JYOTI NIVAS COLLEGE
POST GRADUATE CENTRE

DEPARTMENTOFMCA

I YEAR

TECH-ON-TOP

E-JOURNAL

ON

CLOUD SECURITY

SANDHYA.M(20MCA32)
SUDAGANI SAI SARIKA(20MCA34)

INTRODUCTION:

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections. Cloud security is a form of cybersecurity.

- Cloud security refers broadly to measures undertaken to protect digital assets and data stored online via cloud services providers.
- Cloud computing is the delivery of different services through the Internet, including data storage, servers, databases, networking, and software.
- Measures to protect this data include two-factor authorization (2FA), the use of VPNs, security tokens, data encryption, and firewall services, among others.

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. Cloud computing is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security.

Cloud security is essential for the many users who are concerned about the safety of the data they store in the cloud. They believe their data is safer on their own local servers where they feel they have more control over the data. But data stored in the cloud may be more secure because cloud service providers have superior security measures, and their employees are security experts. On-premise data can be more vulnerable to security breaches, depending on the type of attack. Social engineering and malware can make any data storage system vulnerable, but on-site data may be more vulnerable since its guardians are less experienced in detecting security threats.

SECURITY CONCERNS

Cloud security is a key concern for cloud storage providers. They not only must satisfy their customers; they also must follow certain regulatory requirements for storing sensitive data such as credit card numbers and health information. Third-party audits of a cloud provider’s security systems and procedures help ensure that users’ data is safe.

Major threats to cloud security include data breaches, data loss, account hijacking, service traffic hijacking, insecure application program interfaces (APIs), poor choice of cloud storage providers, and shared technology that can compromise cloud security.

Distributed denial of service (DDoS) attacks are another threat to cloud security. These attacks shut down a service by overwhelming it with data so that users cannot access their accounts, such as bank accounts or email accounts.

Maintaining the security of data in the cloud extends beyond securing the cloud itself. Cloud users must protect access to the cloud that can be gained from data stored on mobile devices or carelessness with login credentials. Another cloud security issue is that data stored on a cloud-hosted in another country may be subject to different regulations and privacy measures.

When choosing a cloud provider, it is important to choose a company that tries to protect against malicious insiders through background checks and security clearances. Most people think outside hackers are the biggest threat to cloud security, but employees present just as large of a risk. These employees are not necessarily malicious insiders; they are often employees who unknowingly make mistakes such as using a personal smartphone to access sensitive company data without the security of the company's own network.

A major benefit of the cloud is that it centralizes applications and data and centralizes the security of those applications and data as well. Eliminating the need for dedicated hardware also reduces organizations' cost and management needs, while increasing reliability, scalability and flexibility.

REFERENCES:

www.investopedia.com
Searchcloudsecurity.techtarget.com

ALL ABOUT CRYPTOCURRENCY

BHOOMIKA S (20MCA06)

HERMAIN K S (20MCA15)

WHAT IS CRYPTOCURRENCY?

A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation.

According to Jan Lansky, a cryptocurrency is a system that meets six conditions:

1. The system does not require a central authority, its state is maintained through distributed consensus.
2. The system keeps an overview of cryptocurrency units and their ownership.
3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
4. Ownership of cryptocurrency units can be proved exclusively cryptographically.
5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

UNDERSTANDING BLOCKCHAIN

A **blockchain** is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. The timestamp proves that the transaction data existed when the block was published in order to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it.

BLOCKS

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking

the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the initial block, which is known as the **genesis block**.

MINING

In cryptocurrency networks, *mining* is a validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward. The reward decreases transaction fees by creating a complementary incentive to contribute to the processing power of the network. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines such as FPGAs and ASICs running complex hashing algorithms like SHA-256 and scrypt This arms race for cheaper-yet-efficient machines has existed since the day the first cryptocurrency, bitcoin, was introduced in 2009.

ADVANTAGES

Cryptocurrencies hold the promise of making it easier to transfer funds directly between two parties, without the need for a trusted third party like a bank or credit card company. These transfers are instead secured by the use of public keys and private keys and different forms of incentive systems, like Proof of Work or Proof of Stake.

In modern cryptocurrency systems, a user's "wallet," or account address, has a public key, while the private key is known only to the owner and is used to sign transactions. Fund transfers are completed with minimal processing fees, allowing users to avoid the steep fees charged by banks and financial institutions for wire transfers.

DISADVANTAGES

The semi-anonymous nature of cryptocurrency transactions makes them well-suited for a host of illegal activities, such as money laundering and tax evasion. However, cryptocurrency advocates often highly value their anonymity, citing benefits of privacy like protection for whistle-blowers or activists living under repressive governments. Some cryptocurrencies are more private than others.

Bitcoin, for instance, is a relatively poor choice for conducting illegal business online, since the forensic analysis of the Bitcoin blockchain has helped authorities arrest and prosecute criminals. More privacy-oriented coins do exist, however, such as Dash, Monero, or ZCash, which are far more difficult to trace.

REFERENCES

https://www.investopedia.com

https://en.wikipedia.org

GOOGLE OPTICAL DISPLAY

EMILIN MERIA JAMES (20MCA10)

NEHA SREESHKUMAR (20MCA25)

ABSTRACT

Google implemented an optical display device called Google glass. Google glass is an upcoming gadget with an optical head mount display (OHMD) which for been developed by Google, lead the whole world through a Google's android operating system and also uses other techniques such as 4G, eye tap, smart clothing,smart grid.

1. INTRODUCTION

Google glass is a computer that includes an optical display with a head mount, touch sensitive pad, a camera and a speaker is compared to a smartphone.This glass is used for hands free and works on natural language with voice commands; hence it helps all kinds of users like handicapped / disabled. It is an eye glass which replaces the lens with head-up display.

Project Glass: Project Glass is a research development program done by Google to develop an augmented reality head-mounted display (HMD). The main view of Project Glass products is the hands free display of information that are currently available for most smart phone users, and allows interaction with the Internet by natural language voice commands.

Virtual reality (VR): Virtual reality creates an entire virtual world. In this type, it is hard to differentiate real world and artificial world. User may not know which is real and which is not real. This is generally achieved by wearing a helmet or goggles.

Augmented reality (AR): Augmented reality is a mix of real world and virtual world.in this type of reality, the user is able to differentiate between real and artificial world. User can communicate with both the worlds. This is generally achieved by holding a smartphone in front of you.

2. TECHNOLOGIES USED

2.1 Wearable Computing: Wearable computers are the electronic devices that are worn by the user under, or on top of clothing.The main featuresof this is, easy to use, long battery life etc... It allows a stable interaction between the computer and user.

2.2 Ambient Intelligence: Ambient Intelligence (AmI) has an electronic environment, which is more sensitive and responsive to the presence of people. It aims to enhance the way people interact with their environment (and it will promote safety and to enrich their lives).

2.3 Smart Clothing: Smart clothing is the new type of clothing in the current generation.The clothing is made with new signal-transfer fabric technology installed with digital devices.

2.4 Eye-Tap Technology: Eye Tap is a device that is worn in front of the eye and this acts as a camera to record the scene and also to display the computer generated imagery of the original scene.

2.5 Smart Grid Technology: An electrical grid that uses some technology to gather and act on information, such as information about the behaviours of producers and customers, to improve the efficiency, reliability, and sustainability of the production and distribution of electricity is called as smart grid.

2.6 4G Technology: 4G is the fourth generation of mobilephone communication standard. It provides mobile internet access with data rates of 300Mbps in mobility to 1Gbps.

2.7Android Operating System: Android is a Linux-based operating system. It is developed by Google.Google has also made an open source operating system called open source Android and it is released under the Apache License.

3. ADVANTAGES AND DISADVANTAGES:

3.1 Advantages:

- Easy to wear, use and it is a new trend for fashion lovers.
- Provides faster access of calls,maps, videos, chats.
- Helpful for handicapped and disabled people.

3.2 Disadvantages:

- It can be easily broken or damaged.
- Users wearing spectacles won't be able to wear Glass.
- Privacy may be violated with Glass.

4.CONCLUSION

Google glasses are wearable computers which use the familiar communicationtechnologies for the physically challenged class of people who cannot use palmtops and mobiles.

