Gayatri Vidya Parishad College Of Engineering for Women

DEPARTMENT of INFORMATION TECHNOLOGY

VOLUME - 3

SPIKE-IQ 2K18

FROM THE PRINCIPAL'S DESK

It is pleasure to know that GVPCEW is bringing out the magazine of IT department "***SPIKE-IQ 2K18***" for the year 2018-2019.

This institution constantly strives in the all-round development of the students through its endless efforts. SPIKE Inspire is one such endeavor providing a wide spectrum of engineering and artistic edifice, swaying from serious thinking to playful inventiveness. The inspiring women students at GVPCEW are brimming with zeal for life empowering themselves with skills and creativity.

I am happy that there is a dedicated team of staff and students who have brought out ***SPIKE-IQ 2K18***. They have presented the stupendous achievements of IT students of GVPCEW in the field of academics, sports and extra- curricular activities.

I extend my heartiest congratulations to the editorial board and all those who have shelved their valuable time to elevate this magazine to unprecedented heights. I wish the readers have a delightful reading. May all our students soar high in uncharted skies and bring glory to the world and their profession with the wings of education.

-Dr.K.V.S.Rao

FROM THE EDITORIAL DESK

It gives an immense joy and satisfaction to introduce our very own department magazine-SPIKE INSPIRE-2K18. Here comes 'SPIKE -IQ 2K18', the magazine of GVPCEW from the IT department. The name of the magazine may see peculiar, but it just means 'the speed at which the technological innovation or advancement is occurring'. So this time, it is the dedication of students, which attempts to bring out the talent concealed within our student community along with teachers. The willingness to share knowledge, concerns and special insights with fellow beings has made this magazine possible. This magazine includes technical articles, biography of a renowned scientist as well as facts regarding computer science, few tricky puzzles with funny corner and exhibits the literary skills and the achievements of students. These contributions have required a generous amount of time and effort. Thank you very much for all the editorial team members who worked for this magazine. It is very glad to take the opportunity of expressing our considerable appreciation to all the contributors of this magazine. Lastly, the contributors and readers of 'SPIKE–IQ 2K18' are always welcome to send us your invaluable feedback and ideas for further improvement of this magazine.

Department Vision:

The department of IT strives to produce competent professionals who are technically sound and ethically strong for IT industry.

Department Mission:

- Provide quality training that prepares Students to be technically component for the Industrial and Societal needs.
- Facilitate an environment that promotes continuous learning to face the challenges in the IT sector.
- Provide opportunities for learning, leadership and communication skills.

Program Educational Objectives:

After successful completion of the program, the graduates will be able to:

- PEO-1: Apply analyze and solve complex Engineering problems using Emerging IT technologies with the help of fundamental knowledge in mathematics, science, and engineering.
- PEO-2: Comprehend Analyze, Design and Create innovative computing products and solutions for real life problems.
- PEO-3: Inculcate the necessary skills to engage in lifelong learning.

Program Specific Outcomes:

Engineering graduates will be able to:

- PSO-1: Develop Software Application s by analyzing, designing and implementing with cutting edge technology to address the needs of IT industry.
- PSO-2: Apply the knowledge of Data Science, machine learning, image processing and allied areas to obtain optimized solutions for real time problems.

FACULTY ARTICLE

Steganography and an Application on Hiding Encrypted Text (RSA Cryptosystem) Using HSI Colour Model using Image Steganography

Dr. Dwiti Krishna Bebarta

Head of the Department IT

Image Steganography refers to hiding information i.e. text, images or audio files in another image or video files. The main objective is sender to send the message in secured way to the receiver using combination of methods like Cryptography and Steganographic methods. By using this hybrid approach one can hide information from others to achieve extra security. This article presents a novel approach of Steganography to hide data in the i-plane of the image and RSA algorithm is used to encrypt the given text. Once the encryption process is done the sender can send the image to the receiver and the receiver can complete the decryption process.

1. Steganography

Definition

Steganography is the art and science of indiscernible communication i.e. data is hidden within the data. Steganography techniques can be applied to images, a video file or an audio file.

Types of Steganography

Almost all digital file formats can be used for Steganography, but the formats that are more suitable are those with a high degree of redundancy is depicted in figure-1. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

