Toc H INSTITUTE OF SCIENCE & TECHNOLOGY

DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING

Tech-e-Bytes

CSI-CSAT Technical Magazine

DECEMBER 2019 EDITION

VOLUME IX, ISSUE 1

"We don't do different things, We do things differently"

Our Vision: To become a globally recognized institution that develops professionals with integrity who excel in their chosen domain making a positive impact in industry, research, business and society.

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

VISION OF CSE DEPARTMENT

To acquire global excellence in the field of Computer Science and Engineering, nurturing in professionals, technical competence, innovative skills, professional ethics and social commitment.

MISSION OF CSE DEPARTMENT

- To equip students with a strong foundation in the area of Computer Science and Engineering using effective teaching -learning practices.
- To provide state-of-the-art infrastructure to suit academic, industry and research needs at the global level.
- **To engage students and faculty in interdisciplinary research that promotes innovative ideas for sustainable development.**
- **To incorporate skill enhancement programmes for students and faculty to cope with the contemporary developments in technology.**
- **To inculcate effective communication skills, professional ethics and social commitment among professionals through value added programs.**

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

Graduates of Computer Science & Engineering will

1. Evolve as globally competent computer professionals, researchers and entrepreneurs possessing collaborative and leadership skills, for developing innovative solutions in multidisciplinary domains.
2. Excel as socially committed computer engineers having mutual respect, effective communication skills, high ethical values and empathy for the needs of society.
3. Involve in lifelong learning to foster the sustainable development in the emerging areas of technology.

PROGRAM SPECIFIC OUTCOMES (PSOs)

Student of the Computer Science and Engineering program will:

- **PSO1**: **Professional Skills:** Attain the ability to design and develop hardware and software based systems, evaluate and recognize potential risks and provide creative solutions.
- **PSO2**: **Successful Career and Entrepreneurship:** Gain knowledge in diverse areas of Computer Science and experience an environment conducive in cultivating skills for successful career, entrepreneurship and higher studies.

Editorial

Meet Sophia...

Hanson Robotics' most advanced human-like robot, Sophia, personifies our dreams for the future of AI. As a unique combination of science, engineering, and artistry, Sophia is simultaneously a human-crafted science fiction character depicting the future of AI and robotics, and a platform for advanced robotics and AI research.

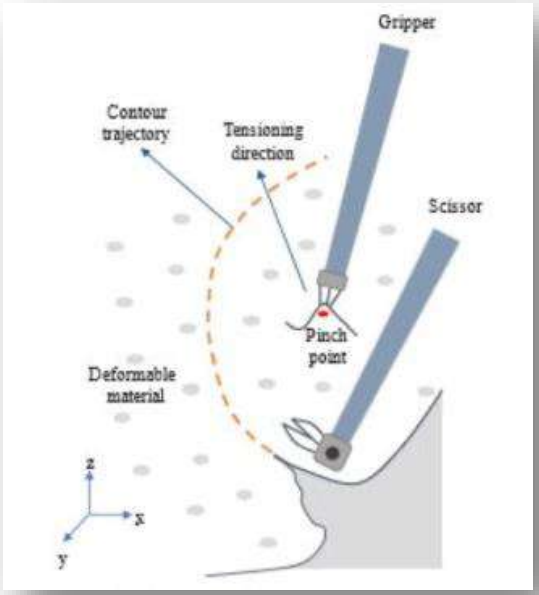
https://www.hansonrobotics.com/sophia/

CONTENTS

- Robotic Surgery; Increased accuracy with deep reinforcement learning
  RIA ELIZABETH JOE | S7 CSE
- Living robots built using frog cells
  RIA SHAJI | S7 CSE
- Artificial intelligence finds disease-related genes
  THARA JOSE | S7 CSE
- Artificial atoms create stable qubits for quantum computing
  NAHAN R N, SAFA V S | S7 CSE
- Storing data in everyday objects
  VARSHA HARI | S7 CSE
- One more thing artificial intelligence can beat you at: Solving a Rubik's cube
  AISWARYA SEN | S7 CSE
- Securing data in IoT using Blockchain
  ABHAY P A | S7 CSE
- Edge Computing
  PRINCE FRANCIS | S7 CSE
- RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning
  ANSA VARKEY | S7 CSE
- Using light to speed up computation
  ASHIKA CHINNU SHABU | S7 CSE

Robotic Surgery; Increased accuracy with deep reinforcement learning

RIA ELIZABETH JOE | S7 CSE



Surgical errors and mistakes injure and kill thousands of patients every year. In fact, a 2016 study concluded that medical errors were the 3rd leading cause of death in the U.S.A alone. Research has been progressing for many years now with the purpose of completely automating surgical procedures. Surgical robots are already an invaluable part of today's operation theaters.

In robotic surgery, manipulation of a deformable sheet, especially cutting through a pre-defined contour trajectory is one of the most critical of tasks. It involves two essential steps: selecting a pinch point and finding how much tension to apply and in which direction (the tensioning policy) from that pinch point. Previous studies considered a single pinch point over the course of cutting, which is only efficient when the contour shape is simple.

For complicated contours, a viable solution is to divide the contour into multiple segments and to find the cutting order among these segments with minimized damage. The use of one pinch point, however, makes it impossible to avoid any damage to the material, especially near the joint areas between segments. To overcome this problem, we add a fixed pinch point in each joint area to avoid distortion. Additionally, if the contour is divided into N segments, we find a set of N different pinch points for cutting each. This method is called Multi-point Deep Reinforcement Learning Tensioning method(MDRLT). The algorithm also finds the best combination of contour segments to cut causing the least damage.