5.REFERENCES

- Thad Starner, "Project Glass: An Extension of the Self", PERVASIVE computing, Editor: Bernt Schiele,15361268/13/$31.00 © 2013 IEEE , Page No.-14-16, Published by the IEEE CS, April–June 2013
- http://www.google.com/glass/start/
- http://en.wikipedia.org/wiki/Project_Glass
- http://en.wikipedia.org/wiki/Virtual_reality
- http://en.wikipedia.org/wiki/Augmented_reality
- http://en.wikipedia.org/wiki/Head-mounted_display
- http://en.wikipedia.org/wiki/EyeTap
- http://en.wikipedia.org/wiki/Android_(operating_system)
- http://www.youtube.com/watch?v=9c6W4CCU9M4

EDGE ARTIFICIAL INTELLIGENCE

SHARMILA S(20MCA33)

THANUJA C(20MCA40)

INTRODUCTION

The Prominent technology trend for the year 2021 – Edge Artificial Intelligence or you can say the future of Artificial Intelligence! What it simply means is in Edge Artificial Intelligence, the AI algorithms are processed at the local level i.e., Edge AI takes and processed the data to the nearest point of user interaction whether it be a computer or an Edge server, or any other device. Amazon Alexa, Google Maps, Drones, etc. are some of the common examples that are supported by the Edge AI. By integrating Edge Artificial Intelligence, businesses can reduce costs and latency times, can enhance the security level through local data processing, can preserve the bandwidth, and much more that subsequently will also help in building great customer experiences. As per the reports, the Edge AI market is expected to reach around $1.12 trillion by the year 2023. However, it won't be wrong to say too that Edge is replacing the cloud but it should be taken in another way as Edge technology will provide new additional possibilities and tech advancements in the coming years.

THE FUTURE OF ARTIFICIAL INTELLIGENCE IS ON THE EDGE

Edge AI is a system that uses Machine Learning algorithms to process data generated by a hardware device at the local level. The device does not need to be connected to the Internet to process such data and make decisions in real time, in a matter of milliseconds. This considerably reduces the communication costs derived from the cloud model. In other words, Edge AI takes the data and its processing to the closest point of interaction with the user, whether it is a computer, an IoT device or an Edge server.

An example of this technology can be seen in the speakers of Google, Alexa or the Apple Homepod, which have learned words and phrases through Machine Learning and then stored them locally on the device. When the user communicates something to applications such as Siri or Google, they send the voice recording to an Edge network where it is passed to text via AI and a response is processed. Without an Edge network the response time would be seconds, with Edge the times are reduced to less than 400 milliseconds.

MARKET VALUE OF EDGE AI (IN MILLION $)

BENEFITS OF EDGE AI

- Reduces costs and latency times for an improved user experience This facilitates the integration of wearable technologies focused on the user experience, where you interact in real time to make payments, or where bracelets monitor your exercise and sleep patterns.
- It increases the level of security in terms of data privacy through local processing. Data is no longer shared in a centralized cloud.
- Technically, the reduction in required bandwidth should lead to a reduction in the costs of the contracted internet service.
- Edge technology devices do not require specialized maintenance by data scientists or AI developers. The graphic data flows are automatically delivered for monitoring, therefore, it is an autonomous technology.

WHY IS EDGE AI IMPORTANT?

On the other hand, the list of Edge AI applications is long. Current examples include facial recognition and real-time traffic updates on smartphones, as well as semi-autonomous vehicles or smart devices. Other Edge AI-enabled devices include video games, smart speakers, robots, drones, security cameras, and wearable health monitoring devices.

- It will reduce costs and improve safety in terms of industrial IoT (IIoT). The AI will monitor machinery for possible defects or errors in the production chain, while the Machine Learning will recompile data in real time of the whole process.
- It will be used for the analysis of medical images in emergency medical care.
- The autonomous vehicles will increase their capacity to process data and images in real time for the detection of traffic signs, pedestrians, other vehicles, and roads, improving the levels of security in transportation.
- It will be possible to use it in image and video analysis, to generate responses to audio-visual stimuli, or for real-time recognition of scenes and spaces, for example, in smartphones.

CONCLUSION

Large companies like Amazon and Google have been investing millions in the development of their Edge AI systems, so the only way to stay competitive is to take a lead and invest in these technologies. On the other hand, the increase in demand for IoT devices will facilitate the adoption of 5G networks and Edge Computing itself.

REFERENCES

- https://www.vectoritcgroup.com/en/tech-magazine-en/artificial-intelligence-en/edge-ai-el-futuro-de-la-inteligencia-artificial/
- https://www.geeksforgeeks.org/top-10-emerging-technology-trends-to-watch-in-2021/

MULTI-CLOUD

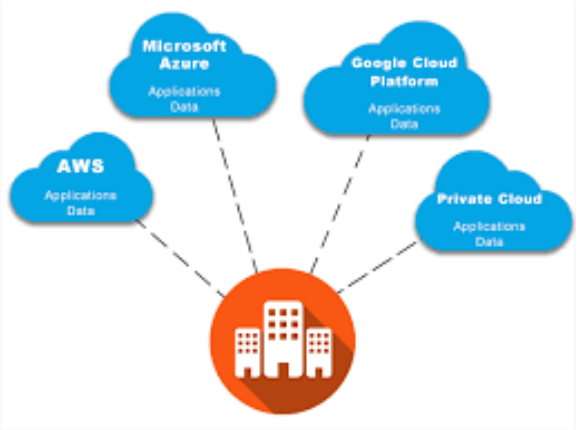
M KOMAL SINGH(20MCA20)

SUSHEELA R(20MCA36)

INTRODUCTION:

Multi-cloud (also multi-cloud or multi cloud) is the use of multiple cloud computing and storage services in a single network architecture.

A multi-cloud environment could be all-private, all-public or a combination of both. Companies use multi-cloud environments to distribute computing resources and minimize the risk of downtime and data loss. They can also increase the computing power and storage available to a business.



This refers to the distribution of cloud assets, software, applications, and more across several cloud environments. With a typical multi-cloud architecture utilizing two or more public clouds as well as private clouds, a multi-cloud environment aims to eliminate the reliance on any single cloud provider or instance.

A multi-cloud strategy allows companies to select different cloud services from different providers because some are better for certain tasks than others. For example, some cloud platforms specialize in large data transfers or have integrated machine learning capabilities. Organizations implement a multi-cloud environment for the following reasons:

• **Choice:** The additional choice of multiple cloud environments gives you flexibility and the ability to avoid vendor lock-in.

• **Disaster Avoidance:** Outages happen; sometimes it is due to a disaster; other times it is due to human error. Having multiple cloud environments ensures that you always have compute resources and data storage available so you can avoid downtime.

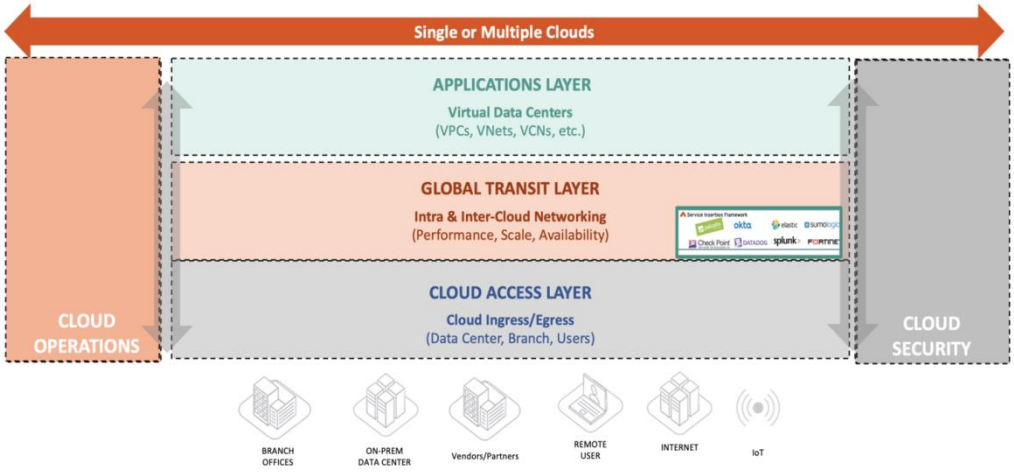
• **Compliance:** Many multi-cloud environments can help enterprises achieve their goals for governance, risk management and compliance regulations.

WHAT ARE THE BENEFITS OF MULTI-CLOUD?

A multi-cloud platform combines the best services that each platform offers. This allows companies to customize an infrastructure that is specific to their business goals. A multi-cloud architecture also provides lower risk. If one web service host fails, a business can continue to operate with other platforms in a multi-cloud environment versus storing all data in one place.

MULTI CLOUD NETWORK ARCHITECTURE

MCNA architecture defines four distinct layers at a high level. These are Cloud Core, Cloud Security, Cloud Access, and Cloud Operations.



REFERENCES:

- https://avinetworks.com/glossary/multi-cloud/
- https://community.aviatrix.com/t/h7h3sta/what-is-a-multi-cloud-network-architecture-mcna-and-how-can-it-help-enterprises

HYBRID CLOUD

POOJA C(20MCA07)

INTRODUCTION:

Hybrid cloud is a solution that combines a private cloud with one or more public cloud services, with proprietary software enabling communication between each distinct service. A hybrid cloud strategy provides businesses with greater flexibility by moving workloads between cloud solutions as needs and costs fluctuate.Hybrid cloud services are powerful because they give businesses greater control over their private data. An organization can store sensitive data on a private cloud or local data centre and simultaneously leverage the robust computational resources of a managed public cloud. A hybrid cloud relies on a single plane of management, unlike a multi-cloud strategy wherein admin must manage each cloud environment separately.

