RISE MAGAZINE

Recent Innovations In Sophisticated Electronics

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

VOLUME 12 | JUL - DEC 2019

INSIDE THIS ISSUE

Vision Mission PEOs and PSOs 1

Block chain technology 2

Artificial intelligence 4

Radio frequency identification 5

Cyber security 6

Solar technology 8

DEPARTMENT VISION
To be identified as a reputed technological department by offering quality education in Electronics and Communication Engineering so as to promote higher learning, research, provide professional career and produce creative solutions to social needs.

DEPARTMENT MISSION	
Mission1 (M1)	To impart quality technical education in Electronics and Communication Engineering with the best pedagogical atmosphere of the highest quality through modern infrastructure and cutting edge skills.
Mission2 (M2)	To promote the establishment of centre of excellence to foster the spirit of innovation and creativeness among faculty and students.
Mission3 (M3)	To develop leadership qualities and also provide ethical and value based education by encouraging operations focused on social needs.

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs) **After successful completion of the program, the graduates can have the ability to**	
PEO1	Be cognizant in basic sciences, fundamental engineering stream along with contemporary problem solving, critical analytical skills in electronics and communication engineering and the allied fields.
PEO2	Understand the issues related to design and development; update the knowledge, and skills through continuous learning in the field of Electronics and Communication Engineering.
PEO3	Demonstrate their technical skills, communication skills and research abilities along with leadership skills in professional environment to empower employability, to go for higher education and to become entrepreneurs.
PEO4	Be motivated with high ethical, human values and team work towards development of the society.

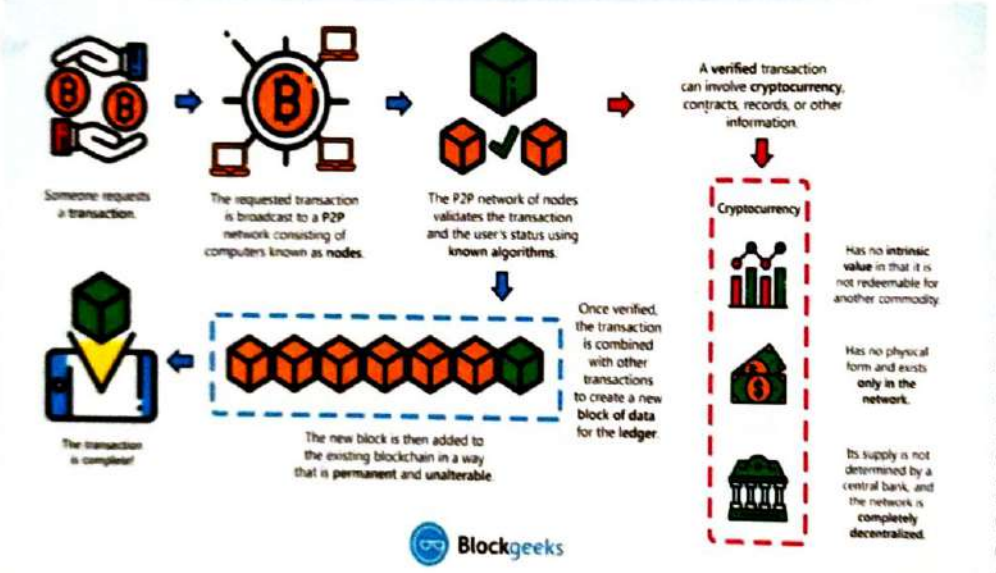
PROGRAMME SPECIFIC OUTCOMES (PSOs) **At the end of the program, the student :**	
PSO1	Able to gain knowledge in diverse areas of electronics and communication for successful career entrepreneurship and higher studies.
PSO2	An ability to make use of acquired technical knowledge in core subjects to analyze and design process for variety of real time application, along with life skills to arrive appropriate solutions.

Block chain technology

The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something greater, and the main question every single person is asking is: What is Blockchain?

By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, (Buy Bitcoin) the tech community has now found other potential uses for the technology.

A blockchain is, in the simplest of terms, a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) is secured and bound to each other using cryptographic principles (i.e. chain).