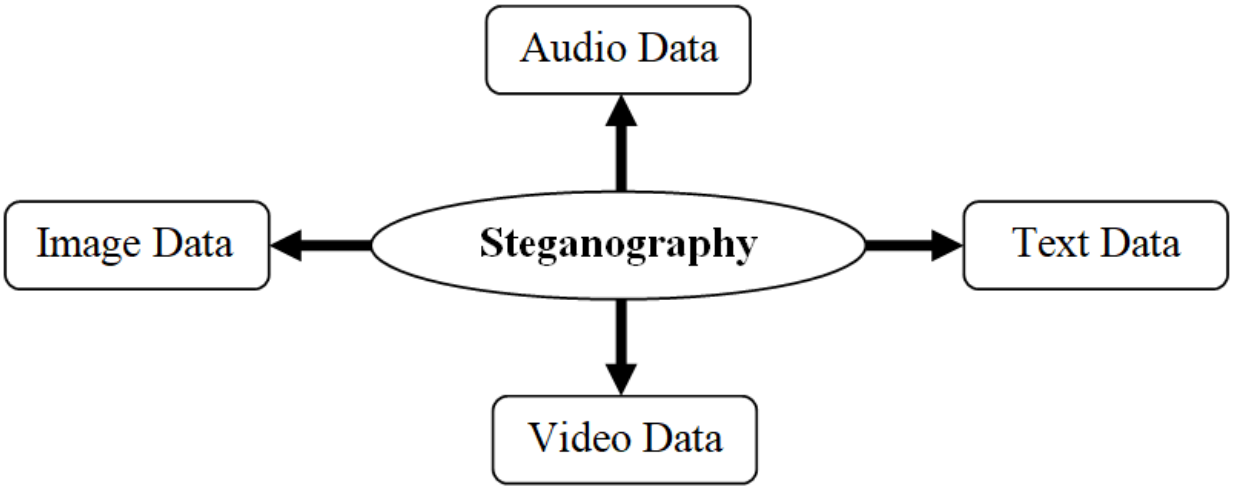


Figure-1: Types of Steganography

Text Steganography

Text Steganography can be achieved by altering the text format, or certain characteristics of textual elements i.e. characters present in the text. The goal in the design of coding methods is to develop alterations that can be decoded even in the presence of noise. The three coding techniques that can be used either separately or jointly. Each technique enjoys certain advantages or applicability is discussed below.

i. **Line-Shift Coding**

This is a method of altering a document by vertically shifting the locations of text lines to encode the document uniquely. This encoding may be applied either to the format file or to the bitmap of a page image.

ii. **Word-Shift Coding**

This is a method of altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely. This encoding can be applied to either the format file or to the bitmap of a page image.

iii. **Feature Coding**

This coding method is applied either to a format file or to a bitmap image of a document. The image is examined for chosen text features, and those features are altered, or not altered, depending on the codeword. Decoding requires the original image, or more specifically, a specification of the change in pixels at a feature.

Image Steganography

Hiding information inside images is a popular technique at the present time. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of Steganography in newsgroups has been researched by German steganographic expert Niels Proves, who created a scanning cluster, which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of Steganography still seems to be limited. To hide a message inside an image without changing its visible properties, the cover source can be altered in ”noisy” areas with many color variations, so less attention will be drawn to the modifications. The universal method is to make the alterations using least-significant bit (LSB) masking, filtering and transformations on the cover image.

Least Significant Bits

A simple approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest Steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies.

Audio Steganography

In audio Steganography, secret message is embedded into digitized audio signal, which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio Steganography.

i. **LSB Coding**
   Sampling technique followed by Quantization converts analog audio signal to digital binary sequence. In this technique, LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.

ii. **Phase Coding**

   Human Auditory System (HAS) cannot recognize the phase change in audio signal as easy it can recognize noise in the signal. The phase coding method exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to- noise ratio.

iii. **Spread Spectrum**

   There are two approaches are used in this technique: the direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). Direct-sequence spread spectrum (DSSS) is a modulation technique used in telecommunication. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated.

iv. **Echo-Hiding**

   In this method, the secret message is embedded into cover audio signal as an echo. Three parameters of the echo of the cover signal namely amplitude, decay rate and offset from original signal are varied to represent encoded secret binary message. They are set below to the threshold of Human Auditory System (HAS) so that echo cannot be easily resolved. Video files are generally consists of images and sounds, so most of the relevant techniques for hiding data into images and audio are also applicable to video media. In the case of Video Steganography sender sends the secret message to the recipient using a video sequence as cover media.

HSI COLOR MODEL

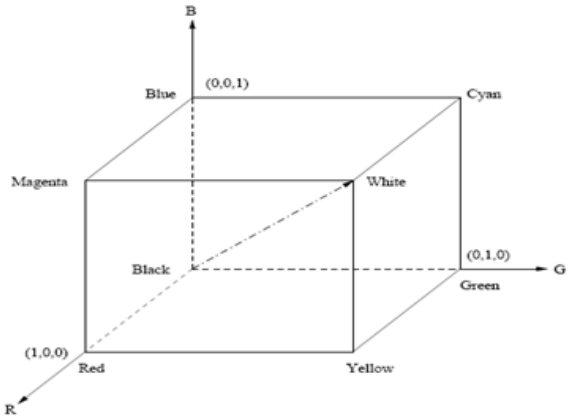
The HSI (hue, saturation, intensity) color model decouples the intensity component from the color-carrying information (hue and saturation) in a color image. The HSI model is an ideal tool for developing image-processing algorithms based on color descriptions that are natural and intuitive to humans.

Hue: A color attribute that describes a pure color.

Saturation: Gives a measure of the degree to which pure color is diluted by white light.

Brightness: A subjective descriptor that is practically impossible to measure.