FUTURE OF HYBRID CLOUD:

Hybrid cloud is already having a positive impact on their despite the consensus that hybrid cloud is the IT operations model of the future, the report also found that escaping from the traditional data centre will take time. The demand of hybrid cloud is increasing every year. According to analytical agency Gartner, the global market for public cloud services will reach $308.5 billion in 2021 this is $ 40 billion more then in 2020 and 90 billion more then 2019.

MARKET VALUE OF HYBRID CLOUD:

Hybrid cloud market size worldwide 2020-2026 In 2020,the global hybrid cloud market was valued at 52 billion U.S dollars and is expected to reach 145 billion U.S dollars in 2026

HYBRID CLOUD BENEFITS:

The benefits of a hybrid cloud strategy stem from the solution's ability to give IT leaders increased control over their data. Essentially, the hybrid model provides the business with multiple options so that stakeholders can pick an environment that best suits each individual use case. Most businesses do not utilize the same level of computation power every day. In fact, an organization may find that its resource needs only balloon during one specific time of year. For instance, a health insurance application may need double the computing power during open enrolment. Rather than paying for those additional resources to sit idle for most of the year, an organization can save on costs by extending their private resources to a public cloud only when necessary. A hybrid model requires much less space on-premises compared to a strictly private model. A business can deploy a private network on-site to handle internal needs, then automatically extend to the private cloud when computational resources exceed local availability. This model can benefit startups that can't afford to invest in a huge private data centre as well as established enterprises that need to scale in a cost effective manner.

WHY HYBRID CLOUD IS IMPORTANT:

The primary benefit of hybrid cloud is agility. The need to adapt and change Direction quickly is a core principle of a digital business. Your enterprise might want (or need) to combine public clouds, private clouds, and on-premises resources to gain the agility it needs for a competitive advantage.

Apps that can easily move to the cloud. Meanwhile, two out of every three apps remain on-premises due to issues such as data gravity, sovereignty, compliance cost and interdependencies with other systems. This leaves enterprises in the middle of old and new struggling to reach their transformation goals with complex dual IT operation environment.

CONCLUSION:

Hybrid cloud can be an effective solution for a businesses with a tight focus on security or unique physical presence demands…….. Ultimately hybrid cloud allows organizations to leverage public cloud services without offloading the eternity of their data to a third -party data centre.

REFERENCES:

https://www.citrix.com/en-in/solutions/app-delivery-and-security/what-is-hybrid-cloud.html

INTERNET OF THINGS

ANJU S M (20MCA03)

RACHANA K Y (20MCA28)

The Internet of things(IOT) refers to a type of network to connect anything with the internet based on stipulated protocols through information sensing equipments to conduct information exchange and communications in order to achieve smart recognitions,positioning,tracing,monitoring,and administration. IOT enables different technologies, about its architecture, characteristics& applications, IOT functional view &what are the future challenges for IOT.

The IOT concept was coined by a member of the Radio Frequency Identification (RFID) development community in 1999, and it has recently become more relevant to the practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics.Imagine a world where billions of objects can sense, communicate and share information, all interconnected over public or private Internet Protocol (IP) networks. These interconnected objects have data regularly collected, analysed and used to initiate action, providing a wealth of intelligence for planning, management and decision making. This is the world of Internet of Things (IOT)

Internet of Things common definition is defining as: Internet of Things (IOT) is a network of physical objects. The Internet is not only a network of computers, but it has evolved into a network of a device of all type and sizes,vehicles,smart phones, home-appliances ,toys,cameras,medical-instruments,animals,people,buildings,all connected, all communicating & sharing information based on stipulated protocols in order to achieve smart

recognitions,positioning,tracing,safe & control & even personal real time online monitoring, onlineupgrade, process control & administration.

INTERNET OF THINGS IS AN INTERNET OF THREE THINGS:

(1).People to people,

(2).People to machine/things,

(3).Things/machine, interacting through internet.

Internet of Things (IOT) is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. Withthe Internet of things the communication is extended via Internet to all the things that surround us. The Internet of Things is much more than machine to machine communication, wireless sensor networks,2G/3G/4G,GSM,GPRS,RFID,WI-FI,GPS,microcontroller,microprocessor…etc. Theseare considered as being the enabling technologies that make "Internet of Things "applications possible.

REFERENCES:

https://www.researchgate.net/publication/330425585_Internet_of_Things-IOT_Definition_Characteristics_Architecture_Enabling_Technologies_Application_Future_Challenges

https://www.plm.automation.siemens.com/global/en/resource/achieve-success-with-iot/84671?gclid=CjwKCAjwzruGBhBAEiwAUqMR8Bm9LTe-Xumg0BIDXfTMrCz_THgJive0GCL3_hgh6Xv5_B8KVKNdZRoC4scQAvD_BwE&stc=indi100002&ef_id=CjwKCAjwzruGBhBAEiwAUqMR8Bm9LTe-Xumg0BIDXfTMrCz_THgJive0GCL3_hgh6Xv5_B8KVKNdZRoC4scQAvD_BwE:G:s&s_kwcid=AL!463!3!527888171429!p!!g!!iot

INTERNET OF BEHAVIOUR (IoB)

ASWATHI MOHAN (20MCA04)

SUPRIYA R (20MCA35)

INTRODUCTION

The Internet of Things (IoT) is a network of interconnected physical objects that collect and exchange information and data over the internet. Data collection provides valuable information about customer behaviors, interests and preferences, and this has been referred to as the Internet of Behavior (IoB). The IoB attempts to understand the data collected from users' online activity from a behavioral psychology perspective. With the results of that analysis, it informs new approaches to designing a user experience (UX), search experience optimization (SXO), and how to market the end products and services offered by companies.

In addition, IoB combines existing technologies that focus on the individual directly such as facial recognition, location tracking and Big Data. Therefore, IoB is a combination of three fields: technology, data analytics and behavioral psychology.

The purpose of IoB is to capture, analyze, understand and respond to all types of human behaviors in a way that allows tracking and interpreting those behaviors of people using emerging technological innovations and developments in machine learning algorithms. Through Big Data, information can be accessed from multiple points of contact. This makes it possible to explore the customer experience (CX) from start to finish, to know where the customer's interest in a product begins, their journey to purchase and methodology used to make the purchase.

The IoB will take the trend of building products and marketing strategies to promote the buyers, to the next level and is set to generate considerable momentum in the development of the sales industry. The technology may still be in its early days, but by the end of 2025, more than 50% of the world's population will be exposed to at least one IoBprogramme.

Companies using the IoT to get us to change our behaviors isn't about the "things" at all. As the IoT links people with their actions, we've verged into the Internet of Behavior. As companies learn more about us(the IoT), they can affect our behaviors(the IoB). Consider a health app on our smartphone that tracks our diet, sleep patterns, heart rate, or blood sugar levels. The app can alert you to adverse situations and suggest behavior modifications towards a more positive or desired outcome.

IoT – harvested data leveraged with IoB technology can be used to sell, Organizations will be able to test the efficiency of their campaigns. Also, healthcare providers can measure patient activation and engagement efforts. In conclusion, IoB's catalogue of applications is already extensive, but will continue to expand as it becomes established in the society.

This evolving technology is going to prove beneficial in multiple ways. From positively engaging customers, knowing where the customer's interest in a product begins, their journey

of purchase, and the methodology they use to make their purchase; there are many aspects of IoB. The IoB makes it easy to study previously unattainable data on how users interact with devices and products, obtain more detailed information about where a customer is in the buying process, and analyze customer buying habits across all platforms. Moreover, it provides real-time notifications, targeting and resolving problems quickly to close sales and keep customers satisfied.

ADVANTAGES OF IOB

The Internet of Behavior will be a tool of revenue generation for most people, companies, and organizations. IoB is surely going to introduce tech-savviness to all the sectors of the population. IoB will provide enough data for market research. IoB can also be used to enhance the security of public places with face recognition. IoB insists on an individual approach for all users. It will provide more business opportunities to people. It is going to reduce the monitoring costs of industries. It will provide a better customer experience due to personalized targeting of the product and services. IoB will start a new era of being in the digital world.

LIMITATIONS OF IOB

Internet of Behavior security is a critical issue. Nothing is 100% safe and so the internet of Behavior is. There are chances of Data Theft and personal information leaks, that may adversely affect the individuals. The abundance of data and insight will be a huge challenge to manage and secure. There will be a greater need for cybersecurity to stop cyber crimes. The Internet of Behavior is still in its early days, so a lot of drawbacks may come out in the future that is currently hidden.