An infrastructure cost yes, but no transaction cost.) The blockchain is a simple yet ingenious way of passing information from A to B in a fully automated and safe manner. One party to a transaction initiates the process by creating a block. This block is verified by thousands, perhaps millions of computers distributed around the net. The verified block is added to a chain, which is stored across the net, creating not just a unique record, but a unique record with a unique history. Falsifying a single record would mean falsifying the entire chain in millions of instances. That is virtually impossible.

Bitcoin uses this model for monetary transactions, but it can be deployed in many other ways.

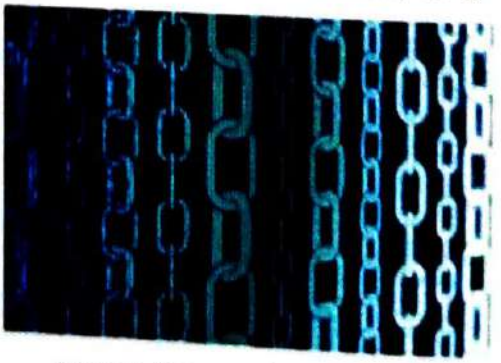
How Does Blockchain Work?

Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.

Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

n The reason why the blockchain has gained so much admiration is that:

- It is not owned by a single entity, hence it is decentralized
- The data is cryptographically stored inside
- The blockchain is immutable, so no one can tamper with the data that is inside the blockchain
- The blockchain is transparent so one can track the data if they want to



The Three Pillars of Blockchain Technology

The three main properties of Blockchain Technology which have helped it gain widespread acclaim are as follows:

- Decentralization
- Transparency
- Immutability

Pillar #1: Decentralization

Before Bitcoin and BitTorrent came along, we were more used to centralized services. The idea is very simple. You have a centralized entity that stored all the data and you'd have to interact solely with this entity to get whatever information you required.

Another example of a centralized system is the banks. They store all your money, and the only way that you can pay someone is by going through the bank.

Pillar #2: Transparency

One of the most interesting and misunderstood concepts in blockchain technology is "transparency." Some people say that blockchain gives you privacy while some say that it is transparent. Why do you think that happens?

Well… a person's identity is hidden via complex cryptography and represented only by their public address. So, if you were to look up a person's transaction history, you will not see "Bob sent 1 BTC" instead you will see "1MF1bhsFLkBzzz9vpFYEmvwT2TbyCt7 NZJ sent 1 BTC". Speaking purely from the point of view of cryptocurrency, if you know the public address of one of these big companies, you can simply pop it in an explorer and look at all the transactions that they have engaged in. This forces them to be honest, something that they have never had to deal with before.

However, that's not the best use-case. We are pretty sure that most of these companies won't transact using cryptocurrencies, and even if they do, they won't do ALL their transactions using cryptocurrencies.

Pillar #3: Immutability

Immutability, in the context of the blockchain, means that once something has been entered into the blockchain, it cannot be tampered with. The use of networks and nodes in cryptocurrencies.

The peer-to-peer network structure in cryptocurrencies is structured according to the consensus mechanism that they are utilizing. , Multi use interference, Space division multiplexing (SDMA), Adaptive SDMA, Increase in range, Multipath mitigation, Decreased inter symbol interference, Best suitability of multi-carrier modulations such as OFDMA and Decreased co-channel interference adjacent

cryptos like Bitcoin and Ethereum which uses a normal proof-of-work consensus mechanism (Ethereum will eventually move on to Proof of Stake), all the nodes have the same privilege. The idea is to create an egalitarian network. The nodes are not given any special privileges, however, their functions and degree of participation may differ. There is no centralized server/entity, nor is there any hierarchy. It is a flat topology.

Who Will Use The Blockchain?

As a web infrastructure, you don't need to know about the blockchain for it to be useful in your life.

Currently, finance offers the strongest use cases for the technology. International remittances, for instance. The World

Bank estimates that over $430 billion US in money transfers were sent in 2015. And at the moment there is a high demand for blockchain developers.

What new business applications will result from this?

#1 Smart contracts

Distributed ledgers enable the coding of simple contracts that will execute when specified conditions are met. Ethereum is an open-source blockchain project that was built specifically to realize this possibility. Still, in its early stages, Ethereum has the potential to leverage the usefulness of blockchains on a truly world-changing scale.

At the technology's current level of development, smart contracts can be programmed to perform simple functions.