It is clear that the use of fixed pinch points in joint areas is the key to significantly outperform the conventional cutting method with respect to accuracy and reliability.

This approach becomes a normative work-flow to ensure safety in the surgical pattern cutting task.

Reference: Ngoc Duy Nguyen, Thanh Nguyen, Saeid Nahavandi, Asim Bhatti and Glenn Guest, "Manipulating Soft Tissues by Deep Reinforcement Learning for Autonomous Robotic Surgery", arXiv:1902.05183v1 [cs.RO] 14 Feb 2019

Living robots built using frog cells

RIA SHAJI | S7 CSE

People have been manipulating organisms for human benefit since at least the dawn of agriculture, genetic editing is becoming widespread, and a few artificial organisms have been manually assembled in the past few years -- copying the body forms of known animals.

But this research, for the first time ever, "designs completely biological machines from the ground up," the team writes in their new study. With months of processing time on the Deep Green supercomputer cluster at UVM's Vermont Advanced Computing Core, the team -- including lead author and doctoral student Sam Kriegman -- used an evolutionary algorithm to create thousands of candidate designs for the new life-forms.

First they gathered stem cells, harvested from the embryos of African frogs, the species *Xenopus laevis*. (Hence the name "xenobots.") These were separated into single cells and left to incubate. Then, using tiny forceps and an even tinier electrode, the cells were cut and joined under a microscope into a close approximation of the designs specified by the computer.

Assembled into body forms never seen in nature, the cells began to work together. The skin cells formed a more passive architecture, while the once-random contractions of heart muscle cells were put to work creating ordered forward motion as guided by the computer's design, and aided by spontaneous self-organizing patterns -- allowing the robots to move on their own. These reconfigurable organisms

were shown to be able move in a coherent fashion -- and explore their watery environment for days or weeks, powered by embryonic energy stores. Later tests showed that groups of xenobots would move around in circles, pushing pellets into a central location -- spontaneously and collectively. "It's a step toward using computer-designed organisms for intelligent drug delivery," says Bongard, a professor in UVM's Department of Computer Science and Complex Systems Center.

Many technologies are made of steel, concrete or plastic. That can make them strong or flexible. But they also can create ecological and human health problems. "These xenobots are fully biodegradable," say Bongard, "when they're done with their job after seven days, they're just dead skin cells."

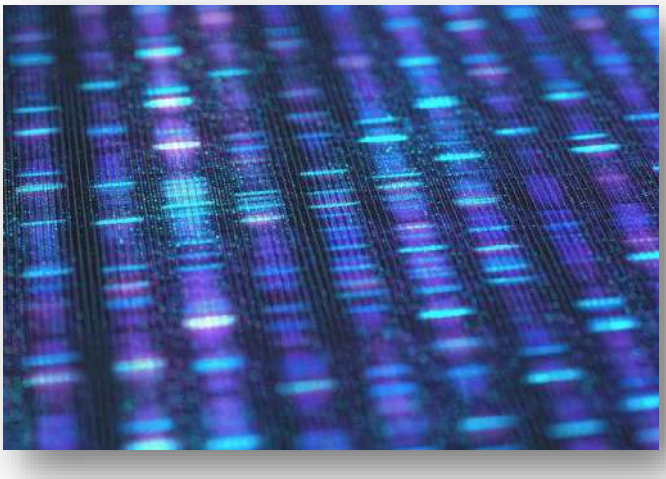
In the new experiments, the scientists cut the xenobots and watched what happened. "We sliced the robot almost in half and it stitches itself back up and keeps going," says Bongard. "And this is something you can't do with typical machines."

Source: University of Vermont

Artificial intelligence finds disease - related genes

THARA JOSE | S7 CSE

It's common when using social media that the platform suggests people whom you may want to add as friends. The suggestion is based on you and the other person having common contacts, which indicates that you may know each other. In a similar manner, scientists are creating maps of biological networks based on how different proteins or genes interact with each other. The researchers behind a new study have used artificial intelligence, AI, to investigate whether it is possible to discover biological networks using deep learning, in which entities known as "artificial neural networks" are trained by experimental data. Since artificial neural networks are excellent at learning how to find patterns in enormous amounts



of complex data, they are used in applications such as image recognition. However, this machine learning method has until now seldom been used in biological research.

"We have for the first time used deep learning to find disease-related genes. This is a very powerful method in the analysis of huge amounts of biological information, or 'big data'," says Sanjiv Dwivedi, postdoc in the Department of Physics, Chemistry and Biology (IFM) at Linköping University.

The scientists used a large database with information about the expression patterns of 20,000 genes in a large number of people. The information was "unsorted," in the sense that the researchers did not give the artificial neural network information about which gene expression patterns were from people with diseases, and which were from healthy people. The AI model was then trained to find patterns of gene expression.

One of the challenges of machine learning is that it is not possible to see exactly how an artificial neural network solves a task. AI is sometimes described as a "black box" -- we see only the information that we put into the box and the result that it produces. We cannot see the steps between. Artificial neural networks consist of several layers in which information is mathematically processed. The network comprises an input layer and an output layer that delivers the result of the information processing carried out by the system. Between these two layers are several hidden layers in which calculations are carried out. When the scientists had trained the artificial neural network, they wondered whether it was possible to, in a manner of speaking, lift the lid of the black box and understand how it works. Are the designs of the neural network and the familiar biological networks similar?