REFERENCES

- https://www.tekkiwebsolutions.com/blog/internet-of-behavior/#Pros_and_Cons_of_Internet_of_Behaviors_IoB
- https://iotdesignpro.com/articles/what-is-internet-of-behavior-iob
- https://www.vectoritcgroup.com/en/tech-magazine-en/user-experience-en/what-is-the-internet-of-behaviour-iob-and-why-is-it-the-future/
- https://internationalbanker.com/technology/what-is-the-internet-of-behaviour/

SMART HOME TECHNOLOGY

G HARSHITHA (20MCA44)
PRANATHI R(20MCA27)

Smart homes are achieving more popularity from the past decades as they have increased comfort and quality life. Smart Home technology can be referred as "Connected home". Majority of home systems are controlled remotely from anywhere with an internet connection with smart phones, microcontrollers or any other device. Home automation allows controlling almost every aspect of our home through the internet of Things (IoT). From energy management and home security systems, to entertainment and online shopping, customers now depend on a range of wireless applications that will enhance our daily experience of domestic life. The modern home is a different place to even how it was 50 years ago. By the turn of the 21 century, most home has things that once thought to be luxury. They needed an actual human to make them do things. The stage was set for the next evolution in home appliance convenience: being smart! The advent of the cloud would be the wave for the new concept in smart tech- IOT. One of kind was Echo IV home automation device (mid 1960's) which was able to compute shopping lists, home temperature control and turn on and off device. But today's smart market kidded off the turn of the millennium, the market has exploded.

Smart home technology refers to any suite of devices, appliances or system that connects into a common network that can be independently and remotely controlled. Smart home automation allows you to tap into high-tech functionalities and luxury that wasn't possible in the past. As development of technology expands so will the possibility for the customer, home automations makes life easier and more enjoyable. The two ways in which home automation working is implemented is central controlled and app based.

Central controlled controls everything in our home and allows us from a single source, to controls the lights, thermostats, sprinklers, phones, washer, drier and more. This type of automation is mostly popular with businesses and upscale private residencies. These are run through a wall mounted terminals. Namely, Wondrwall's reactive house management system-single-handedly manages house heating, lighting and security in one place. It can access all the different aspects of our home from one convent system and also fairly high end, which in turn means high quality. These systems are expensive and need professional installation.

App based smart home system uses our home network to communicate with the cloud. Cloud technology is vital part of IoT and both have grown very popular in the last few years. Once we have created personalized account with these apps, we can coordinate with the smart home devices. Until the home devices are connected to the internet, we can communicate most of this cloud based home automation devices from anywhere (in the vicinity of our home automation devices for them to work). These devices are affordable, easy to set up, use and update. It is a huge market now; new devises are coming out constantly.
Some applications that has easy installation, namely,

- Smart Speakers can perform more task than playing music, like tell us about the weather, give us news briefing, works as personal assistant and acts as a central control hub namely Alexa, Amazon Echo, apple Home pod and much more.
- Robot Vacuums - unlike many traditional vacuums most robots don't use bags to hold the dust. They use an easy to remove dustbin, we can simply eject and empty into the nearest garbage can. Naming few, iRobot Roomba S9+, Neato Botvac D4 much more.
- Light Automation - smart light switches is controlled by app and has many choices like dimming. Low battery level detection and notification for all battery sensors. Wake up light alarm with sunrise effect automation blueprint.
- Smart Dishwasher – Companies like HeatWorks, are producing smart mini dishwashers that can also cook food.Example- Xiaomi Mijia, LG, GE, Whirlpool etc.
- Digital Smart showers allows us to fully control every aspect of showering experience-temperature, flow, duration , outlet, and an option of playing our favourite spotify playlist from phone/ even through voice activation when paid with smart speakers such as Amazon Alexa.
- Smart Refrigerators – also known as internet refrigerators able to determine itself whenever a food item needs to be replenished and also can order groceries as and when we need them. It also alerts the person if the door is left open.

The new future is very healthy for the industry. But, with the increased interconnectivity of devices, it is not inconceivable that our home will become very personal assistant in time. Our home in future would know us better than ourselves. This entire smart home Automation has its own potential pitfalls. Example, Security is endangered because we are all the time connected to the internet, anyone can hack which leads into seriously compromise our personal space, privacy and data that is a huge problem today.

Cyber security will be critical for the future smart home tech. The role of cyber security is important as it adds firewall to each of the devices present in dwelling that are controlled by a cyber attack, it could not be able to access the rest of the home network or get any personal information. Security operation tasks require human intervention. These tasks can be automated such as monitoring intrusions detection systems to search for threats. It helps in protecting organization and individuals from the theft of personal information. It prevents or mitigates harm to – or destruction of – computer networks, applications, device and data.

Another major disadvantage is that people become over dependent on technology which leads to health issues and mental stress.

Be it good or bad, the rise of these smart technologies would be growing!!

REFERENCES

https://www.otelco.com/resources
https://www.youtube.com/watch?v=hYJTPNyCacs

VIRTUAL REALITY

S SWATHI (20MCA38)

V UVA RANI (20MCA41)

The concept of virtual reality is built on the natural combination of two words: the virtual and the real. The former means "nearly" or "conceptually," which leads to an experience that is near-reality through the use of technology.

WHAT IS VIRTUAL REALITY?

Virtual Reality (VR) is a computer-generated environment with scenes and objects that appear to be real, making the user feel they are immersed in their surroundings. This environment is perceived through a device known as a Virtual Reality headset or helmet. VR allows us to immerse ourselves in video games as if we were one of the characters, learn how to perform heart surgery or improve the quality of sports training to maximise performance.

Although this may seem extremely futuristic, its origins are not as recent as we might think. In fact, many people consider that one of the first Virtual Reality devices was called Sensorama, a machine with a built-in seat that played 3D movies, gave off odours and generated vibrations to make the experience as vivid as possible. The invention dates back as far as the mid-1950s. Subsequent technological and software developments over the following years brought with them a progressive evolution both in devices and in interface design.

MAIN APPLICATIONS OF VIRTUAL REALITY

That's enough about the theory that is projecting us into the future. Which sectors is Virtual Reality actually being used in today? Medicine, culture, education and architecture are some of the areas that have already taken advantage of this technology. From guided museum visits to the dissection of a muscle, VR allows us to cross boundaries that would otherwise be unimaginable.

VIRTUAL REALITY USE CASES

The simplest example of VR is a three dimensional (3D) movie. Using special 3D glasses, one gets the immersive experience of being a part of the movie with on-spot presence. The leaf falling from a tree appears to float right in front of the viewer, or the shot of a speeding car going over a cliff makes the viewer feel the chasm's depth and may give some viewers the feeling of falling. Essentially, the light and sound effects of a 3D movie make our vision and hearing senses believe that it's all happening right in front of us, though nothing exists in physical reality.

Technological advances have enabled further enhancement beyond standard 3D glasses. One can now find VR headsets to explore even more. Aided by computer systems, one can now play "real" tennis (or other sports) right in their living room by holding sensor-fitted racquets for playing within a computer-controlled game simulation. The VR headset that players wear

on their eyes gives the illusion of being on a tennis court. They move and try to strike depending upon the speed and direction of the incoming ball and strike it with the sensor-fitted racquets. The accuracy of the shot is assessed by the game-controlling computer, which is shown within the VR game accordingly—showing whether the ball was hit too hard and went out of bounds or was hit too soft and was stopped by the net.

Other uses of this VR technology involve training and simulation. For example, those wanting to get a driver's license can get a first-hand experience of road driving using a VR setup that involves handling car parts like the steering wheel, brake, and accelerator. It offers the benefit of experience without the possibility of causing an accident, so students can develop a certain level of expertise in driving before actually being on the road.

THE FUTURE OF VIRTUAL REALITY

Virtual Reality is one of the technologies with the highest projected potential for growth. According to the latest forecasts from IDC Research (2018), investment in VR and AR will multiply 21-fold over the next four years, reaching 15.5 billion euros by 2022. In addition, both technologies will be key to companies' digital transformation plans and their spending in this area will exceed that of the consumer sector by 2019. It is, therefore expected that by 2020 over half of the larger European companies will have a VR and RA strategy.

The big technology companies are already working to develop headsets that do not need cables and that allow images to be seen in HD. They are developing Virtual Reality headsets in 8K and with much more powerful processors. There is even talk that in the next few years they could integrate Artificial Intelligence. The latest 5G standard can also provide very interesting scenarios for the evolution of VR. This standard will allow more devices and large user communities to be connected. In addition, its almost imperceptible latency will make it possible for consumers to receive images in real time, almost as if they were seeing them with their own eyes.

All this means that Virtual Reality is no longer science fiction. It is integrated into our present and, in the coming years, it will lead to advances that will shape the future.