For instance, a derivative could be paid out when a financial instrument meets a certain benchmark, with the use of blockchain technology and Bitcoin enabling the payout to be automated.

#2 The sharing economy

With companies like Uber and Airbnb flourishing, the sharing economy is already a proven success. Currently, however, users who want to hail a ride-sharing service have to rely on an intermediary like Uber. By enabling peer-to-peer payments, the blockchain opens the door to direct interaction between parties — a truly decentralized sharing economy results.

An early example, OpenBazaar uses the blockchain to create a peer-to-peer eBay. Download the app onto your computing device, and you can transact with OpenBazzar vendors without paying transaction fees. The "no rules" ethos of the protocol means that personal reputation will be even more important to business interactions than it currently is on eBay.

#3 Crowdfunding

Crowdfunding initiatives like Kickstarter and Gofundme are doing the advance work for the emerging peer-to-peer economy. The popularity of these sites suggests people want to have a direct say in product development. Blockchains take this interest to the next level, potentially creating crowd-sourced venture capital funds.

In 2016, one such experiment, the Ethereum-based DAO (Decentralized Autonomous Organization), raised an astonishing $200 million USD in just over two months. Participants purchased "DAO tokens" allowing them to vote on smart contract venture capital investments (voting power was proportionate to the number of DAO they were holding). A subsequent hack of project funds proved that the project was launched without proper due diligence, with disastrous consequences. Regardless, the DAO experiment suggests the blockchain has the potential to usher in "a new paradigm of economic cooperation." 4 Governance

By making the results fully transparent and publicly accessible, distributed database technology could bring full transparency to elections or any other kind of poll taking. Ethereum-based smart contracts help to automate the process.

The app, Boardroom, enables organizational decision-making to happen on the blockchain. In practice, this means company governance becomes fully transparent and verifiable when managing digital assets, equity or information. 5 Supply chain auditing

Consumers increasingly want to know that the ethical claims companies make about their products are real. Distributed ledgers provide an easy way to certify that the backstories of the things we buy are genuine. Transparency comes with blockchain-based timestamping of a date and location — on ethical diamonds, for instance — that corresponds to a product number. Blockchain, a Provenance pilot project ensures that fish sold in Sushi restaurants in Japan have been sustainably harvested by its suppliers in Indonesia.

Design by
K M V RUCHITHA
(179E1A04C1)

Artificial Intelligence

Artificial intelligence (AI) is wide-ranging branch of computer science concerned with building smart machines capable of performing tasks that typically require human intelligence. AI is an interdisciplinary science with multiple approaches, but advancements in machine learning and deep learning are creating a paradigm shift in virtually every sector of the tech industry.

HOW DOES ARTIFICIAL INTELLIGENCE WORK?

Less than a decade after breaking the Nazi encryption machine Enigma and helping the Allied Forces win World War II, mathematician Alan Turing changed history a second time with a simple question: "Can machines think?"

Turing's paper "Computing Machinery and Intelligence" (1950), and it's subsequent Turing Test, established the fundamental goal and vision of artificial intelligence. At it's core, AI is the branch of computer science that aims to answer Turing's question in the affirmative. It is the endeavor to replicate or simulate human intelligence in machines.

The expansive goal of artificial intelligence has given rise to many questions and debates. So much so, that no singular definition of the field is universally accepted.

The major limitation in defining AI as simply "building machines that are intelligent" is that it doesn't actually explain what artificial intelligence is? What makes a machine intelligent?

In their groundbreaking textbook Artificial Intelligence: A Modern Approach, authors Stuart Russell and Peter Norvig approach the question by unifying their work around the theme of intelligent agents in machines. With this in mind, AI is "the study of agents that receive percepts from the environment and perform actions." (Russel and Norvig viii) Norvig and Russell go on to explore four different approaches that have **Historically defined the field of AI:**