"When we analysed our neural network, it turned out that the first hidden layer represented to a large extent interactions between various proteins. Deeper in the model, in contrast, on the third level, we found groups of different cell types. It's extremely interesting that this type of biologically relevant grouping is automatically produced, given that our network has started from unclassified gene expression data," says Mika Gustafsson, senior lecturer at IFM and leader of the study.

The scientists then investigated whether their model of gene expression could be used to determine which gene expression patterns are associated with disease and which is normal. They confirmed that the model finds relevant patterns that agree well with biological mechanisms in the body. Since the model has been trained using unclassified data, it is possible that the artificial neural network has found totally new patterns. The researchers plan now to investigate whether such, previously unknown patterns, are relevant from a biological perspective.

"We believe that the key to progress in the field is to understand the neural network. This can teach us new things about biological contexts, such as diseases in which many factors interact. And we believe that our method gives models that are easier

to generalise and that can be used for many different types of biological information," says Mika Gustafsson.

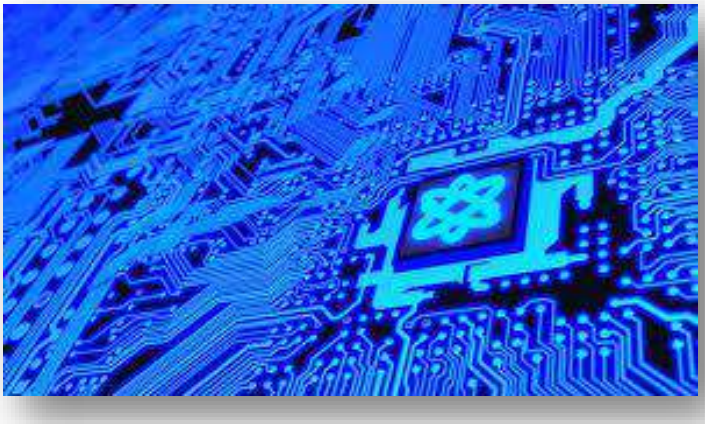
Mika Gustafsson hopes that close collaboration with medical researchers will enable him to apply the method developed in the study in precision medicine. It may be possible, for example, to determine which groups of patients should receive a certain type of medicine, or identify the patients who are most severely affected.

The study has received financial support from the Swedish Foundation for Strategic Research (SSF) and the Swedish Research Council.

Source: Linköping University

Artificial atoms create stable qubits for quantum computing

NAHAN R N, SAFA V S | S7 CSE



In a paper published in the *Nature Communications*, UNSW quantum computing researchers describe how they created artificial atoms in a silicon 'quantum dot', a tiny space in a quantum circuit where electrons are used as qubits (or quantum bits), the basic units of quantum information.

Scientia Professor Andrew Dzurak explains that unlike a real atom, an artificial atom has no nucleus, but it still has shells of electrons whizzing around the centre of the device, rather than around the atom's nucleus.

"The idea of creating artificial atoms using electrons is not new, in fact it was first proposed theoretically in the 1930s and then experimentally demonstrated in the 1990s -- although not in silicon. We first made a rudimentary version of it in silicon back in 2013," says Professor Dzurak, who is an ARC Laureate Fellow and is also director of the Australian National Fabrication Facility at UNSW, where the quantum dot device was manufactured.

"But what really excites us about our latest research is that artificial atoms with a higher number of electrons turn out to be much more robust qubits than previously

thought possible, meaning they can be reliably used for calculations in quantum computers. This is significant because qubits based on just one electron can be very unreliable."

Professor Dzurak and his team from UNSW's School of Electrical Engineering -- including PhD student Ross Leon who is also lead author in the research, and Dr Andre Saraiva -- configured a quantum device in silicon to test the stability of electrons in artificial atoms.

They applied a voltage to the silicon via a metal surface 'gate' electrode to attract spare electrons from the silicon to form the quantum dot, an infinitesimally small space of only around 10 nanometres in diameter.

"As we slowly increased the voltage, we would draw in new electrons, one after another, to form an artificial atom in our quantum dot," says Dr Saraiva, who led the theoretical analysis of the results.

Mr Leon, who ran the experiments, says the researchers were interested in what happened when an extra electron began to populate a new outer shell. In the periodic table, the elements with just one electron in their outer shells include Hydrogen and the metals Lithium, Sodium and Potassium.

"When we create the equivalent of Hydrogen, Lithium and Sodium in the quantum dot, we are basically able to use that lone electron on the outer shell as a qubit," Ross says.

"Up until now, imperfections in silicon devices at the atomic level have disrupted the way qubits behave, leading to unreliable operation and errors. But it seems that the extra electrons in the inner shells act like a 'primer' on the imperfect surface of the quantum dot, smoothing things out and giving stability to the electron in the outer shell."

Achieving stability and control of electrons is a crucial step towards silicon-based quantum computers becoming a reality. Where a classical computer uses 'bits' of information represented by either a 0 or a 1, the qubits in a quantum computer can store values of 0 and 1 simultaneously. This enables a quantum computer to carry out calculations in parallel, rather than one after another as a conventional computer would. The data processing power of a quantum computer then increases exponentially with the number of qubits it has available.

In a continuation of this latest breakthrough, the group will explore how the rules of chemical bonding apply to these new artificial atoms, to create 'artificial molecules'. These will be used to create improved multi-qubit logic gates needed for the realisation of a large-scale silicon quantum computer.