Conceptual relation between RGB and HS



CMY Model

CMY (cyan-magenta-yellow) model asks what is subtracted from white.

$$\begin{pmatrix} C \\ M \\ Y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} R \\ G \\ B \end{pmatrix}.$$

(RGB Model)

I. The hue is determined by the dominant wavelength

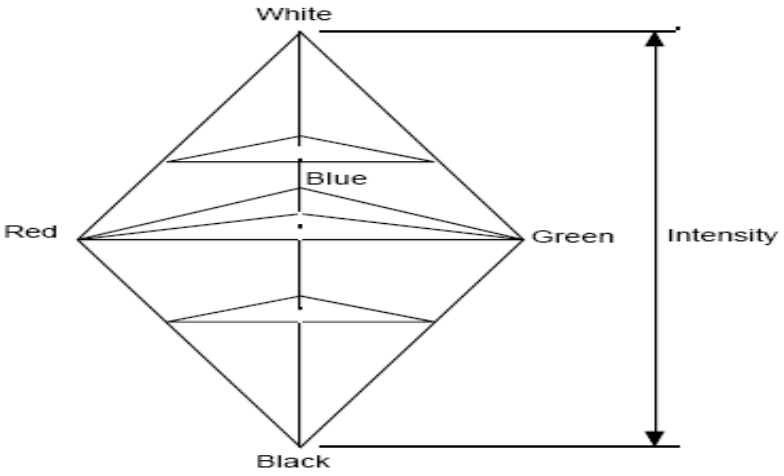
$$H = \cos^{-1}\left(\frac{\frac{1}{2}[(R-G)+(R-B)]}{[(R-G)^2+(R-B)(G-B)]^{1/2}}\right)$$

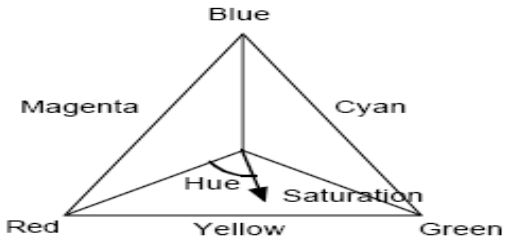
II. The saturation is determined by the excitation purity, and depends on the amount of white light mixed with the hue

$$S = 1 - \frac{\min(R,G,B)}{I} = 1 - \frac{3}{R+G+B}\min(R,G,B)$$

III. the intensity is determined by the actual amount of light

$$I = \frac{R+G+B}{3}$$





1. Cryptography

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

Features of Cryptography:

Confidentiality:
Information can only be accessed by the person for whom it is intended and no other person except him can access it.

Integrity:
Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

Non-repudiation:
The creator/sender of information cannot deny his or her intention to send information at later stage.

Authentication:
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types of Cryptography

Symmetric key:

The sender and receiver exchange messages using a single common key to encrypt and decrypt the messages. It is faster and simpler but the sender and receiver must have to exchange key in a secure manner. The popular symmetric key methods are Data Encryption System (DES), Advance Encryption Symmetric (AES), etc.

Asymmetric Key:

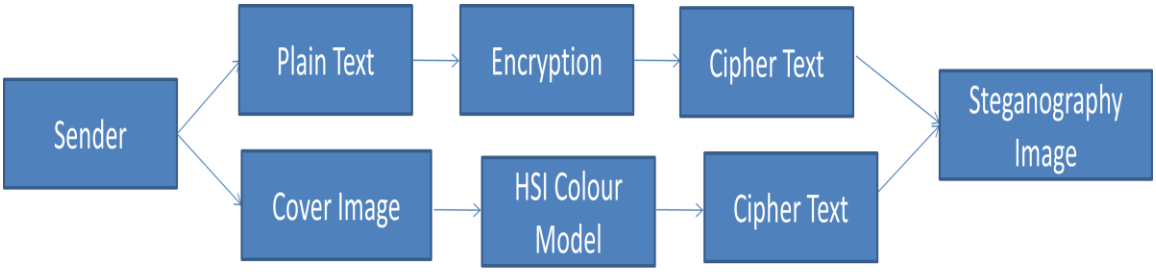
A pair of keys is used to encrypt and decrypt messages. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everybody and the intended receiver can decode it because he only knows the private key. The popular Asymmetric key method is **RSA** (**Rivest–Shamir–Adleman**) algorithm

Hash Functions:

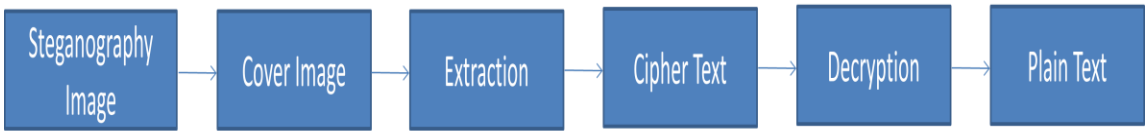
A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords. There is no usage of any key in these algorithms.

2. Design of Proposed Application

Sender Process



Receiver Message



Steps to implement the process at sender and receiver side

- Encrypting the data using RSA algorithm
- Embed the cipher text to the image using HSI color mode
- Send the image
- Receive the image
- Retrieve the secret data from image
- Decrypt the cipher text using RSA algorithm

Results

Cover Image

Stego image

Conclusion

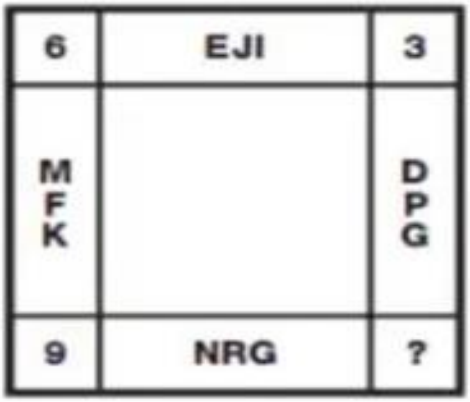
An image steganographic approach for hiding encrypted text (RSA cryptosystem) using HSI color model is designed to satisfy the user goals i.e. to hide the data in a very secure way so that except sender and receiver no one can know what is hidden inside the image. Steganography is a process of hiding the text in a image and cryptography is the process of encrypting and decrypting the text using the public key and private key. This hybrid approach is designed and implemented for achieving greater security than implementing the approach of cryptography and **Steganography** separately