Thinking humanly

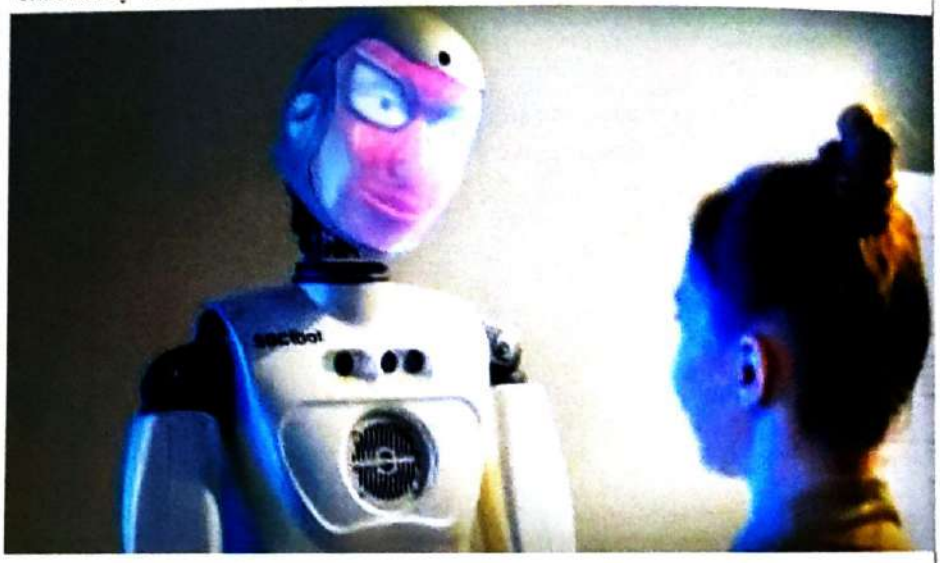
Thinking rationally

Acting humanly

Acting rationally

The first two ideas concern thought processes and reasoning, while the others deal with behavior. Norvig and Russell focus particularly on rational agents that act to achieve the best outcome, noting "all the skills needed for the Turing Test also allow an agent to act rationally." (Russel and Norvig 4).

Patrick Winston, the Ford professor of artificial intelligence and computer science at MIT, defines AI as "algorithms enabled by constraints, exposed by representations that support models targeted at loops that tie thinking, perception and action together."



While these definitions may seem abstract to the average person, they help focus the field as an area of computer science and provide a blueprint for infusing machines and programs with machine learning and other subsets of artificial intelligence.

HOW IS AI USED?

rtificial intelligence generally false under two broad categories:

Narrow AI: Sometimes referred to as "Weak AI," this kind of artificial intelligence operates within a limited context and is a simulation of human intelligence. Narrow AI is often focused on performing a single task extremely well and while these machines may seem intelligent, they are operating under far more constraints and limitations than even the most basic human intelligence.

Artificial General Intelligence (AGI): AGI, sometimes referred to as "Strong AI," is the kind of artificial intelligence we see in the movies, like the robots from Westworld or Data from Star Trek: The Next Generation. AGI is a machine with general intelligence and, much like a human being, it can apply that intelligence to solve any problem. Narrow Artificial Intelligence

Narrow AI is all around us and is easily the most successful realization of artificial intelligence to date. With its focus on performing specific tasks, Narrow AI has experienced numerous breakthroughs in the last decade that have had "significant societal benefits and have contributed to the economic vitality of the nation," according to "Preparing for the Future of Artificial Intelligence," a 2016 report released by the Obama Administration.

Design by
K PAVITHRA
(179E1A0464)

Radio frequency identification

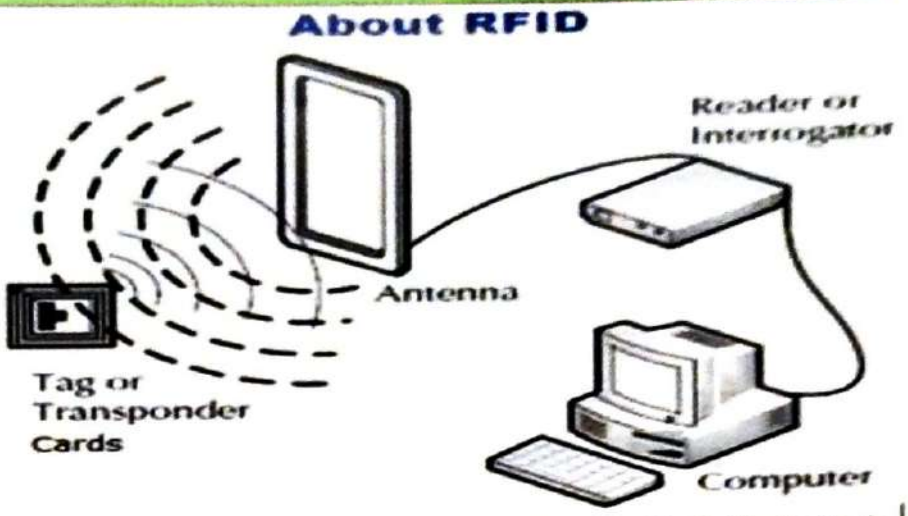
RFID is an acronym for "radio-frequency identification" and refers to a technology whereby digital data encoded in RFID tags or smart labels (defined below) are captured by a reader via radio waves. RFID is similar to barcoding in that data from a tag or label are captured by a device that stores the data in a database. RFID, however, has several advantages over systems that use barcode asset tracking software. The most notable is that RFID tag data can be read outside the line-of-sight, whereas barcodes must be aligned with an optical scanner. If you are considering implementing an RFID solution, take the next step and contact the RFID experts at AB&R® (American Barcode and RFID).