Source: University of New South Wales

Storing data in everyday objects

VARSHA HARI | S7 CSE

Researchers at ETH Zurich have now collaborated with an Israeli scientist to develop a means of storing extensive information in almost any object. "With this method, we can integrate 3D-printing instructions into an object, so that after decades or even centuries, it will be possible to obtain those instructions directly from the object itself," explains Robert Grass, Professor at the Department of Chemistry and Applied Biosciences. The way of storing this information is the same as for living things: in DNA molecules.

Several developments of the past few years have made this advance possible. One of them is Grass's method for marking products with a DNA "barcode" embedded in miniscule glass beads. These nanobeads have various uses; for example, as tracers for geological tests, or as markers for high-quality foodstuffs, thus distinguishing them from counterfeits. The barcode is relatively short: just a 100-bit code (100 places filled with "0"s or "1"s). This technology has now been commercialised by ETH spin-off Haelixa.

At the same time, it has become possible to store enormous data volumes in DNA. Grass's colleague Yaniv Erlich, an Israeli computer scientist, developed a method that theoretically makes it possible to store 215,000 terabytes of data in a single gram of DNA. And Grass himself was able to store an entire music album in DNA -- the equivalent of 15 megabytes of data.

The two scientists have now wedded these inventions into a new form of data storage, as they report in the journal *Nature Biotechnology*. They call the storage form "DNA of Things," a takeoff on the Internet of Things, in which objects are connected with information via the internet.

As a use case, the researchers 3D printed a rabbit out of plastic, which contains the instructions (about 100 kilobytes' worth of data) for printing the object. The researchers achieved this by adding tiny glass beads containing DNA to the plastic. "Just like real rabbits, our rabbit also carries its own blueprint," Grass says.

And just like in biology, this new technological method retains the information over several generations -- a feature the scientists demonstrated by retrieving the printing instructions from a small part of the rabbit and using them to print a whole new one. They were able to repeat this process five times, essentially creating the "great-great-great-grandchild" of the original rabbit.

"All other known forms of storage have a fixed geometry: a hard drive has to look like a hard drive, a CD like a CD. You can't change the form without losing information," Erlich says. "DNA is currently the only data storage medium that can also exist as a liquid, which allows us to insert it into objects of any shape."

A further application of the technology would be to conceal information in everyday objects, a technique experts refer to as steganography. To showcase this application, the scientists turned to history: among the scant documents that attest to life in the Warsaw Ghetto during World War II is a secret archive, which was assembled by a Jewish historian and ghetto resident at that time and hidden from Hitler's troops in milk cans. Today, this archive is listed on UNESCO's Memory of the World Register.

Grass, Erlich and their colleagues used the technology to store a short film about this archive (1.4 megabytes) in glass beads, which they then poured into the lenses of ordinary glasses. "It would be no problem to take a pair of glasses like this through airport security and thus transport information from one place to another undetected," Erlich says. In theory, it should be possible to hide the glass beads in any plastic objects that do not reach too high a temperature during the manufacturing process. Such plastics include epoxides, polyester, polyurethane and silicone.

Furthermore, this technology could be used to mark medications or construction materials such as adhesives or paints. Information about their quality could be stored directly in the medication or material itself, Grass explains. This means medical supervisory authorities could read test results from production quality control directly from the product. And in buildings, for example, workers doing renovations can find out which products from which manufacturers were used in the original structure.

At the moment the method is still relatively expensive. Translating a 3D-printing file like the one stored in the plastic rabbit's DNA costs around 2,000 Swiss francs, Grass says. A large sum of that goes towards synthesising the corresponding DNA molecules. However, the larger the batch size of objects, the lower the unit cost.

Source: ETH Zurich

One more thing artificial intelligence can beat you at: Solving a Rubik's cube

AISWARYA SEN | S7 CSE

Scramble a Rubik's cube, and you will create one of 43 quintillion possible arrangements of those 54 colorful square stickers. But that part—the messing it up part—is easy. Solving it, as any amateur knows, is hard.

People are capable of figuring it out, of course, and doing so astonishingly quickly. The best, like 2019 champion Philipp Weyer, solve it in less than 7 seconds. And generally, the whizzes who specialize in getting the jumbled cube back to sides of pure red, blue, green, white, yellow, and orange, make that happen in around 50 moves.

While humans have been solving these puzzles for decades, it's time for artificial intelligence's turn: AI can now quickly compute a very efficient solution to a scrambled cube. And 60 percent of the time, this AI will calculate a solution that involves the fewest possible moves, which is generally around 20 or so. In fact, there's a concept in the world of the Rubik's cube known as God's algorithm, which would be the way to solve a cube if an all-knowing deity eyeballed it and simply knew how to solve it in the fewest possible moves. "We are close to God's algorithm," says Pierre Baldi, a computer science professor at the University of California, Irvine, and the senior author on a new study describing the Rubik's-Cube-solving bot in the journal *Nature Machine Intelligence.*

Before you start picturing a robot with mechanical fingers manipulating a cube and climbing atop a podium at speedcubing competitions, consider that this AI creation is just software. It solves the cube virtually. In fact, there is a decades-long tradition of

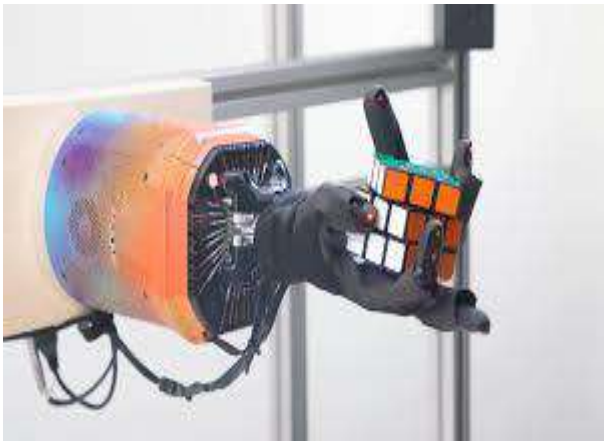
using games as challenges for artificial intelligence systems, and they can already dominate at contests like chess, Go, and multiplayer Texas hold 'em poker.