REFERENCES :

www.google.com

https://www.iberdrola.com/

INTELLIGENT APPS

HARSHITHA M(20MCA14)

MAHIMA I(20MCA21)

Intelligent Apps are applications that use historical and real time data from the user interactions and other sources to make predictions, suggestions and personalized and uses predictive analytics to quickly adapt to the information it receives. It uses built-in machine learning algorithms to process vast amounts of data to continuously improve performances

EXAMPLES OF GREAT INTELLIGENT APPS: Alexa, Siri, Cortana, and Google Assistant: All these personal assistant apps are great AI applications that leverage natural language generation and machine learning to become excellent assistants and companions to its users. Elsa: It is a renowned teacher of English pronunciation. The app gives accurate feedback on the user's pronunciation and adapts the training to his unique needs.Socratic: The smart app helps students with math and other homework. Users may ask or simply take a photo of the complex concept, and AI-powered assistant will provide a visual explanation.Ada Health: This app is often called as Doctor in your pocket. It carefully listens to users symptoms, asks clarifying questions, and helps to navigate to the most suitable care analyzing the responses against a rich data of similar cases.Hound: It is also another perfect example of how Artificial Intelligence in mobile apps can simplify your life. The app seizes voice commands to execute different actions such as getting familiar with the best hotel, restaurant, or doctors.

BENEFITS OF INTELLIGENT APPS-Action-oriented: The major factor of i-apps is that these applications do not wait for users to make every move. Instead, they study user behaviour and provide personalized and actionable outcomes using the power of Predictive Analytics. In this way, they cut down the conflict of users and urge them to seize desired actions.The great example to understand this trait of Intelligent Applications is Hound app.Data-driven:One of the key features of Intelligent Apps is delivering a data-driven output. The i-apps collect information from different sources like be it IOT sensors, websites, mobile apps, beacons, etc., and examine it in real-time. An outcome of which is that you get the exact results for almost everything when asked. Adaptive in nature: Supported by Machine learning algorithms, these apps are adaptive. They can effortlessly promote their knowledge as per their surroundings. Exclusion of keyboard inputs: Since providing high comfort is a core objective of i-apps, these applications also stimulate the opportunity to provide commands without using keyboards. It means that these apps respond to commands offered in the form of speech, image, gesture movement, etcOmni Channel: It is one of the most fundamental features of Intelligent Apps. These applications understand that users want a familiar experience, irrespective of which outlet they are interacting with. And therefore, assures that they receive the same experience on all the communication channels.

FEATURES OF INTELLIGENT APPS: Data-driven: These apps process and combine different data sources and with the help of these multiple sources of data they can

offer valuable insights.Relevant and contextual: The Intelligent Apps make proper use of the features of the device in order to deliver highly proactive suggestions and information. There is no need for the users to go to the apps, instead, the apps will come to them. Continuously adapting: These apps are capable of adopting continuously in order to improve their output.Action-oriented: These apps are capable of anticipating the behaviour of the users with the help of predictive analytics and they can offer actionable and personalized suggestions.

FUTURE OF INTELLIGENT APPS: Organizations around the world are already widely adopting Intelligent Apps approach and steering away from just 'big data'. While data is a huge and the most basic element in information technology, organizations are expanding the use of machine learning and cloud infrastructure to create more intelligent applications and systems. Effective intelligent apps will be able to use the richness of all available data made available to reveal the true content in real-time in the future. As data volumes increase and organizations scale, security will be a big issue to deal with for Intelligent App developers. And therefore the developers need to focus on building up the security wants and needs.

REFERENCES:

https://appsierra.com/what-are-intelligent-apps/

https://becominghuman.ai/how-intelligent-apps-are-changing-the-mobile-app-industry-and-our-lives-834ea2273861

https://www.futuristictechnologies.co.uk/intelligent-apps/

https://www.validatek.com/technologies/intelligent-apps-and-analytics

CYBER SECURITY MESH

GUDIYA KUMARI (20MCA12)

RAMYA S(20MCA30)

Cybersecurity Mesh is a broader concept thatinvolvesabroader network of nodes than that of confidential computing which relates more to security around data processing.More specifically, a Cybersecurity Mesh consists in designing and implementing an IT security infrastructure that does not focus on building a single 'perimeter' around all devices or nodes of an IT network, but instead establishes smaller, individual perimeters around each device or access point. This creates a modular and more responsive security architecture covering physically disparate access points of the network. Cyber security mesh is a distributed architectural approach to scalable, flexible and reliable cyber security control. Cyber security mesh essentially allows for the security perimeter to be defined around the identity of a person or thing.With the cyber security mesh, one can get to any digital security asset – regardless of its location. The advantage of this technology is that it permits individuals to put the security divider around people instead of the whole organization.

The goal is to ensure that each access point's security can be effectively managed from a centralized point of authority. In this way, the mesh can be viewed as centralization of your security policy, and a distribution of that policy's enforcement.A Cybersecurity Mesh can establish a more robust, flexible and modular approach to a network's security. By ensuring that each node has its own perimeter, it allows an IT network manager to better maintain and track different levels of access to various parts of a given network. This aims to prevent hackers from exploiting a given node's weakness to access the broader network.

The abrupt ascent in remote workforces and cloud technology has influenced the security of company assets outside the organization's edge. Because of the assistance of the cyber security mesh, the security border goes beyond and covers people working remotely.

HOW WILL INFORMATION TECHNOLOGY(IT) DEVELOPMENT BE AFFECTED BY CYBERSECURITY MESH?

The 'password-protected' approach to IT security is moving towards a slow but sure sunset with the rise of complex cyber-attacks that can use any techniques, including Artificial Intelligence and Machine Learning to figure out weak links and passwords. Cybersecurity mesh is more likely to be integrated right into the network or platform development. This is especially important since Big Data Analytics grows to play more significant role in collecting business intelligence from data in any business.

Organisations that use customised website or software solutions for employee management and communication or customer interaction would want to reduce the risk of unauthorised access to any user's data or device. Cybersecurity mesh could play a massive role in ensuring or overall protection in such cases irrespective of the device's security environment.

Those organisations planning to implement the security mesh from the initial stages should get the developer to implement the mesh right from the planning stage to ensure the steps are taken to mitigate their networks' threats. Cybersecurity Mesh can establish a more flexible, robust, and modular approach to network security. Ensuring each node has its own perimeter, which allows IT, network managers, to maintain better and keep track of differentiated levels of access to different parts of a given network, and prevent hackers from exploiting a given node's weakness access the broader network. According to the market research, "The global cybersecurity market size was estimated at USD 156.45 billion in 2019 and is expected to reach USD 326.36 billion by 2027 growing at a compound annual growth rate of 10.0%."

Key factors that are driving the market growth include the vulnerable data on web and computer, loophole in new technologies such as IoT and big data, along with deployment of the cyber solutions across industries such as retail, financial institutions and IT sector.

The last few years has witnessed a dramatic expansion in the number and complexity of devices and processes connected to the internet – collectively known as the Internet of Things (IoT). With a proliferation of devices and activity on the internet, the number of potential access points for hackers to steal data has increased too. As the security of an IT system is only as strong as its weakest link, this situation has resulted in a new approach to IT security.

REFERENCES:

https://smartz-solutions.com/what-is-cybersecurity-mesh/

https://techutzpah.com/what-is-cybersecurity-mesh/

https://www.bankofbaroda.in/banking-mantra/fintalkblog/blogdetail.htm?139/cybersecurity-mesh

AMBIENT INTELLIGENCE

RAMYAK.P(20MCA29)

SWETHA M(20MCA39)

INTRODUCTION:

In computing, **ambient intelligence** (**AmI**) refers to electronic environments that are sensitive and responsive to the presence of people. Ambient intelligence was a projection on the future of consumer electronics, telecommunications and computing that was originally developed in the late 1990s by Eli Zelkha and his team at Palo Alto Ventures for the time frame 2010–2020.Ambient intelligence would allow devices to work in concert to support people in carrying out their everyday life activities, tasks and rituals in an intuitive way using information and intelligence that is hidden in the network connecting these devices (for example: The Internet of Things). As these devices grew smaller, more connected and more integrated into our environment, the technological framework behind them would disappear into our surroundings until only the user interface remains perceivable by users.

The ambient intelligence paradigm builds upon pervasive computing, ubiquitous computing, profiling, context awareness, and human-centric computer interaction design, of which, is characterized by systems and technologies that are:[5]

- embedded: many networked devices are integrated into the environment
- context aware: these devices can recognize you and your situational context
- personalized: they can be tailored to your needs
- adaptive: they can change in response to you
- anticipatory: they can anticipate your desires without conscious mediation.

A typical context of ambient intelligence environment is home, but may also be extended to work spaces (offices, co-working), public spaces (based on technologies such as smart street lights), and hospital environments.