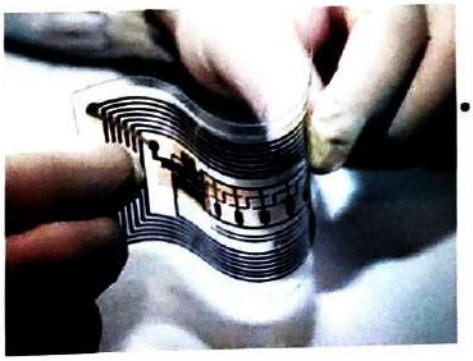
How it does work?

RFID belongs to a group of technologies referred to as Automatic Identification and Data Capture (AIDC). AIDC methods automatically identify objects, collect data about them, and enter those data directly into computer systems with little or no human intervention. RFID methods utilize radio waves to accomplish this. At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader (also called an interrogator). The reader then converts the radio waves to a more usable form of data. Information collected from the tags is then transferred through a communications interface to a host computer system, where the data can be stored in a database and analyzed at a later time.

RFID tags and smart labels

As stated above, an RFID tag consists of an integrated circuit and an antenna. The tag is also composed of a protective material that holds the pieces together and shields them from various environmental conditions. The protective material depends on the application. For example, employee ID badges containing RFID tags are typically made from durable plastic, and the tag is embedded between the layers of plastic. RFID tags come in a variety of shapes and sizes and are either passive or active. Passive tags are the most widely used, as they are smaller and less expensive to implement.





Passive tags must be "powered up" by the RFID reader before they can transmit data. Unlike passive tags, active RFID tags have an onboard power supply (e.g., a battery), thereby enabling them to transmit data at all times. For a more detailed discussion, refer to this article: Passive RFID Tags vs. Active RFID Tags.

Smart labels differ from RFID tags in that they incorporate both RFID and barcode technologies. They're made of an adhesive label embedded with an RFID tag inlay, and they may also feature a barcode and/or other printed information. Smart labels can be encoded and printed on-demand using desktop label printers, whereas programming RFID tags are more time consuming and requires more advanced equipment.

RFID applications

- Although RFID technology has been in use since World War II, the demand for RFID equipment is increasing rapidly, in part due to mandates issued by the U.S. Department of Defense (DoD) and Wal-Mart requiring their suppliers to enable products to be traceable by RFID.
- Whether or not RFID compliance is required, applications that currently use barcode technology are good candidates for upgrading to a system that uses RFID or some combination of the two. RFID offers many advantages over the barcode, particularly the fact that an RFID tag can hold much more data about an item than a barcode can. In addition, RFID tags are not susceptible to the damages that may be incurred by barcode labels, like ripping and smearing.
- From the read distance to the types of tags available, RFID has come a long way since World War II and there is a bright future ahead. Review the evolution of RFID.
- For more information about how RFID works and how to integrate this technology into your business. processessers connecting to a RAS services, through a modem, can limited to accessing only that server, or can be access to the entire network. effectively, this is same as the local connection to the network, except that any type of data transfer runs

Cyber Security

Cybersecurity is the practice of securing networks, systems and any other digital infrastructure from malicious attacks. With cybercrime damages projected to exceed a staggering $6 trillion by 2021, it's no wonder banks, tech companies, hospitals, government agencies and just about every other sector are investing in cybersecurity infrastructure to protect their business practices and the millions of customers that trust them with their data.

