitcoin and other altcoin investments.

Zebpay is an Ahmedabad-based bitcoin exchange which was founded in 2012. It was the first in India to introduce a user-friendly digital wallet for enabling bitcoin transactions using a 4-digit PIN, and without the complexities of understanding bitcoin addresses and taking back-ups for fear of losing currency. By the end of 2016, Zebpay became the first Indian exchange to cross the turnover of INR 6 billion in bitcoin transactions. It has a user base of over 8,00,000 and was voted as best new bitcoin exchange platform at the CoinAgenda conference in Las Vegas in 2014.

Unocoin, India's second most popular bitcoin exchange platform and wallet after Zebpay, was launched in Bangalore in the year 2013. Unocoin is a member of NASSCOM and has over 1,30,000 customers. It recently partnered with BTCJam, a global peer-to-peer bitcoin lending platform, to bring bitcoin loans service to India. Unocoin has also collaborated with over 25 Indian merchants and launched a mobile app for its customers to buy goods and

services in exchange for bitcoins. In addition, Unocoin enables users to convert their blockchain assets such as Ethereum, Monero, Zcash and Dash, directly into bitcoin and then if required, into INR. Unocoin bills a transaction fee of 1 percent for each bitcoin transaction.

Coinsecure was founded in 2014 and has its head office in New Delhi and a research division in Bangalore. It offers a bitcoin trading platform and wallet, along with other blockchain-based services. Coinsecure claims to provide the most secure wallet and merchant payment gateway for real-time trading. It also provides a mock trading platform for its customers. Coinsecure has partnered with Netki to help users to make their own simple wallet addresses instead of 32-character bitcoin public addresses. It has also collaborated with BitPay, a global bitcoin payment provider, to enable Indian merchants to accept bitcoins from customers. It charges 0.3 percent of a bitcoin transaction as fees.



BuyUcoin is another major exchange platform and introduced India's first altcoin exchange and has one of the simplest payment wallets which can be used to trade, store, use and accept digital currencies. It deals in a total of 18 cryptocurrencies and altcoins, including currency tokens like Bitcoin, Ethereum, Litecoin, AntShare, Bitcoin Cash and more with Indian rupees. BuyUcoin has a unique 0 percent trading fee model and does not charge any fee on the transitions. The exchange is based out of Uttar Pradesh and serves more than 15,000 customers.

Bitxoxo is India's first company to launch bitcoin pre-paid gift cards, in addition to buying and selling bitcoins. Bitxoxo has been involved in conducting workshops throughout India so as to enhance the knowledge and

applications of bitcoin among people. Bitxoxo charges no fees for any of its services and has a 0 percent fee model. Bitxoxo is open 24*7 and allows payments and withdrawals through IMPS, ensuring instant payments to customers' accounts, irrespective of banking hours. It recently crossed more than 100,000 users and runs out of Warangal, Telangana.

BTCXIndia was launched in Hyderabad and is also one of the major bitcoin exchanges in India. Apart from dealing in bitcoin, the platform offers real-time trading of the third-largest cryptocurrency in the world, Ripple (XRP), after it collaborated with Google-backed Ripple Labs. Bitxoxo's customers can store their currencies in a securely encrypted, passcode protected wallet with no holding fees. On transactions, a trading commission of 1 percent is charged.

EthexIndia is an online platform that allows the exchange of the second most-widely used cryptocurrency in the world, Ethereum (ETH). Started in 2016, ETHEXIndia is India's first ether exchange and provides real-time trading with the usage of an effective wallet system based on Ethereum. The company is reportedly growing rapidly with the surge in demand of Ethereum, especially after the skyrocketing of bitcoin prices. Ethexindia is owned by S Capital Solutions, which is the same company that owns BTCXIndia.

BitBay, one of the world's major digital currency trading platforms, has entered the Indian market, thus becoming the first international exchange to do so. Bitbay's platform currently accounts for more than 60% of the cryptocurrency market in central Europe. With its entry in India, BitBay will support bitcoin and allow trade and exchange of eight other types of cryptocurrencies like Ether, Gamecredits, Litecoin, Monero, Dash, Lisk, etc.

POORANI G
III B.Sc. (Computer Technology)

LACIE SAFE MOBILE HARD DRIVE

Storing your files on this mobile hard drive gives you multiple levels of protection because it uses advanced encryption and biometric authentication technology. The Safe uses 128-bit AES encryption (Advanced Encryption Standard) which is the same standard used by governments to protect top secret information.

Encryption converts information that is readable into a mixture of unreadable characters. Decryption processes the encrypted unreadable characters back into a readable format. The algorithm that encrypts and decrypts the information is known as a cipher. The cipher allows access to the readable information when you enter a password.

Most ciphers will use passwords that are four to eight characters in length, but a 128-bit AES cipher uses a 16 character password which is extremely difficult to hack. The AES cipher or "Rijndael" (pronounced Rein Dahl) is named after the Belgian inventors Joan Daemen and Vincent Rijmen.