Reference

1. Khan Muhammad. Jamil Ahmad, Haleem Farman, Muhammad Zubair “A Novel Image Steganographic Approach For hiding Text In Colour Images Using HSI Colour Model”.
2. M. Hussain and M. Hussain, "A Survey of Image Steganography Techniques," International Journal of Advanced Science & Technology, vol. 54, 2013.
3. Gandharba Swain and Saroj Kumar Lenka "LSB Array Based Image Steganography Technique by Exploring the Four Least Significant Bits".
4. Rafel C. Gonzale and Richard E. Woods “Digital Image Processing” 2nd edition.
5. Luis von Ahn and Nicholas J. Hopper “Public-key Steganography”.

PUZZLES:

Which number replaces the question mark?



A.15 B.12 C.9 D.6

Answer & Explanation:

Answer : 12

Explanation :

The value at each corner of the diagram equals the sums of the numerical values of the letters in the bc corner.

STUDENT ARTICLES

Plastic hitches a ride on rain, snow, and wind to pollute the whole planet

M. MANASA, 18JG1A1225, Department of IT

Gayatri Vidya Parishad College of Engineering for Women

You have probably already heard that micro plastics have made their way into our soil, oceans, poop, and even beer. Now, scientists have found that these tiny bits of plastic can even infiltrate our air—which carries them off to invade even the wildest corners of the Earth.

Researchers from the University of Strathclyde in Scotland and Ecolab in France spent five months collecting plastic fibres in some of the highest reaches of the Pyrenees mountain range, a string of peaks that separate France and Spain. The team found that rain, snow, and wind carried micro plastics at least 60 miles to this remote ecosystem previously thought to be free of garbage. This is just the beginning' hitchhiking particles like these could potentially travel thousands of miles. The threat they pose is two-fold.

"Atmospheric transportation enables the movement of microplastic away from its pollution source to otherwise clean environments," says Steve Allen, a researcher at the University of Strathclyde, who co-authored the study with his wife, Deonie, a researcher with Ecolab. Animals, including humans, can also breathe them in.

Micro plastics are basically everywhere. They flake off our synthetic clothing materials and wash down the shower drain in the form of exfoliating beads; they are flecks of paint and remnants of weathered plastic bottles. Some are as thick as a couple pieces of spaghetti while others, called nanoplastics, are microscopic. It is easier for the atmosphere to carry these

Extra-tiny particles long distances, to places like the top of the Pyranese mountain range.

Although this new research sheds light on just how far these bits of pollution can travel, airborne microplastic is not a novel phenomenon. In 2018, researchers at Heriot-Watt University estimated that the average U.K. citizen consumes more than 10,000 microplastic particles every year through household dust alone.

A 2017 study found plastic fibres in Parisian air, both outdoors and inside buildings—the air inside your home likely has more plastic floating around in it than even urban outdoor environments, because of

The abundance of sources and lack of ventilation. At the time, scientists speculated that the particles themselves could cause tiny cuts in the lungs, and that the chemicals they encase could trigger long-term illness in humans.

It is likely that all of us inhale fibres, but not all will suffer negative consequences from this exposure High concentrations could pose an occupational hazard to people who work under poorly-ventilated conditions, but we're not sure to what extent as research on the topic is thin. While human impact is still murky, current findings tend to agree on one thing: globetrotting micro plastics will very likely impact wildlife. Water—bound plastic already work their way through marine animals' digestive systems and can hinder their ability to reproduce. When airflow carries plastics, too far off places—like nearly 4,700 feet above sea level, the elevation of the Pyranese study site— virtually every habitat on the planet, no matter how remote, is susceptible to pollution. Scientists now need to figure out how far micro plastics travel, where they are coming from, and where they are landing. One thing is certain: the

problem is not likely to disappear anytime soon. The world produces roughly 370 million tons of plastic every year, the same weight as around 2.5 million blue whales. More than 90 percent of what we produce is not recycled, meaning we burn it, send it to landfills, or dump it into the ocean. Scientists have documented plastic pollution for decades, but this new information shows it's even worse than we thought: it's not just in our water and sneaking up our food chains, but drifting through the wind in our most pristine natural environments.

Review on Mitigation of Security Threats in Wireless Networks

V. B. Tripura Sundari, P.S.S. Sushmita, K. Sravani

(17JG1A1251, 17JG1A1243, 17JG1A1231)
DEPARTMENT OF IT, 3rd YEAR

Gayatri Vidya Parishad College of Engineering for Women

ABSTRACT-

Wireless network is a modern technology that offers deep protection for flawless and high-speed communication enabling future- oriented applications for both the community and military with low cost and adaptability. Anyways, in the calculation of resource capability of the sensor nodes are limited by the insufficiency and intrinsic features of the main sensor network in compared to present networks, and wireless networks have more security threats. The main aim of this review paper is to investigate security concerns and problems in wireless sensor networks. It also summarizes both sides of wireless networks that should be pointed out for the research investigation progress and study of wireless security issues.

KEYWORDS:

access point, set identifier, Open system authentication, shared key authentication, wired equivalent privacy protocol.