What's the best cybersecurity strategy? A strong security infrastructure includes multiple layers of protection dispersed throughout a company's computers, programs and networks. With cyber attacks occurring every 14 seconds, firewalls, antivirus software, anti-spyware software and password management tools must all work in harmony to outwit surprisingly creative cybercriminals. With so much at stake, it's not hyperbolic to think that cybersecurity tools and experts act as the last line of defense between our most vital information and digital chaos.

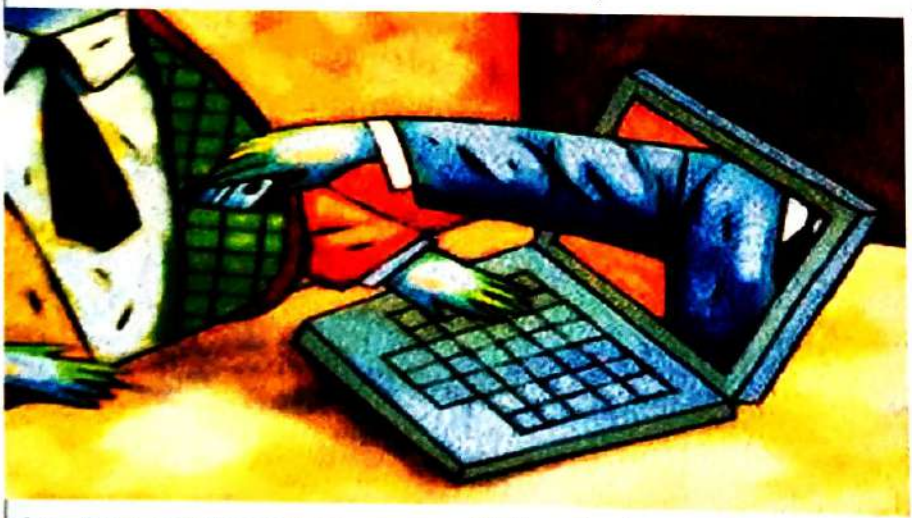
Types of Cyber Attacks:

Cyber attacks come in all shapes and sizes. Some may be overt ransom ware attacks (hijacking important business products or tools in exchange for money to release them), while some are covert operations by which criminals infiltrate a system to gain valuable data only to be discovered months after-the-fact, if at all. Criminals are getting craftier with their malicious deeds and here are some of the basic types of cyber attacks affecting thousands of people each day.

Malware

Malware is used to describe malicious software, including spyware, ransomware and viruses. It usually breaches networks through a vulnerability, like clicking on suspicious email links or installing a risky application. Once inside a network, malware can obtain sensitive information, further produce more harmful software throughout the system and can even block access to vital business network components (ransomware).

Phishing:



Phishing is the practice of sending malicious communications (usually emails) designed to appear from reputable, well-known sources. These emails use the same names, logos, wording, etc., as a CEO or company to dull suspicions and get victims to click on harmful links. Once a phishing link is clicked, cyber criminals have access to sensitive data like credit card, social security or login information.

Social Engineering

Social engineering is the process of psychologically manipulating people into divulging personal information. Phishing is a form of social engineering, where criminals take advantage of people's natural curiosity or trust. An example of more advanced social engineering is with voice manipulation. In this case, cyber criminals take an individual's voice (from sources like a voicemail or social media post) and manipulate it to call friends or relatives and ask for credit card or other personal information.

Man-in-the-Middle Attack

Man-in-the-Middle (MitM) attacks occur when criminals interrupt the traffic between a two-party transaction. For example, criminals can insert themselves between a public Wi-Fi and an individual's device. Without a protected Wi-Fi connection, cyber criminals can sometimes view all of a victim's information without ever being caught.

Zero-day attack

Zero-day attacks are becoming more-and-more common. Essentially, these attacks occur between a network vulnerability announcement and a patch solution. In the name of transparency and security, most companies will announce that they found a problem with their network safety, but some criminals will take this opportunity to unleash attacks before the company can come up with a security patch.