OVERVIEW:

Ambient intelligence is primarily of interest because of its relationship to user experience and the advancement in sensor technology and sensor networks.The interest in user experience grew in importance in the late 1990s as a result of the increasing volume and importance of digital products and services that were difficult to understand or use. In response, the user experience design emerged to create new technologies and media around the user's personal experience. Ambient intelligence is influenced by user-centered design where the user is placed in the center of the design activity and asked to give feedback through specific user evaluations and tests to improve the design or even co-create the design with the designer (participatory design) or with other users (end-user development).

CRITICISM:

As far as dissemination of information on personal presence is out of control, ambient intelligence vision is subject of criticism (e.g. David Wright, Serge Gutwirth, Michael Friedewald et al., Safeguards in a World of Ambient Intelligence, Springer, Dordrecht, 2008). Any immersive, personalized, context-aware and anticipatory characteristics brings up societal, political and cultural concerns about the loss of privacy. The example scenario above shows both the positive and negative possibilities offered by ambient intelligence. Applications of ambient intelligence do not necessarily have to reduce privacy in order to work.

Power concentration in large organizations, a fragmented, decreasingly private society and hyperreal environments where the virtual is indistinguishable from the real are the main topics of critics.Several research groups and communities are investigating the socioeconomic, political and cultural aspects of ambient intelligence.

TECHNOLOGIES:

Ambient Intelligence builds on three recent key technologies:

- **Ubiquitous Computing** means integration of microprocessors into everyday objects.
- **Ubiquitous Communication** enables these objects to communicate with each other and the user by means of ad-hoc and wireless networking.
- An **Intelligent User Interface** enables the inhabitants of the Aml environment to control and interact with the environment in a natural (voice, gesture) and personalized way (preferences, context).
- Other technologies used for implementing Aml are:
  - Bluetooth low energy
  - RFID
  - Sensors
  - Software Agents
  - Biometrics

FUTURE SCOPE:

- Many Aml applications relying upon wireless sensors are at the mercy of the battery life for the sensors.
- Challenge is to model multiple residents in an environment.
- Issues related to security and privacy for Aml systems.

CONCLUSION:

Ambient Intelligence is establishing fast as an area where a confluence of topics can converge communication, computing, consumer electronics to help society through technology.

REFERENCES:

https://en.m.wikipedia.org/wiki/Ambient_intelligence

https://www.slideshare.net/chandrika95/ambient-intelligence-58604649

INTELLIGENT AUTOMATION

NEHA KOUSER(20MCA24)
MISBA RAFIA KHANUM(20MCA23)

Intelligent automation is a combination of Robotic Process Automation and artificial intelligence technologies which together empower rapid end-to-end business process automation and accelerate digital transformation.

To extend the horizons of business process automation by an order of magnitude, intelligent automation combines the task execution of RPA with the machine learning and analysis capabilities of automatic process discovery and process analytics as well as well as cognitive technologies, like computer vision, natural language, processing and fuzzy logic.

First, with the emergence of field area networks, it has become possible to collect data from sensors distributed across geographically dispersed areas, while their processing was done centrally in Programmable Logic Controllers (PLCs). Second, there were attempts to facilitate integration of PLCs into systems communicating via networks, by proposing integration component architectures such as Modbus-IDA.

Finally, it comes to genuinely distributed automation development, where the intelligence is designed from the very beginning as decentralized and embedded into software components, which can be freely distributed across networked hardware devices. The design of distributed systems, in general, has been identified as grand challenge of computing.

The IEC architecture has been conceived to facilitate the use of distributed automation intelligence, but for some time the standard could not make its way to the industrial practice. Now, with the emergence of professionally made software tools and dozens of hardware platforms one can expect stronger industrial interest to distributed automation.

The technologies in intelligent automation are unattended robots or server bots that fully automate processes that do not require human judgment or invention. Machine learning algorithms that find patterns in structured data through “supervised” and “unsupervised” learning.

For example, an automotive manufacturer may use IA to speed up production or reduce the risk of human error, or pharmaceutical or life sciences company may use intelligent automation to reduce costs and gain resource efficiencies where repetitive processes exist.

Robotic Process automation(RPA) is an essential element of a fully realized IA strategy. With RPA, “bots” become a part of your workforce-your digital workforce.

By letting bots perform repetitive, high-volume data processes, you free your work for higher-value tasks.

A successful RPA solution will analyze processes down to click-level quickly, accurately and intuitively. It automaticallydocument process steps. It runs unattended and attended automations ensuring maximum bot utilization scalability.

It Orchestrate your bots using a real-time dashboard for live monitoring and intuitive management.

Administrative tasks are often the first that organizations identify as RPA candidates, but you can apply RPA to nearly any task that follows the same process each time.

Examples include responding to frequently asked questions in customer service, verifying the accuracy of invoices based on predefined rules in according, recording, staff hours and absences in HR and tracking deliveries in logistics.

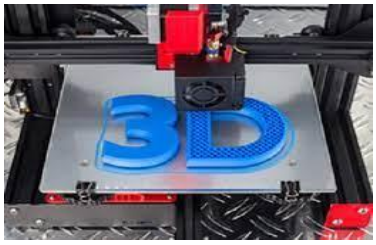
REFERENCES

www.appian.com
https://scholar.google.co.in/intelligent-automation

3D PRINTING

DAINY JOSE(20MCA09)
HARSHA P C (20MCA13)

INTRODUCTION:



3D printing is a method of creating a three dimensional object layer-by-layer using a copier created design. It is also known as Additive manufacturing. It was developed by Kodma of the Nagoya Municipal Industrial Research Institute

TECHNOLOGIES:

There are three broad types of 3D printing technology.

Sitering: It is a technology where the material is heated, but not to the point of melting, to create high resolution items. Metal powder is used for direct metal laser sintering while thermoplastic powders are used for selective laser sintering.

Melting: It is a method of 3D printing including powder bed fusion, electron beam melting and direct energy deposition. These are lasers, electric arcs or electronic beams to print objects by melting the materials together.

Stereolithography: It utilisesphotopolymerization to create parts. This technology uses the correct light source to interact with the material in a selective manner to cure and solidify a cross section of the object in thin layers.

TYPES OF 3D PRINTING:

3D printing has been categorised into seven groups by ISO/ASTM 52900 additive manufacturing-general principles -terminology.

BinderJetting: It is a 3D printing process that uses a liquid binding agent deposited onto a build platform to bond layers of powder material and form a part. It can be used in 3D metal printing, full color prototype and large scale ceramic moulds.

Material Extrusion: It is used to process thermoplastic materials in filament form to create three dimensional objects. And it is also known as Fused Filament Fabrication or Fused Deposition Modeling.

Material Jetting: It enables the multi-material production of parts with accuracy and minimal material waste. It is used for medical models, prototypes and casting patterns.

Powder Bed Fusion(PBF): This method uses either a laser or electron beam to melt and fuse material powder together. Electron beam melting(EBM) methods require a vacuum involving the spreading of the powder material over previous layers.

Sheet Lamination: This method can be bonding, ultrasonic welding or brazing while the final shape is achieved by laser cutting or CNC machining.

VAT Photopolymerisation: It uses a vat of liquid photopolymer resin, out of which model is constructed layer by layer. An UV light is used to cure or harden the resin where required, whilst a platform moves the object being made downwards after each new layer is cured.

3D PRINTING INDUSTRIES:

Aerospace:3D printing is used across the aerospace industry due to the ability to create light, yet geometrically complex parts, such as blisks. Rather than building a part from several components, 3D printing allows for an item to be created as one whole component, reducing lead times and material wastage.

Robotic: The speed of manufacture, design freedom, and ease of design customization make 3D printing perfectly suited to the robotic industry. This includes work to create bespoke exoskeletons and agile robots with improved agility and efficiency.

Medical: The medical sector has found uses for 3D printing in the creation of made-to-measure implants and devices. For example, hearing aids can be created quickly from a digital file that is matched to a scan of the patient's body.

Rail: The rail industry has found a number of applications for 3D printing, including the creation of customised parts, such as arm rests for drivers and housing covers for train couplings.

REFERENCES:

https://www.twi-global.com/technical-knowledge/faqs/what-is-3d-printing#Historyof3DPrinting

ROBOTICS

AMRUTHA MB (20MCA02)

VIJAYLAKSHMI Y(20MCA43)

Robotics is the inter disciplinary field that integrates computer science and engineering. Robotics involves design, construction, operation, and use of robotics. The goal of robotics is to design machine that can help and assist humans.

TYPES OF ROBOTICS SOFTWARE

1.Offline Programming:

Offline programming software provides a way for you to program your industrial robot without needing to be physically connected to the robot at the time. This means that you don't need to take the robot out of production to program it. It reduces downtime, improves the quality of programming and allows you to change between product lines quickly, amongst other benefits.

2.Simulators:

Robot simulators come in many forms. Some only allow for simple 2D simulation of specific aspects of robotics whilst other include 3D simulation with complex physics engines and realistic environment. If you wanted to, you could spend a lot of time testing all the many different simulation packages available. Unfortunately, it's difficult to tell from a promotional video haw easy a simulator is to use. You have to go out and test if for yourself.