1. INTRODUCTION

Presently, wireless communication is omnipresent across the globe. It has a wide- spread existence and role all over the world irrespective of the field it is being used. It is an essential part of space stations, agriculture, office, business, institutions, intelligence organizations, government organizations, firms, etc. In brief, wireless networks are being highly used both in the domestic sector and social sectors. Keeping in view the intense use of wireless connections, one can't ignore the inhibit security threats that are always in the active state to attack the wireless networks. on the contrary, certain technologies have been developed to mitigate these security threat issues. Some of the basic elements of a wireless network are briefly presented in this section. Basic technologies are outlined. This is followed by a discussion on some important attacks resulting in high risks.

1.1 Wireless Local Area Network (WLAN)

High-frequency values of radio waves are used as the medium to perform wireless communications among peers in this type of networks [1]. A typical illustration of a WLAN with a single router is shown in Fig.1.

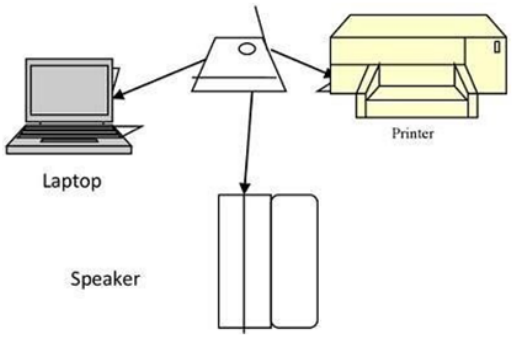


Fig.1. A typical WLAN connection

1.2. Access Point: Specifically known as the wireless access point that helps the user in connecting to a network, thereby send and receive data signals. It is also called a transceiver as it performs both the operation of transmission and receiving of the signal. It acts as a wall between both wireless, wired network. it is a kind of hardware device which allows connecting all kinds of devices.

1.3. Service Set Identifier (SSID):

It is a set of symbols that uniquely refer o a particular wireless network. We can assume as if it is the name of a network Using this SSID various stations can connect to the required network in a scenario where numerous networks are operating in the system.

1.4. Open System Authentication (OSA):

This one is the dedicated protocol giving rise to a communication token whenever an authentication request is made through a network. It is also as per the IEEE standard. By default, it is an open system and can be customized up to an extent. The token generated by this compulsorily contains station identifier (ID). This protocol is also responsible for generating the response token. This is why it falls under the mutual authentication mechanism. The success or failure of data transmission is acknowledged by OSA. It is generally used with the WEP (Wired Equivalent Privacy) for providing secure communications. The OSA enables a system to receive and send data through wireless modem without any encryption. The General block diagram of an OSA is represented in Fig. 2.

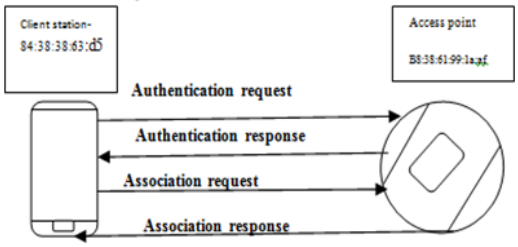
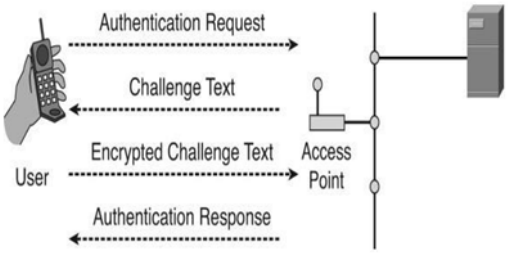


Fig- 2. Open authentication system.

1.5. Shared Key Authentication: This is a response mechanism that is accomplished with the help of WEP. So far, this has been a challenge and researchers are still working towards a complete sharing authentication process. As of now, a sharing key is being used for the same with a prior request from end-users. It is suggested that a standard- free communication should be established while doing shared key authentication. For example, the password a user gives as input to have access to work with a Wi-Fi network.Implementation of the same (Fig.3) is listed below-1. A User seeking the wireless access inputs an identity with an authentication request to the access point.

2. A challenging string is sent by the access point to the client.
3. Upon acknowledging the challenge string, the client connects to the access point.

Fig.3. Representing shared key authentication.



1.6. Infrastructure Mode: In Infrastructure mode (Fig. 4), wireless devices can commune with each other or by the wired network such as modems and all. When one access point is connected to a wired network and some set of wired networks then this is referred to as a Basic Service Set (BSS). Extended Service Set(ESS) is of more BSS from a single network. Most private z wireless Lans work in infrastructure mode because they have required access to the wired LAN in order to use services such as file system or printers.