Biometric authentication is a technology that recognizes physical or behavioral characteristics such as fingerprints, palm geometry, retina patterns, voice and signature. Fingerprint recognition is the most popular because it's easier to use.

Your finger is scanned for minutia, which are the points on a fingerprint where a ridge ends or splits into two. An algorithm extracts the minutia points and creates a template image that is used for authentication.

Features

• Fingerprint recognition
• Up to 5 user profiles
• Register 10 fingerprints
• Cross-platform for PC and Mac
• USB bus powered: no AC adapter needed**
• Plug & play: no software to install

ACCESSORIES

• Hi-Speed USB 2.0 cable
• USB power-sharing cable
• CD with User's Manual
• Quick Start Guide

SYSTEM REQUIREMENTS

• Windows 2000, XP, Vista™ / Mac OS 10.2.x or higher
• PC or Mac with built-in powered USB bus
• Pentium II 350 MHz / G3 processor compatible or greater
• Minimum 128MB of RAM

RASIKA M
III B.Sc. (Computer Technology)

ORIGAMI-STYLE SUITS TURN ROBOTS INTO REAL-LIFE TRANSFORMERS

Just as one might done a wet suit to work underwater or a spacesuit to work in space, researchers are designing exoskeletons for robots so the machines can wear a variety of outfits tailored to different missions. In experiments, self-folding, heat-activated origami suits created for robots could help the machines walk, roll, sail and glide, according to the new study.

Imagine future applications for space exploration, where you could send a single robot with a stack of exoskeletons to Mars. The robot could then perform different tasks by wearing different outfits

Unlike the shape-shifting robots in the "Transformers" films, in real life, existing bots are typically much less adaptable. Each part of a robot usually has a fixed structure and a single, defined purpose, making it difficult for robots to perform a wide variety of actions, the researchers said. In contrast, animals can often change their shapes to adapt to their environments. For instance, caterpillars undergo metamorphosis to become butterflies, and hermit crabs can switch their shells.

The scientists drew inspiration from nature to develop a robot that could transform itself with different outfits that enable it to perform different tasks.

If we want robots to help us do things, it's not very efficient to have a different one for each task, study senior author Daniela Rus, director of MIT's Computer Science and Artificial Intelligence Laboratory, said in a statement. "With this metamorphosis-inspired approach, we can extend the capabilities of a single robot by giving it different accessories to use in different situations."

The researchers used a small magnetic cube that they called "Primer." They placed the cube in an arena where they could use magnetic fields to make Primer move like a robot. In experiments, the scientists had Primer move onto various plastic origami sheets mounted on hot plates. Turning on the hot plates could then make the heat-activated sheets fold around the cube into various shapes in roughly 3 minutes.

Each of the exoskeletons Primer could wear had its own advantages. For example, "Wheel-bot" had wheels that helped it to move twice as fast as "Walk-bot." "Boat-bot" could float on water and carry nearly twice its weight. And "Glider-bot" could soar through the air.

Primer can even don multiple outfits at once, like a Russian nesting doll, according to the study. It could add one exoskeleton to become "Walk-bot," and then interface with another, larger suit that allows it to carry objects and move two body lengths per second. After Primer was finished with a task, it could step into water to dissolve any exoskeleton the device wore in less than 1 minute, the researchers said.

Now that the scientists have shown that Primer can wear a variety of exoskeletons, future research could show that similar suits could be developed for motorized robots as well, said study lead author Shuhei Miyashita, director of the microrobotics group at the University of York, in England. Potential applications could include ingestible robots that could use several exoskeletons to perform a number of tasks in the body, such as removing objects and patching wounds, he said.

Future research will also aim to create even more functional exoskeletons, to perform tasks ranging "from burrowing in sand to driving through water," Miyashita told Live Science. The scientists would also like "to make these robots smaller and more intelligent, and potentially use different types of biomaterials" so they can perform long-term operations in the body, he said.

RASIKA M
III B.Sc. (Computer Technology)

FUTURE OF BIG DATA REQUIRES HUMAN-MACHINE COOPERATION

Collecting, analyzing, and interpreting data is becoming essential for more businesses and more individuals than ever before. Now that we have the automated tools to process this data, we can make better decisions and more cost-efficiently as well. As more companies employ these tactics, competition rises, and it becomes even more imperative to take advantage of this efficiency. However, the real future of data management doesn't solely lie with machines instead, it lies with human-machine interfaces and cooperation.

1. **Machines need direction:** Machines or at least those we can foresee are highly skilled at answering questions, and terrible at generating the questions that need to be asked. Big data highlights this problem perfectly, imagine you have quadrillions of data points, collected from millions of people. In all likelihood, if you knew the right questions to ask and had a machine to pick through the data, you could easily find the answer you seek. But machines don't see patterns or meaning in data, they can only fetch it, or combine it in ways instructed by humans. Accordingly, humans remain a necessary part of the equation.