CYBERSECURITY IN BANKING AND FINANCIAL SERVICES

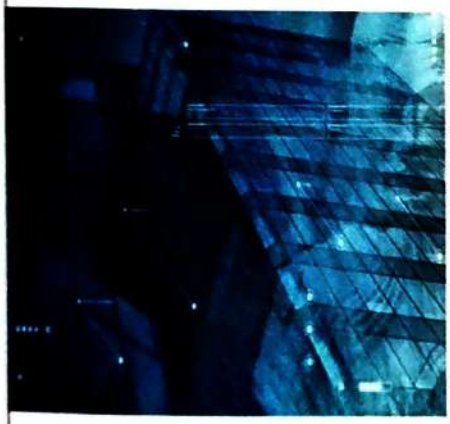
The financial sector invests heavily in cybersecurity — after the Equifax hack, it's only logical — but it's not an early adopter of new technologies. In banking and financial services the Cloud, especially, has been met with skepticism. In addition to being upsetting, financial sector breaches can be wildly expensive. The wireless communication and networking on a large scale is carried out through satellites. g are on their way to destroy the whole system of satellites and space stations orbiting around our globe in the near future. This deadly debris must be eliminated in order to have a

Heavily regulated offline and on, financial institutions must comply with more than 800 cybersecurity laws and standards — and Microsoft has helpfully compiled all of them into a free Universal Compliance Framework. The company also offers detailed maps of how these required controls can be activated in Azure, and how they integrate with typical banking workloads. Azure also comes with built-in finance-friendly security features, like AI that crawls real-time activity logs for signs of fraud.

Force point

Forcepoint's security platform constantly weighs security against convenience by

calculating constant real-time risk scores for each user to carefully distinguish accidental flubs from suspicious behavior. The lowest-risk users then face fewer authentication hurdles in the Forcepoint system, while higher-risk users — potential hackers or internal threats — are flagged. This user-centric



system protects on-premise and Cloud-based data centers equally well. It can also scan webs of disparate endpoints, including computers and phones, for trouble.

Proof Point

Proofpoint offers protection against some of the fringe digital threats faced by financial institutions and other prime hacker targets. The software safeguards of enterprise social media accounts (which can be used to phish customers, among other things) and screens attempted hacker invasions via social engineering. The platform even protects against non-compliance threats using ultra-modern archiving features that ensure banks neither lose nor delete data that must legally be on hand.

Fire Eye

FireEye's consultants patch vulnerabilities by custom-fitting the company's security platform, Helix, into existing bank security systems. Though heavily regulated, financial sector companies often have digital vulnerabilities. Routine mergers and acquisitions, for example, create various gaps in threat coverage. Helix offers a versatile fix, with features like malware communication tracking — which comes in handy at Citizens National Bank of Texas, where Helix sits between the enterprise firewall and the Wild West of the internet, blocking threats that might otherwise leak through.

Check Point

Check Point's comprehensive architecture secures on-premise data warehouses mobile devices like phones and laptops, even global networks of ATMs. It's designed to ward off persistent attacks, whether targeted phishing campaigns or swarming bots. And it does so while hewing to federal and local regulations and prioritizing macro-scale efficiency.

CLOUD MIGRATION?

In the near future, McIntosh said, financial institutions will cautiously migrate to the Cloud. Though the industry faces high-tech threats, it's never been known for early adoption. Financial data is too sensitive for true experimentation, McIntosh explained, and off-premise cloud storage is "a big paradigm shift" for the field.

"The old security mentality was: I've got a building and then I'm going to put some walls around it and I put up a moat and a drawbridge and all these perimeters and defenses," she said.

In other words, it was all about on-premise data storage. The notion of entrusting sensitive information to outside servers banks can't directly manage raises security question, which McIntosh ponders daily. Potential solutions include virtual firewalls and encrypted Cloud storage — but it's unclear what's right for banking.

"We're not just going and buying the latest, greatest thing," McIntosh said of infosec professionals in the finance sector. "[We're] very strategic."

The same goes for machine learning solutions, though McIntosh sees potential applications in banking — especially in fraud protection.

"If you think of the amount of raw data that [our systems] ingest on a daily basis… [it's] thousands and thousands of events per second. Humans cannot make sense of all that data," she said. "In the next couple of years I think that we're going to have better algorithms to analyze that data."