When it comes to the Erno Rubik's 1974 puzzle, traditional programs could already produce a solution to a scrambled cube using rules-based computing, but the news here is that a type of AI called deep reinforcement learning can now do so.

Since the Rubik's cube is so complex, you can't just expect an AI system to figure it out without training. And just virtually twisting and turning it and trying to solve it randomly definitely doesn't work, either. Instead, the researchers behind the project began with baby steps—a cube that is very close to its solution, and just needed a few moves to complete. They progressed through "scrambles of increasing complexity" while teaching it, Baldi says."It's like a child," he says. "We first give it easy problems, and then progressively harder problems."

So how does this algorithm stack up—how good a speedcuber is it? A version of the Baldi team's algorithm is online and that version takes only around a second to examine a scrambled cube and then produce a solution. Its solution will be significantly less than the 50 moves or so a human typically uses to solve a cube in competition, but it's less likely to produce a solve that's perfectly minimal. Meanwhile, the version of the AI that the researchers report in their paper is more powerful but slightly slower: it can produce the shortest possible solution 60 percent of the time, but the computational delay for that is around 20 seconds long, according to Baldi. Still, that's much, much faster than it would take a human, a cube in their hands, to figure out a solve that involves a minimal number of moves.

In comparison, remember that humans can do this in around 6 seconds, but since they're working in the real world, they have to physically twist and turn it. Speedcubers can actually solve the cube using fewer moves than 50, but the faster method by time is actually for them to not to do in the fewest possible twists.



The cube is an elegant puzzle, because while there are quintillions of different ways to mess it up, and many routes to take to solve it, there's only one destination to get to: the solved cube.Software engineers use games as a framework for building AI algorithms, but also keep an eye on the ways that software that can play games could also be applied to real-world situations. In this case, Baldi says there could be

applications in the field of robotics. For example, he imagines a robot that cleans up your kitchen.

Like the cube, a kitchen can be scrambled, or dirty, in many different ways, but there's just one solved state: a clean cooking space, with everything in its place. Algorithms like the cube-solver could be applied to situations like this one. "If the robot was to move things randomly—take dirty dishes and move them randomly around in the kitchen—the kitchen would never get cleaned," he says. "You [can] see the similarity between certain robotic tasks and what we did."

References

[1] *www.popsci.com/rubiks-cube-solution-artificial-intelligence*

[2] *https://www.theverge.com/2019/10/15/20914575/openai-dactyl-robotic-hand-rubiks-cube-one-handed-solve-dexterity-ai*

Securing data in IoT using Blockchain

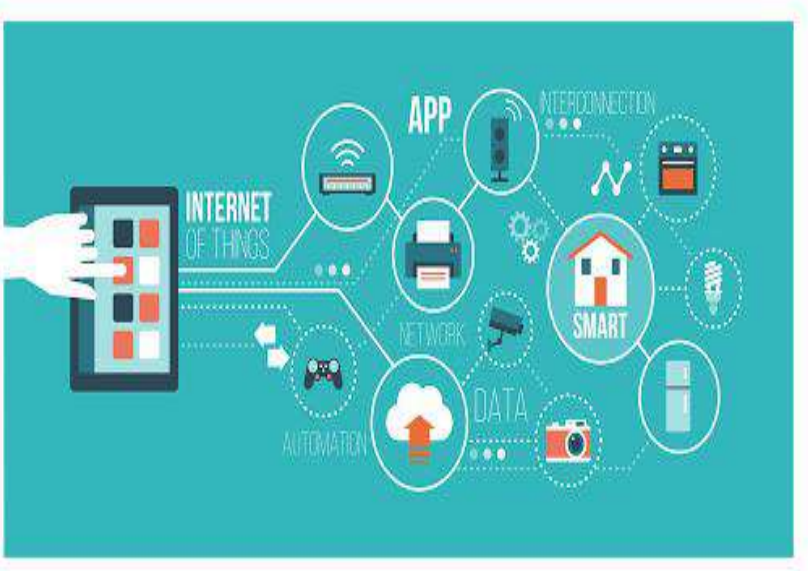
ABHAY P A | S7 CSE

Blockchain technology has seen increasing adoption in recent years. It is appreciated by many people for its role as providing an underlying framework for Bitcoin cryptocurrency and other crypto assets. This has proven to be something that a lot of industries need, and its increased adoption shows a growing realization of that fact.The Internet of Things is all about getting and transmitting large amounts of data through systems and linkages on real-time. Since any business needs privacy and security, the major task here is to ensure the protection of all data and communication.

Now, imagine that data flows across various kinds of integrated solutions and devices, including analytics capabilities, machines, devices, and platforms. Also, the data needs to pass various administrative boundaries, with each having its own set of policies. In this case, it becomes complicated to ensure the safe functioning of an IoT system and the proper management of data.Also, apart from just protecting data, it is important to ensure safe data delivery to the right place, form and time.