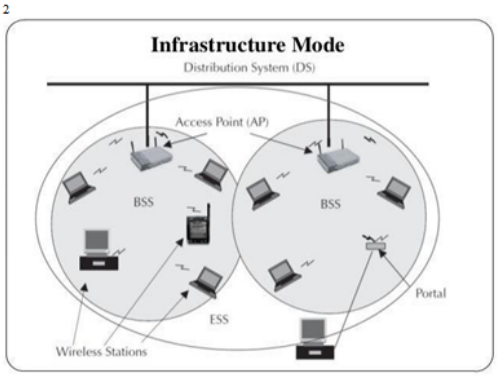


Fig.4. Infrastructure mode analysis

1.7. Wired Equivalent Privacy Protocol (WEP):

This protocol has been benchmarked in the IEEE Wireless fidelities and constituent standards (802.11B). This protocol comes in line with a general WLAN that has a standard level of securities, and authentications

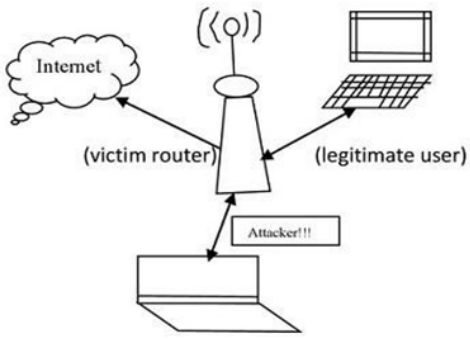


Fig.5. Intercepts the communication between the legitimate user and router.

However, certain flaws have been identified in WEP which has deemed the used of the same presently because of the short time de-authentication of its key strings.

II. THREATS AND RISKS

Various threats and risks for wireless networks are listed below and discussed in a sequence.

1. Attacks in mobile environment
2. Denial of attacks
3. Weak IV attack

2.1. Attacks in Mobile Environment –

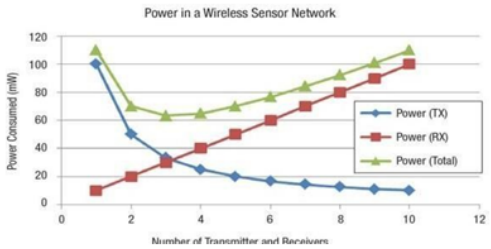
To compromise security protocols many ingenious attacks have developed. These attacks results can span from a mild difficulty to severe methods of security. So, if they are not unsuccessful they can take the processing resources of the attacked party and thus reduce the deep pockets available speak others. It is difficult to reduce the general problem with wireless communications is that attacks transmit over the network. Most of the wireless access points have the ability to log traffic and connections. In a wired network, the attacker must physically "click" to a network. Standard measures can be acquainted with reducing the network accessing, such as constricted building access or locked communication, and upon finding and locating a tap, it can be very easily removed. This same property does not there in a wireless network. [9].The attacks described in the following sections are particularly troublesome in wireless communications because they are easy to execute.

2.2. Denial of Service Attacks

Denial of Service (DoS) is generated by unintended nodes or malicious errors. The simplest DoS attack attempts to take the abundant network users from accessing the service or resource. A DoS attack is meaningful for every incident where an adversary not only tries to destroy, destroy a network but also degrades its ability to deliver services. Multiple categories of DoS attacks can be executed on multiple layers in a wireless network. DoS attacks at the physical layer can be disturbed and tampered within the link layer, collision, consumption, unfair, network layer, ignore and greed, homing, false alarms, black holes, and transport layer. Mechanisms to avoid DoS attacks take account of expense for network sources, pushback, tough authentication, and traffic identification. A precaution to defend against jamming is to recognize the jam in the sensor network and effectively route the unavailable parts. To handle jamming at the MAC layer the node can use MAC admission control, which is a rate constraint. This allows the network to ignore requests that are designed to consume power conservation of the node. However, this method is certainly not secure because the network has to be able to legitimately handle large traffic volumes (Refer to Table 1).

Dos Attacks preventi on	https://www.researchgate.net/figure/Comparison-table-for-DoS-attack-prevention-techniques_tbl1_300080039
Dos Attack s reason S	https://zeltser.com/reasons-for-denial-of-service-attacks/

While we discuss 3G and 4G wireless, from the year 2012-2017. It has been increased to7000millions. And now coming to the cellular and Wi-Fi networks Average data users on Wi-Fi are more than Mobile data consumption. So we can understand that most of the people are showing interest in the wireless networks only. 96% globally, 128% in developed countries, 89% in developing countries. This is one of the basic data or rather we can say the survey proved that 4%Wi-Fi is used more. US Wireless industry is valued at $195.5 billion publishing, also in agriculture, and hotels and lodging, as in air transportation, and also in moving picture and recording. Wireless industry indirectly/directly provides more than 2.6% of all the US employment, as wireless revenue is expanding (Fig. 7).



2.3. The Weak IV attack

Some IV's do not work well with RC4.Using a formula; one can take a weak IV and infer part of the WEP key. Once again, passively monitoring the network for a few hours can be enough time to gather enough weak IV's to figure out the WEP key. Airport and varients use this attack.

Table 2- Summary of different Security Methods applied to Wireless Sensor Networks

Security method	Attacks	Network architecture	Main characteristics
JAM [12], [13]	DoS	Traditional WSN.	Uses linked neighboring nodes prevent the avoidance of the jammed region.
Based on Wormhole [14]	DoS	Hybrid network	Uses Wormholes to avoid it
Random key predistribution, radio resource testing, etc.	Sybil attack	A Large number of sensors. Highly dense wireless network	Uses radio resources, random key pre-distribution, registration procedure, verification of position, and code testing for detecting the Sybil entity.

111. EXISTING SECURITY APPROACHES

This section details the various existing security mechanisms proposed to protect against attacks. These technologies are used in other layers such as "physical layer", "data link layer", "network layer"," transport layer" and "application layer". [6].Below is a review of the protocol with prominent features. In current years, the search for symmetric ciphers has not stopped wireless network authentication. Qiu et al. recommended a proficient extensible authentication protocol that can update an authentication key based on a dynamically changing wireless network where there is at slightest one likelihood of a contribution to key among two nodes [7].