But it's a slow process. Machine learning algorithms must be trained to read cues the way human security officers do, and they need to be integrated into ultra-secure software. McIntosh has yet to come across the right machine learning product for her bank.

"A college degree isn't a prerequisite to do a lot of the things that are in IT," McIntosh explained. "There are high school kids who can probably hack things more effectively than some

professionals."

The bootcamp, she thinks, can "tune up" some of that organic talent that might not flock to university campuses.

Design by

TIRAKALVA UDAYAPRIYA
(179E1A04L4)

Solar Technology

Solar energy works by capturing the sun's energy and turning it into electricity for your home or business.

Our sun is a natural nuclear reactor. It releases tiny packets of energy called photons, which travel the 93 million miles from the sun to Earth in about 8.5 minutes. Every hour, enough photons impact our planet to generate enough solar energy to theoretically satisfy global energy needs for an entire year.

Currently photovoltaic power accounts for only five-tenths of one percent of the energy consumed in the United States. But solar technology is improving and the cost of going solar is dropping rapidly, so our ability to harness the sun's abundance of energy is on the rise.

A 2017 report from the International Energy Agency shows that solar has become the world's fastest-growing source of power – marking the first time that solar energy's growth has surpassed that of all other fuels. In the coming years, we will all be enjoying the benefits of solar-generated electricity in one way or another.

How Do Solar Panels Work?

When photons hit a solar cell, they knock electrons loose from their atoms. If conductors are attached to the positive and negative sides of a cell, it forms an electrical circuit. When electrons flow through such a circuit, they generate electricity. Multiple cells make up a solar panel, and multiple panels (modules) can be wired together to form a solar array. The more panels you can deploy, the more energy you can expect to generate.

What are Solar Panels Made of?

Photovoltaic (PV) solar panels are made up of many solar cells. Solar cells are made of silicon, like semiconductors. They are constructed with a positive layer and a negative layer, which together create an electric field, just like in a battery.

How Do Solar Panels Generate Electricity?

PV solar panels generate direct current (DC) electricity. With DC electricity, electrons flow in one direction around a circuit. This example shows a battery powering a light bulb. The electrons move from the negative side of the battery, through the lamp, and return to the positive side of the battery.

With AC (alternating current) electricity, electrons are pushed and pulled, periodically reversing direction, much like the cylinder of a car's engine. Generators create AC electricity when a coil of wire is spun next to a magnet. Many different energy sources can "turn the handle" of this generator, such as gas or diesel fuel, hydroelectricity, nuclear, coal, wind, or solar.

AC electricity was chosen for the U.S. electrical power grid, primarily because it is less expensive to transmit over long distances. However, solar panels create DC electricity. How do we get DC electricity into the AC grid? We use an inverter.

What Does a Solar Inverter Do?

A solar inverter takes the DC electricity from the solar array and uses that to create AC electricity. Inverters are like the brains of the system. Along with inverting DC to AC power, they also provide ground fault protection and system stats, including voltage and current on AC and DC circuits, energy production and maximum power point tracking.

Central inverters have dominated the solar industry since the beginning. The introduction of micro-inverters is one of the biggest technology shifts in the PV industry. Micro-inverters optimize for each individual solar panel, not for an entire solar system, as central inverters do. This enables every solar panel to perform at maximum potential. When a central inverter is used, having a problem on one solar panel (maybe it's in the shade or has gotten dirty) can drag down the performance of the entire solar array. Micro-inverters, such as the ones in SunPower's Equinox home solar system, make this a non-issue. If one solar panel has an issue, the rest of the solar array still performs efficiently.

How Does a Solar Panel System Work?

Here's an example of how a home solar energy installation works. First, sunlight hits a solar panel on the roof. The panels convert the energy to DC current, which flows to an inverter. The inverter converts the electricity from DC to AC, which you can then use to power your home. It's beautifully simple and clean, and it's getting more efficient and affordable all the time.

However, what happens if you're not home to use the electricity your solar panels are generating every sunny day? And what happens at night when your solar system is not generating power in real time? Don't worry, you still benefit through a system called "net metering."

A typical grid-tied PV system, during peak daylight hours, frequently produces more energy than one customer needs, so that excess energy is fed back into the grid for use elsewhere.

Design by

P. Krupa

(179E1A04F1)