Essentially, no matter the way and manner that your company participates in the IoT ecosystem, some nitty-gritty will arise. You will need to deal with some of these IoT security challenges. Now, a good number of companies are pre-occupied with establishing the proper safeguards.The IoT ecosystem as seen currently is one that works on a centralized model. This means that various devices are identified, connected and verified through cloud services that provide high data storage capabilities. Even if these devices are placed two steps from each other, the Internet still serves as a conduit for information passage.

In the centralized model, businesses are made to deal with high infrastructure and maintenance costs of an integrated IoT solution.Also, one important issue to be considered is the number of IoT devices. Just imagine how much costs will increase when it reaches millions of Internet-connected objects. The number of communications will also be increased, which will lead to issues with scalability, economics, and engineering.



In the case that these issues are overcome, another bottleneck that can disrupt the entire network is the issue of cloud services. Hence, providing security for IoT devices will be even more difficult.Essentially, this means that if you choose to apply a centralized model to small-sized IoT solutions, savings can occur. You might not come across problems relating to scalability and maintenance costs. However, large IoT ecosystems will see these associated issues arise and find a way to resolve them. This calls for a decentralized approach.

A blockchain is a distributed ledger that maintains a growing number of data records and transactions. While transactions are related by network participants, they are recorded in blocks. This also ensures that they are arranged in the right sequence and assigns a record timestamp when they become added.Since blockchain technology is decentralized, there is no central authority or specific administrator is necessary.In addition, blockchain technology is based on cryptography algorithms that are designed to ensure the prevention of data distortion and ensure high security.

One of the most important emerging trends is the amalgamation of blockchain technology and the Internet of Things.The decentralization of an IoT network will provide it with the ability to solve a lot of its security challenges. Capabilities of the technology, including trustworthiness, decentralization, scalability, and autonomy, make it a potentially essential component of the overall IoT ecosystem.In the context of the Internet of Things, blockchain technology can be applied to ensure the successful processing of multiple transactions, the tracking, and coordination of millions of smart devices, etc.Essentially, blockchain technology investment by the IoT industry can ensure the proper management of data at various levels.

Also, since blockchain technology is based on cryptography, its integration into IoT network s can provide additional privacy and security. Moreover, blockchain technology gets transactions recorded orderly and carefully. This means that the history of connected devices can be recorded.Add this to the fact that blockchain technology works without the necessity of central authority and you will see that integration possibilities and benefits are truly endless.

References

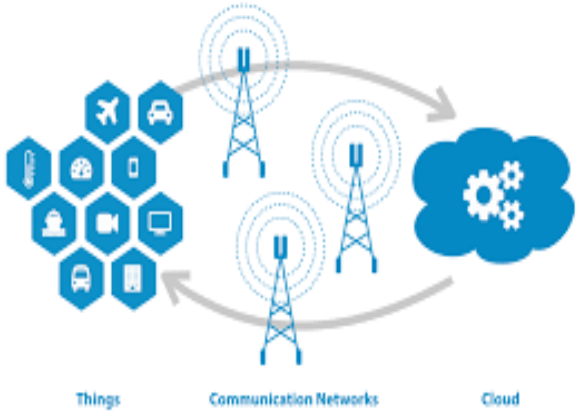
[1] *www.popsci.com/rubiks-cube-solution-artificial-intelligence*

[2]*https://www.theverge.com/2019/10/15/20914575/openai-dactyl-robotic-hand-rubiks-cube-one-handed-solve-dexterity-ai*

Edge Computing

PRINCE FRANCIS | S7 CSE

Edge computing is transforming the way data is being handled, processed, and delivered from millions of devices around the world. The explosive growth of internet-connected devices – the IoT – along with new applications that require real-time computing power, continues to drive edge-computing systems.Faster networking technologies, such as 5G wireless, are allowing for edge computing systems to accelerate the creation or support of real-time applications, such as video processing and analytics, self-driving cars, artificial intelligence and robotics, to name a few.While early goals of edge computing were to address the costs of bandwidth for data traveling long distances because of the growth of IoT-generated data, the rise of real-time applications that need processing at the edge will drive the technology ahead.



Gartner defines edge computing as “a part of a distributed computing topology in which information processing is located close to the edge – where things and people produce or consume that information.”At its basic level, edge computing brings computation and data storage closer to the devices where it’s being gathered, rather than relying on a central location that can be thousands of miles away.

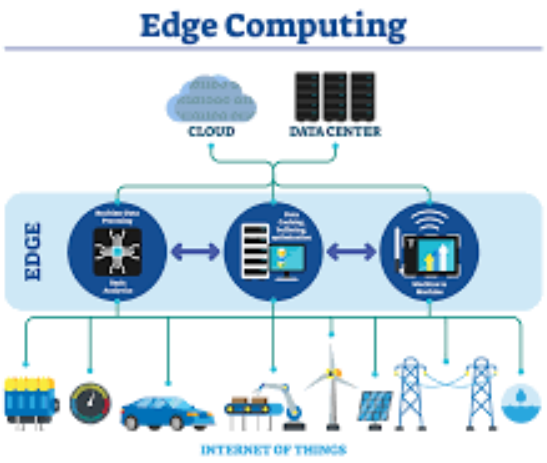
This is done so that data, especially real-time data, does not suffer latency issues that can affect an application’s performance. In addition, companies can save money by having the processing done locally, reducing the amount of data that needs to be processed in a centralized or cloud-based location.