An efficiency time-based stream authentication protocol that allows loss packages. The main contribution of TESLA is the use of symmetric key technology to accomplish asymmetric cryptography, and the key idea is to accomplish irreversible broadcast authentication using key allotment delays and one-way hash methods.[4] TTESLA first broadcasts the packet through key authentication and then releases the key. The irreversibility of a one-way hash function is nothing because it guarantees that no one can get the statistics authentication key before publishing the key How to fake the correct transmit packet before the broadcast packet is authenticated.

1V. INTENDS AND SCOPE FOR FUTURE RESEARCH

In current years, we have accomplished many achievements in wireless network security. However, security and network applicability still have many disadvantages. Based on the analysis and summary of WSN security research above, this section presents some views on future research on three aspects of key management, authentication, and secure routing.

V. CONCLUSION

Most attacks on the security of wireless networks are caused by the inclusion of bad information by corrupted nodes in the network. We need a way to detect false reports to prevent corrupted nodes from containing false descriptions. However, the development of mechanisms such as findings and make them more effective is a major challenge. Once more, guarantee holistic security in wireless networks is a most important consideration for the challenge. Many security schemes proposed today are based on specific network models. Because there is not enough effort to use a common model to ensure security for each tier, security mechanisms will be well established for each tier, but in the future, we will combine all the mechanisms to work together. It causes difficult research tasks. Although holistic security can be assured in wireless networks, the cost efficiency and energy efficiency of using these mechanisms can continue to be a key argument in the future.

VI. REFERENCES

[1]. Q. Yang, X. Zhu, H. Fu, and X. Che, "Survey of Security Technologies on Wireless Sensor Networks", Hindawi Journal of Sensors, Volume 2015.

[2]. K. Ren, S. Yu,W. Lou, and Y. Zhang, "PEACE: a novel

privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks", in IEEE Transactions on Parallel and Distributed Systems, Vol.-21, No 2, pp. 203–215, February 2010.
[3]. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", in Proceedings of the 9th ACM Conference on Computer and Communications Security, pp.41– 47, November 2002.

[4]. H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks", in Proceedings of the IEEE Symposium on Security and Privacy, pp. 197–213, Washington, DC, USA, May 2003.
[5]. K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: a novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks", in IEEE Transactions on Parallel and Distributed Systems, Vol.-21, No 2, pp. 203– 215, February 2010[6]. W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography", International Journal of Distributed Sensor Networks, vol.2013.
[7]. J. J. Li, L.Tan and D. Y. Long, "A new key management and authentication method for WSN based on CPK", in Proceedings of the International Colloquium on Computing, Communication, Control, and Management, Vol.2,pp.486–490, Guangzhou, China, August 2008.
[8]. Bird, R., et al., "Systematic Design of a Family of Attack-Resistant Authentication Protocols," IEEE Journal on Selected Areas in Communications, Vol. 11, No. 5, 1993, pp.
[9]. Samrat, D., R. Molve, and N. Asokan,"Untreacibility in Mobile Networks," Proc. Of ACM Int. Conf. on Mobile Computing and Networking, Berkeley, CA, November 1995.
[10]. D. S. Alberts, J. J. Garska, and F. P. Stein. (1999) Network Centric Warfare: Developing and

Analysis on Augmented Reality: Limitations and Technologies evolving

K.Sravani, 17JG1A1231

Department of IT, 3rd year

Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam

Abstract: We are on the verge of ubiquitously adopting Augmented Reality (AR) technologies to enhance our perception and help us see, hear, and feel our environments in new and enriched ways. AR will support us in fields such as education, maintenance, design and reconnaissance, to name but a few. This paper describes the field of AR, the enabling technologies and their characteristics. And how it is being useful in field of education It surveys the state of the art by reviewing some recent applications of AR technology as well as some known limitations regarding human factors in the use of AR systems that developers will need to overcome.

Keywords: augmented reality, technologies, aural displays, limitations

1. INTRODUCTION:

Imagine a technology with which you could see more than others see, hear more than others hear, and perhaps even touch, smell and taste things that others can not. What if we had technology to perceive completely computational elements and objects within our real world experience, entire creatures and structures even that help us in our daily activities, while interacting almost unconsciously through mere gestures and speech? With such technology, mechanics could see instructions what to do next when repairing an unknown piece of equipment, surgeons could see ultrasound scans of organs while performing surgery on them, fire fighters could see building layouts to avoid otherwise invisible hazards, soldiers could see positions of enemy snipers spotted by unmanned reconnaissance aircraft, and we could read reviews for each restaurant in the street were walking in, or battle 10-foot tall aliens on the way to work Augmented reality (AR) is this technology to create a "next generation, reality-based interface" and is moving from laboratories around the world into various industries and consumer markets. AR supplements the real world with virtual (computer-generated) objects that appear to coexist in the same space as the real world. AR was recognized as an emerging technology of 2007, and with today's smart phones and AR browsers we are starting to embrace this very new and exciting kind of human-computer interaction

II. ENABLING TECHNOLOGIES

The technological demands for AR are much higher than for virtual environments or VR, which is why the field of AR took longer to mature than that of VR. However, the key components needed to build an AR system have remained the same since Ivan Sutherlands pioneering work of the 1960s. Displays, trackers, and graphics computers and software remain essential in many AR experiences. Following the definition of AR step by step, this section first describes display technologies that combine the real and virtual worlds, followed by sensors and approaches to track user position and orientation for correct registration of the virtual with the real, and user interface technologies that allow real-time, 3D interaction. Finally some remaining AR requirements are discussed.