3.Middleware:

The most popular being ROS (Robot Operating System). Robot middleware provides a framework for running and managing complex robotic system from a single unified interface. Middleware is the "Software glue" that helps robot builders to avoid reinventing the wheel when they are designing a new robotic system.

4.Mobil Robot Planning:

Mobile robots are programmed in a different way from other robots which means using a different type of software too. There are lot of interesting software tools available for mobile robot programming, ranging from warehouse logistics to autonomous vehicles. For example, path planners are used to program the route that the robot will take through the environment while obstacle avoidance algorithms react to changes in the moment.

5.Real-Time path planning:

Path planning software is used in many areas of robotics. Basic path planners, like our PRM feature, are simply used to speed up the programming phase for industrial robotics. Real-time path planning is much more complex than basic path planning because it involves continually

updating the program to respond to changes in the environment. These allow the robot to be reactive but can also make the robot more unsafe.

6.UAV (Drone) Control:

A growing type of robotic software is drone control. This refers to any software which is used to program and coordinate unmanned aerial vehicles (UAV's/drones).There have been a growing number of application areas for drones over the last decade or so with drones now used in agriculture, inspection, and security. Software for drones tends to focus on particular application areas or aspects of drone control (e.g. data collection, image analysis, mapping etc.)

7.Artificial Intelligence for Robotics:

Artificial intelligence (AI) has been used with robotics for many years - almost as long as robotics have been around. However, there has recently been a rising number of software solutions specifically for using Ai with robots in particular application areas. As with the other types of robot software, AI tends to be focused on specific aspects of their applications.

REFERENCES:

https://www.automate.org/news/9-types-of-robotics-software-you-might-consider-for-your-robot

5G NETWORK

AISHAWRYA K V(20MCA01)

GOPIKASUCHARITHA (20MCA11)

INTRODUCTION:

In our hyperconnected era, the number of networked devices may reach 29.3 billion by 2023-more than three devices for devices for every human being on the planet. Next-generation wireless technologies such as 5G and Wi-Fi 6 are poised to become a circular part of the networks that link machines and people. By offering significant performance improvements-such as faster speeds, increased data capacity, lower latency, greater device density and precise location sensing-these new wireless technologies are already enabling novel solutions, including autonomous vehicles, precision automation and robotics. Innovative solutions such as these are why leaders across industries see advanced wireless networks as increasingly essential to their strategies. And rising urgency is accelerating a shift in focus to 5G and wi-fi 6, far faster than what executives forecast less than a year ago.

SPEED UPGRADES:

Each wireless network generation has reflected a significant increase in speed and the benefits of 5G-the fifth generation of cellular network technology-will push far beyond 4G LTE predicted speeds of up to 10Gbps represent up to a 100X increase compared to 4G.In practical terms 4G vs.5G speed enhancements will mean exciting possibilities for consumers transferring a high - resolution movie at peak download speed will go from taking 7minutes to just 6 second. That time saving could mean being able to grab that new hit film before the flight attendant asks you to put the phone in airplane mode.

LOW LATENCY:

Latency measures how long a signal takes to go from source to its receiver, and then back again. One of the goals for each wireless generation has been to reduce latency. New 5G networks will have even lower latency than 4G LTE, with the round-trip transmission of data taking less than five milliseconds. 5G latency will be faster than visual processing making it possible to control devices remotely in near-real time human reaction speed will be become the limiting factor for remote applications that use 5G and IoT-and many new applications will involve machine-to-machine communication that isn't limited by how quickly humans can respond.

INCREASED BANDWIDTH:

for business the impact of increased bandwidth will echo across many departments and division in the form of big data. Today, companies receive far more information from customers, suppliers, and teams than they can process and analyze for insight. With 5G connectivity and big data analytics, these businesses can turn large volumes of data into actionable knowledge. After carriers roll out full 5G features, consumers and businesses may begin to consider 5G networks a strong alternative for fats broadband connections. While agriculture, manufacturing, and logistics will all benefit from lower latency, gamers also eagerly anticipate the 5G rollout. The combination of high speed and minimal lag is perfect for virtual reality.

THINGS TO KNOW ABOUT 5G:

5G is currently in the earliest phase of deployment, with carries rolling out limited 5G availability by the end of 2021.Icreased mobile network capacity and low latency from 5G will make new applications possible, form 5G-enabled smart factories and cities to constantly connected medical devices.5G represents the first time wireless network has been created with more than phones in mind-with edge computing and the internet of thins(IoT) becoming vital to 5G from the start.

REFERENCES:

www.hpe.com/hep5G_solutions

www.deloitte.com/global/en/insigghts/industry/technology

BLOCK CHAIN

LAVANYA S(20MCA18)

LAVANYA SA(20MCA19)

INTRODUCTION:

A blockchain is a distributed software network that functions both as a digital ledger and a mechanism enabling the secure transfer of assets without an intermediary. ... Anything from currencies to land titles to votes can be tokenized, stored, and exchanged on a blockchain network.

Blockchain Technology first came to light when a person or Group of individuals name 'Satoshi Nakamoto' published a white paper on "BitCoin: A peer to peer electronic cash system" in 2008. Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible.

FUTURE OF BLOCK CHAIN:

Blockchain was invented by Satoshi Nakamoto. As the name suggests, blockchain is a chain of blocks that contains information. Each block consists of a number of transactions and each transaction is recorded in the form of Hash. Hash is a unique address assigned to each block during its creation and any further modification in the block will lead to a change in its hash.

MARKET VALUE OF BLOCK CHAIN:

The global blockchain technology market size was valued at USD 3.67 billion in 2020. It is expected to expand at a compound annual growth rate (CAGR) of 82.4% from 2021 to 2028.

BLOCK CHAIN BENEFITS:

- It is an immutable public digital ledger, which means when a transaction is recorded, it cannot be modified
- Due to the encryption feature, Blockchain is always secure
- The transactions are done instantly and transparently, as the ledger is updated automatically
- As it is a decentralized system, no intermediary fee is required
- The authenticity of a transaction is verified and confirmed by participants

WHY BLOCK CHAIN IS IMPORTANT:

- Make sure that all words are spelled correctly.
- Try different keywords.

- Try more general keywords.
- Try fewer keywords.

CONCLUSION:

The Bitcoin is the first successful implementation of blockchain. ... Today, the world has found applications of blockchain technology in several industries, where the trust without the involvement of a centralized authority is desired.

REFERENCES:

https://www.simplilearn.com/tutorials/blockchain-tutorial/why-is-blockchain-important

https://www.grandviewresearch.com ›

ARTIFICIAL INTELLIGENCE

S.V.TEJASHREE(20MCA31)

JOICE RANI J(20MCA16)

INTRODUCTION:

Artificial intelligence is intelligence demonstrated by machines, unlike the natural intelligence displayed by humans and animals, which involves consciousness and emotionality. The distinction between the former and the latter categories is often revealed by the acronym chosen. In the twenty-first century, AI techniques have experienced a resurgence following concurrent advances in computer power, large amounts of data, and theoretical understanding; and AI techniques have become an essential part of the technology industry, helping to solve many challenging problems in computer science, software engineering and operations research.

FUTURE OF ARTIFICIAL INTELLIGENCE:

There's virtually no major industry modern AI more specifically, "narrow AI," which performs objective functions using data-trained models and often falls into the categories of deep learning or machine learning hasn't already affected. That's especially true in the past few years, as data collection and analysis has ramped up considerably thanks to robust IoT connectivity, the proliferation of connected devices and ever-speedier computer processing. Some sectors are at the start of their AI journey, others are veteran traveller's. Both have a long way to go. Regardless, the impact artificial intelligence is having on our present day lives is hard to ignore.

HISTORY OF AI:

The concept of inanimate objects endowed with intelligence has been around since ancient times. The Greek god Hephaestus was depicted in myths as forging robot-like servants out of gold. Engineers in ancient Egypt built statues of gods animated by priests. Throughout the centuries, thinkers from Aristotle to the 13th century Spanish theologian Ramon Llull to René Descartes and Thomas Bayes used the tools and logic of their times to describe human thought processes as symbols, laying the foundation for AI concepts such as general knowledge representation.The late 19th and first half of the 20th centuries brought forth the foundational work that would give rise to the modern computer. In 1836, Cambridge University mathematician Charles Babbage and Augusta Ada Byron, Countess of Lovelace, invented the first design for a programmable machine. In the 1940s, Princeton mathematician John Von Neumann conceived the architecture for the stored-program computer -- the idea that a computer's program and the data it processes can be kept in the computer's memory. And Warren McCulloch and Walter Pitts laid the foundation for neural networks.