Edge computing was developed due to the exponential growth of IoT devices, which connect to the internet for either receiving information from the cloud or delivering data back to the cloud. And many IoT devices generate enormous amounts of data during the course of their operation. Think about devices that monitor manufacturing equipment on a factory floor, or an internet-connected video camera that sends live footage from a remote office. While a single device producing data can transmit it across a network quite easily, problems arise when the number of devices

transmitting data at the same time grows. Instead of one video camera transmitting live footage, multiply that by hundreds or thousands of devices. Not only will quality suffer due to latency, but the costs in bandwidth can be tremendous.

Edge-computing hardware and services help solve this problem by being a local source of processing and storage for many of these systems. An edge gateway, for example, can process data from an edge device, and then send only the relevant data back through the cloud, reducing bandwidth needs. Or it can send data back to the edge device in the case of real-time application needs.These edge devices can include many different things, such as an IoT sensor, an employee's notebook computer, their latest smartphone, the security camera or even the internet-connected microwave oven in the office break room. Edge gateways themselves are considered edge devices within an edge-computing infrastructure.

For many companies, the cost savings alone can be a driver towards deploying an edge-computing architecture. Companies that embraced the cloud for many of their applications may have discovered that the costs in bandwidth were higher than they expected.



Increasingly, though, the biggest benefit of edge computing is the ability to process and store data faster, enabling for more efficient real-time applications that are critical to companies. Before edge computing, a smartphone scanning a person's face for facial recognition would need to run the facial recognition algorithm through a cloud-based service, which would take a lot of time to process. With an edge computing model, the algorithm could run locally on an edge server or gateway, or even on the smartphone itself, given the increasing power of smartphones. Applications such as virtual and augmented reality, self-driving cars, smart cities and even building-automation systems require fast processing and response.

However, as is the case with many new technologies, solving one problem can create others. From a security standpoint, data at the edge can be troublesome, especially when it's being handled by different devices that might not be as secure as a centralized or cloud-based system. As the number of IoT devices grow, it's imperative that IT understand the potential security issues around these devices, and to make sure those systems can be secured. This includes making sure that data is

encrypted, and that the correct access-control methods and even VPN tunneling is utilized.

Furthermore, differing device requirements for processing power, electricity and network connectivity can have an impact on the reliability of an edge device. This makes redundancy and failover management crucial for devices that process data at the edge to ensure that the data is delivered and processed correctly when a single node goes down.

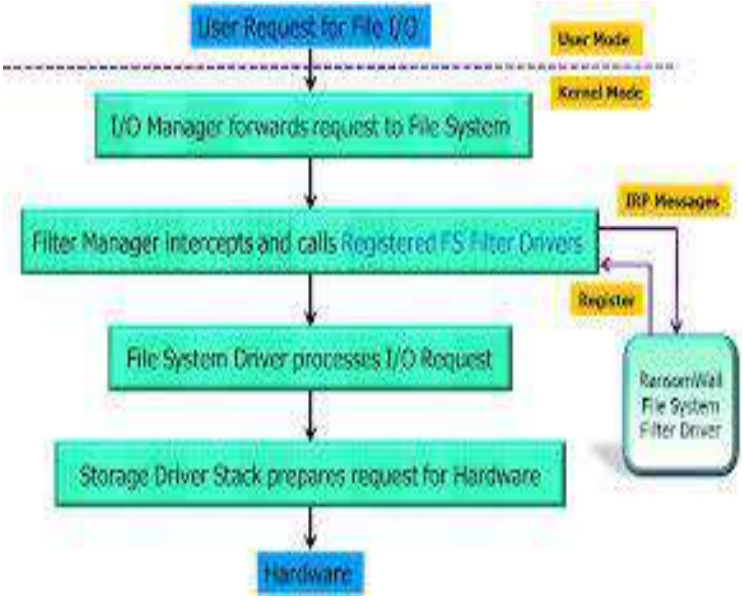
References

[1] *www.hpe.com/in/en/what-is/edge-computing.html*

[2] *www.sdxcentral.com/edge/*

RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning

ANSA VARKEY | S7 CSE

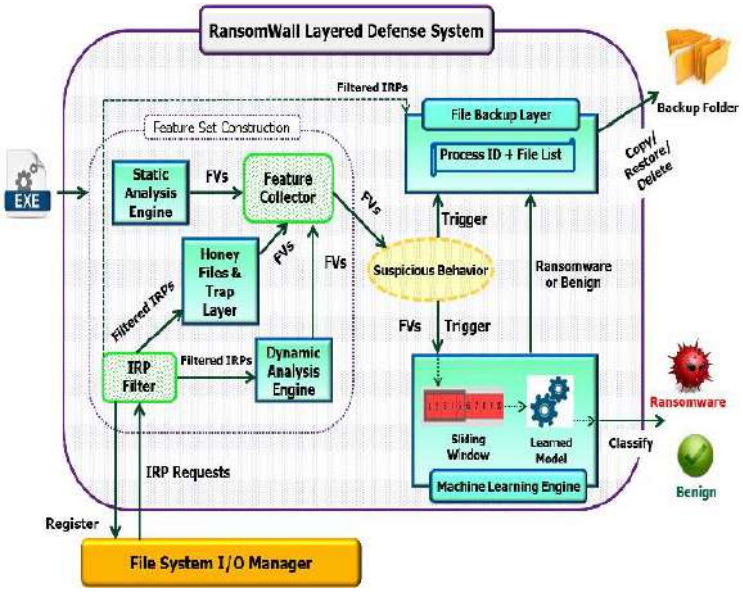


Recent worldwide cybersecurity attacks caused by Cryptographic Ransomware infected systems across countries and organizations , with millions of dollars lost in paying extortion amounts. This form of malicious software takes user files hostage by encrypting them and demands a large ransom payment for providing the decryption key. Signature-based methods employed by Antivirus Software are insufficient to evade Ransomware attacks due to code obfuscation techniques and creation of new polymorphic variants everyday.