2. **Not all things are easily quantifiable:** You should also realize that not all decisions are easily quantifiable. In some

scenarios, you'll be presented with two options, one of which is inherently more cost-efficient, with no real downsides. But in others, the decision is not so clear. Take project portfolio management as an example; you can't use a single criterion, or even an unchanging aggregation of criteria, to prioritize one project over another. That's why it's helpful for machines to quantify and project what they can, but it's still necessary for humans to make the final call.

3. **Human biases:** Humans alone aren't great at decision-making. When faced with objective values and data, we can't help but distort that information based on our own persistent cognitive biases. For example, if we plumb the data with an assumption already in mind even if it's only subtle, and in the background we'll end up finding and prioritizing any data that reinforces those assumptions. Machines can't do this, because they won't extend beyond the logical parameters set for them.

4. **Processing limitations**: AI has yet to exceed the general abilities of the human brain, but in specific applications, it can't be beat. Anything requiring mathematical calculations can be done faster by a machine than with a human attempting a manual approach. However, machines have limits as well; humans see complex sets of data and automatically filter out what's unnecessary, instinctively honing in on high-level patterns. In machines, those patterns have to be taught or discovered from the ground up, or else, they'll brute-force the calculations one at a time until they arrive at a conclusion; this is why Go was much harder for computer programs to master than chess. With both humans and machines having processing limitations, they need each other to keep advancing.

5. **Long-term flexibility:** Great thinkers have long speculated about the power of a machine-human interface, and some (like Elon Musk) are working hard to make it a reality. We don't need to have machines embedded in our brains, but working together with human-machine interfaces gives us far more flexibility in future developments than abandoning tech or prioritizing tech usage exclusively.

SINDUJA T

I B.Sc. (Computer Technology)

POSSIBLE SOLUTIONS FOR WORKPLACE SECURITY THREATS IN THE AGE OF IOT

The internet-of-things (IoT) keeps growing larger, and soon, our workplaces will be brimming with embedded internet-connected devices meant to keep us in close contact and improve our collective productivity. Optimistic estimates of 50 billion connected devices by 2020 may have been a bit far-fetched, but we're not far behind estimates for the number of currently connected devices range from 6.4 billion to 17.6 billion.

However, there are some important security concerns with IoT that we'll need to address before we accept the system as the new normal for American workplaces. Knowing what challenges lie ahead and proactively preparing for them is the best course of action for anyone in an IT positionand for most American workers in general.

IoT :Security Risk

IoT isn't inherently more dangerous than any other kind of technology. It doesn't suffer from inherently inferior security standards or firewalls, but there are a few vulnerabilities that, by the nature of IoT, make devices in its network a potential target.

For example, IoT devices tend to collect lots of data, which could make any shared networks a prime target for cybercriminals looking to exploit that information. Because these networks comprise many individual devices, it's easier than usual to find a rogue vulnerability and infiltrate the network from there. Plus, because users may find it easy to pick up, exchange, or jump between devices, the opportunity for a connection or management mistake may be greater.

Possible Solutions

1. **Centralize and tightly control users.** First, you need to know who on your staff is accessing what, when, and where. Instituting a centralized management server that allows you to manage users, licenses, passwords, and access can help you do this. Only allow users to access the devices they need to perform their own duties, and keep close tabs on who's using what. This will help you prevent a number of simple mistakes, and can also help you identify root causes in any potential breaches that unfold in your future.

2. **Only purchase tested devices.** There are hundreds of companies all racing to produce the best devices and software for the IoT era. On one hand, this is exciting because all that competition is spurring tremendous innovation. On the other, this is concerning because it means companies may be spending their efforts on getting devices to market, rather than making the best products they can. Do extensive research on all the IoT products you procure, and avoid buying anything in its first iteration. Pay attention to the brands with a

history of secure and reliable performances, and don't take unnecessary risks.

3. **Forbid or control personal and professional cross-pollination.** Many companies now have a BYOD (bring your own device) policy, due to the ubiquity of personal laptops, tablets, and smartphones. In the age of IoT, however, this could be an increased liability. Using company devices on unsecured public networks could leave you vulnerable to attack, and any compromised device (including personal devices) that returns to your office's network could cause a company-wide breach. You'll need to consider forbidding this type of cross-pollination, or otherwise stating very clearly what security precautions are to be followed.

4. **Instill better personal security habits.** The vast majority of hacks and breaches are attributable to human error. You might have chosen a weak password and you may have failed to change your passwords regularly or you may have fallen for a phishing scheme (or similar attempt to steal your credentials or introduce malware to your device). Since the possibility for human error is going to multiply with each new connected device you add, you'll need to prevent this possibility by instilling your team with better ongoing security habits (and better knowledge of how breaches happen).

5. **Keep your software up-to-date.** It's a simple step, but an important one. Most software developers and device manufacturers are going to regularly release new updates as they discover the inevitable vulnerabilities of their work and repair them. Simply keeping your devices up-to-date can protect you from hundreds of potential threats.

KARTHIKEYAN S
II B.Sc. (Computer Technology)

It's fine to celebrate sucess but it is more important to heed the lesson of failure.

-Bill Gates