APPLICATIONS:

AI is relevant to any intellectual task. Modern artificial intelligence techniques are pervasiveand are too numerous to list here. Frequently, when a technique.

reaches mainstream use, it is no longer considered artificial intelligence; this phenomenon is described as the AI effect. High-profile examples of AI include autonomous vehicles (such as drones and self-driving cars), medical diagnosis, creating art (such as poetry), proving mathematical theorems, playing games (such as Chess or Go), search engines (such as Google Search),

online assistants, image recognition in photographs, spam filtering, predicting flight delays prediction of judicial decisions,targeting online advertisements,and energy storage.

COMPONENTS OF AI:

As the hype around AI has accelerated, vendors have been scrambling to promote how their products and services use AI. Often what they refer to as AI is simply one component of AI, such as machine learning. AI requires a foundation of specialized hardware and software for writing and training machine learning algorithms. No one programming language is synonymous with AI, but a few, including Python, R and Java, are popular.

AI as a service (AIaaS):

Because hardware, software and staffing costs for AI can be expensive, many vendors are including AI components in their standard offerings or providing access to artificial intelligence as a service platforms. AIaaS allows individuals and companies to experiment with AI for various business purposes and sample multiple platforms before making a commitment.

CONCLUSION:

Artificial intelligence developments are transforming the world for good. It is making our lives simpler and also making our society inclusive. But machines with AI must have some limitations. the ethics of artificial intelligence has to be implemented strictly. international policies on AI are very important to tackle security issues posed by artificial intelligence.

REFERENCES:

https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/what-is-artificial-intelligence

https://en.m.wikipedia.org/wiki/Artificial_intelligence

https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence

BIOMETRIC SECURITY

BABY(20MCA05)

K M POOJA MAURYA(20MCA17)

INTRODUCTION:

Biometric security is a security mechanism that identifies people by verifying their physical or behavioral characteristics. It is currently the strongest and most accurate physical security technique that is used for identity verification. Biometrics are mainly used in security systems of environments that are subject to theft or that have critical physical security requirements. Such systems store characteristics that remain constant over time – for instance, fingerprints, voice, retinal patterns, facial recognition, and hand patterns.

These characteristics are stored as "templates" in the system. When somebody tries to access the system, the biometric security system scans them, evaluates the characteristics, and attempts to match them with stored records. Then, if a match is found, the person is given access to the facility or device.

WORKING OF BIOMETRIC SECURITY:

The importance of biometric security in modern society is ever-growing. Physical characteristics are unique and fixed – including among siblings and even twins. An individual's biometric identity is able to replace (or, at the very least, supplement) password systems for phones, computers, and restricted areas.

After a person's biometric data is gathered and matched, the system saves it to be matched with subsequent access attempts. Usually, the biometric data is encrypted and then stored either in the device itself or in a remote server.

Hardware known as biometrics scanners captures physical characteristics for identity verification and authentication. The hardware's scans are compared to the saved database – and, depending on whether a match is found, access is granted or restricted. You can think of your own body as a key to unlock secure areas.

TYPE OF BIOMETRIC SECURITY:

- **Physical:**are based on the analysis of the invariable physiological characteristics of a person.
  eg: Facial geometry, Fingerprints, Skull shape, Retina, Iris, Hand geometry, Palm of figure veins, DNA.

- **Behavioral:** are based on the analysis of a person's behavioral characteristics — the characteristics inherent in each person in the process of reproducing an action.
  eg: Speaker recognition, Signature, Keystroke dynamics, Gait.

USE OF BIOMETRIC SECURITY:

- **Banking:**Many banks that have mobile apps allow user authentication via biometrics such as facial recognition, fingerprint scanning, and voice verification. And other banks use a combination of these biometrics; multi-factor authentication, when combined with biometrics, can create a nearly impenetrable layer of security.

- **Business security:**Many companies nowadays are installing access control and time tracking systems that incorporate biometric authentication. Take, for instance, Id time from RecFace. This software automatically records employees' working hours and

compliance with labor regulations, and it uses biometric data to do so. Identification takes less than 1 seconds, and 7 kinds of reports are generated during the execution.

- **Money security:**We mentioned how biometrics are used by banks; however, there is another financial application: biometric payment security. This technology is integrated during transaction authorization processes and, for now, mostly involves a fingerprint scan.

- **Home security:**Biometric technology can allow an individual to enter a home once its scanning unit has verified their identity. Access to office buildings, entire houses, or particular rooms can be controlled via biometrics. Biometric locks negate the need for a key and are operated with the swipe of a fingerprint instead.

BENIFTS OF BIOMETRIC SECURITY:

- Biometrics are inherent to the user.
- Biometrics are difficult to duplicate.
- Permission is easily managed.
- Efficiency is increased.
- Fewer security staff.
- No replacement costs.

FUTURE OF BIOMETRIC SECURITY:

We strongly believe that biometrics are the future of e-security systems – and the proof is in the pudding: more institutions are embracing biometrics by the day. Even the Windows 10 OS has incorporated a biometric security platform. Biometrics are also used in stadiums, airports, and banks across the world. Government agencies and law enforcement have also migrated to biometric systems – therefore, it is very likely that even more organizations will follow suit in the near future.

While biometric security systems are not fool-proof, they are still faster, more cost-efficient (in the long run), and more accurate than traditional security methods.

REFERENCES:

https://www.kaspersky.com/resource-center/definitions/biometrics

https://en.wikipedia.org/wiki/Biometrics

https://recfaces.com/articles/types-of-biometrics

https://www.techopedia.com/definition/6203/biometric-security

https://www.elprocus.com/different-types-biometric-sensors/

WIRELESS INTEGRATED NETWORK SENSORS

SWATHI N (20MCA37)

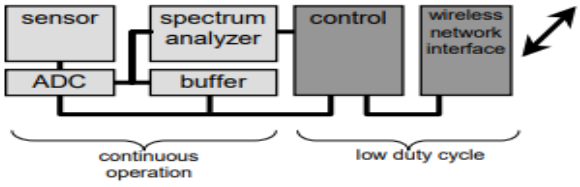
VIDHYA RATHOD (20MCA42)

INTRODUCTION:

Wireless Integrated Network Sensors (WINS) provide distributed network and internet access to sensors, controls, and processors that are deeply embedded in equipment, facilities, and the environment. The WINS network is a new monitoring and control capability for applications in transportation, manufacturing, healthcare, environmental monitoring, and safety and security, border security. WINS combine micro sensor technology, low power signal processing, low power computations, low-cost wireless networking capability in a compact system. WINS networks provide sensing, local control, and embedded intelligent systems in structures, materials, and environments.

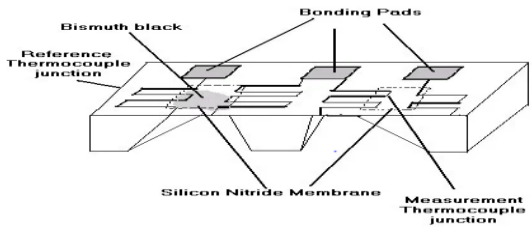
WIRELESS INTEGRATED NETWORK SENSOR ARCHITECTURE:

The wireless integrated network sensor (WINS) Includes sensors, data converter, signals processing, and control functions. Micropower RF communicationProvides bidirectional network access for low bite rate,Short range communication. The micro power components operate continuously for event recognition. While the network interface operates at low duty cycle.



WINS MICRO SENSORS:

The detector show in the thermal detector. It just captures the harmonic signals produced by the footsteps of the stranger entering the border. Whole area is partitioned into hexagonal region. These signals are then converted into their PSD values and are then compared with the reference values set by user.



BORDER SECURITY USING WIRELESS INTEGRATED NETWORK SENSOR:

Wireless Integrated Network Sensors (WINS) now provide a new monitoring and control for monitoring the borders of the country. Using the concept we can easily identify a stranger or some terrorists entering the border. The border area is divided into number of nodes. Each node is in contact with each other and with each other and with the main node. The noise produced by the foot-steps of the stranger and collected using the sensor. This sensed signal is then converts into power spectral density and compared with reference value of our convenience.Accordingly the compared value is processed using a microprocessor, which sends appropriate signals to the main node. Thus the stranger is identified at the main node.

CONCLUSION:

A series of interface, signal processing, and communication systems have been implemented in micro power CMOS circuits. A micro power spectrum analyzer has been developed to enable low power operations of the entire WINS system.Thus WINS require a microwatt of power. But it is very cheaper when compared to the other security system RADAR under use. It is even used for short distance communication less than 1 km, it produces a less amount of delay. Hence it is reasonably faster. On a global scale, WINS will permit monitoring of land, water, and air resources for environmental monitoring, on a national scale, transportation system, and borders will be monitored for efficiency safety, and security.

REFERENCES:

Wireless Integrated Network Sensors - Krazytech

https://www.slideshare.net/deepakmohapatra102/wirelwireless-integrated-network-sensors