Generic Malware Attack vectors are also not robust enough for detection as they do not completely track the specific behavioral patterns shown by Cryptographic

Ransomware families. This work based on analysis of an extensive dataset of Ransomware families presents RansomWall, a layered defense system for protection against Cryptographic Ransomware. It follows a Hybrid approach of combined Static and Dynamic analysis to generate a novel compact set of features that characterizes the Ransomware behavior.

Presence of a Strong Trap Layer helps in early detection. It uses Machine Learning for unearthing zero-day intrusions. When initial layers of RansomWall tag a process for suspicious Ransomware behavior, files modified by the process are backed up for preserving user data until it is classified as Ransomware or Benign. Each RansomWall layer is based on a specific functionality.



The layers are organized in computation order of the features that are generated during the sample's execution . Successful tracking of suspicious Ransomware behavior by an early defense layer results in faster detection. We implemented RansomWall for Microsoft Windows operating system (the most attacked OS by Cryptographic Ransomware) and evaluated it against 574 samples from 12 Cryptographic Ransomware families in real-world user environments.

The testing of RansomWall with various Machine Learning algorithms evaluated to 98.25% detection rate and near-zero false positives with Gradient Tree Boosting Algorithm. It also successfully detected 30 zero-day intrusion samples (having less than 10% detection rate with 60 Security Engines linked to VirusTotal).

References

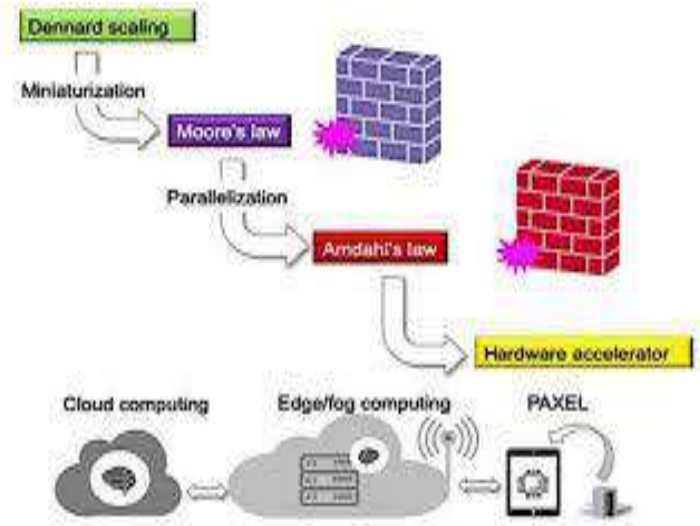
[1] Saiyed Kashif Shaukat , Vinay J. Ribeiro , "*A layered defense system against cryptographic ransomware attacks*", Indian Institute of Technology, Delhi

[2] *jglobal.jst.go.jp/en/detail?JGLOBAL_ID=201802291218190382*

Using light to speed up computation

ASHIKA CHINNU SHABU | S7 CSE

A group of researchers in Japan has developed a new type of processor known as PAXEL, a device that can potentially bypass Moore's Law and increase the speed and efficiency of computing. PAXEL, which stands for photonic accelerator, is placed at the front end of a digital computer and optimized to perform specific functions but with less power consumption than is needed for fully electronic devices.



Metal-oxide semiconductor field-effect transistors are the basis for most integrated electronic circuits, but they are limited by Moore's Law, which says the number of microprocessor chips on a single electronic circuit will double every two years.

There is an inherent limit to this, though, based on the way the size of the microprocessor chips relates to the quantum mechanical nature of electrons.

It is possible to partially overcome the Moore's Law problem by using parallel processing, in which multiple processors carry out simultaneous computations. This approach does not work for every application, however.

In a paper in *APL Photonics*, from AIP Publishing, the researchers looked at another technique to use light for the data transport step in integrated circuits, since photons are not subject to Moore's Law. Instead of integrated electronic circuits, much new development now involves photonic integrated circuits (PICs). The PAXEL accelerator takes this approach and uses power-efficient nanophotonics, which are very small PICs.

Nanophotonics, such as those used in PAXEL, operate at the speed of light and can carry out computations in an analog fashion, with data mapped onto light intensity levels. Multiplications or additions are then performed by varying light intensity. The investigators considered different PAXEL architectures for a variety of uses including artificial neural networks, reservoir computing, pass-gate logic, decision-making and compressed sensing.

One particularly interesting application of PAXEL is in so-called fog computing. This is like cloud computing but uses computational resources (servers) near the "ground" where the originating event occurs. A compact PAXEL attached to a tablet or other hand-held device could detect signals and transmit the information through a 5G wireless link to nearby fog computing resources for data analysis.

Applications of this new technology are expected in a wide array of areas including medical and veterinary point-of-care testing, diagnostics, drug and food testing, and biodefense. As more of our household and business devices are connected through the web, better computing capacity, including data transport with higher energy efficiency, will be needed. Advances such as PAXEL are expected to help meet these needs.

References

[2] *www.sdxcentral.com/edge/*