2.1 Displays

Of all modalities in human sensory input, sight, sound and/or touch are currently the senses that AR systems commonly apply. This section mainly focuses on visual displays, however aural (sound) displays are mentioned briefly below. Haptic (touch)

displays are discussed with the interfaces in Section 2.3, while olfactory (smell) and gustatory (taste) displays are less developed or practically non-existent AR techniques and will not be discussed in this essay.

2.2 Aural display

Aural display application in AR is mostly limited to self-explanatory mono (0-dimensional), stereo (1-dimensional) or surround (2-dimensional) headphones and loudspeakers. True 3D aural display is currently found in more immersive simulations of virtual environments and augmented virtuality or still in experimental stages. Haptic audio refers to sound that is felt rather than heard and is already applied in consumer devices such as Turtle Beach's Ear Force5 headphones to increase the sense of realism and impact, but also to enhance user interfaces of e.g. mobile phones. Recent developments in this area are presented in workshops such as the international workshop on Haptic Audio Visual Environments6 and the international workshop on Haptic and Audio Interaction Design.

III. LIMITATIONS

AR faces technical challenges regarding for example

binocular (stereo) view, high resolution, color depth, luminance, contrast, field of view, and focus depth. However, before AR becomes accepted as part of users everyday life, just like mobile phones and personal digital assistants (PDAs), issues regarding intuitive interfaces, costs, weight, power usage, ergonomics, and appearance must also be addressed. A number of limitations, some of which have been mentioned earlier, are categorized here. 4.1 Portability and outdoor use Most mobile AR systems mentioned in this survey are cumbersome, requiring a heavy backpack to carry the PC, sensors, display, batteries, and everything else. Connections between all the devices must be able to withstand outdoor use, including weather and shock, but universal serial bus (USB) connectors are known to fail easily. However, recent developments in mobile technology like cell phones and PDAs are bridging the gap towards mobile AR. Optical and video see-through displays are usually unsuited for outdoor use due to low brightness, contrast, resolution, and field of view. However, recently developed at Micro Vision, laser-powered displays offer a new dimension in head-mounted and hand-held displays that overcomes this problem. Most portable computers have only one CPU which limits the amount of visual and hybrid tracking. More generally, consumer operating systems are not suited for real-time computing, while specialized real-time operating systems don't have the drivers to support the sensors and graphics in modern hardware. 4.2 Tracking and (auto)calibration Tracking in unprepared environments remains a challenge but hybrid approaches are becoming small enough to be added to mobile phones or PDAs. Calibration of these devices is still complicated and extensive, but this may be solved through calibration-free or auto-calibrating approaches that minimize set-up requirements. The latter use redundant sensor information to automatically measure and compensate for changing calibration parameters. Latency A large source of dynamic registration errors are system delays. Techniques like pre calculation, temporal stream matching (in video see-through such as live broadcasts), and prediction of future viewpoints may solve some delay. System latency can also be scheduled to reduce errors through careful system design, and pre-rendered images may be shifted at the last instant to compensate for pan-tilt motions. Similarly, image warping may correct

delays in 6DOF motion (both translation and rotation). 4.3 Depth perception One difficult registration problem is accurate depth perception. Stereoscopic displays help, but additional problems including accommodation-vergence conflicts or low resolution and dim displays cause object to appear further away than they should be Correct occlusion ameliorates some depth problems , as does consistent registration for different eye point locations In early video see-through systems with a parallax, users need to adapt to vertical displaced viewpoints. In an experiment by Biocca and Roll and, subjects exhibit a large overshoot in a depth-pointing task after removing the HMD. 4.4 Overload and over-reliance Aside from technical challenges, the user interface must also follow some guidelines as not to overload the user with information while also preventing the user to overly rely on the AR system such that important cues from the environment are missed At BMW, Bengler and Passaro use guidelines for AR

system design in cars, including orientation on the driving task, no moving or obstructing imagery, add only information that improves driving performance, avoid side effects like tunnel vision and cognitive capture, and only use information that does not distract, intrude or disturb given different situations. 4.5 Social acceptance Getting people to use AR may be more challenging than expected, and many factors play a role in social acceptance of AR ranging from unobtrusive fashionable appearance (gloves, helmets, etc.) to privacy concerns. For instance, Accenture's Assistant (Fig. 14) blinks a light when it records for the sole purpose of alerting the person who is being recorded. These fundamental issues must be addressed before AR is widely accepted .

IV.CONCLUSION

We surveyed the state of the art of technologies, applications and limitations related to augmented reality. AR has come a long way but still has some distance to go before industries, the military and the general public will accept it as a familiar user interface. On the other hand, companies like Information in Place estimated that by 2014, 30% of mobile workers will be using augmented reality. Within 5-10 years, Feiner believes that "augmented reality will have a more profound effect on the way in which we develop and interact with future computers." With the advent of such complementary

technologies as tactile networks, artificial intelligence, cybernetics, and (non-invasive) brain-computer interfaces, AR might soon pave the way for ubiquitous (anytime-anywhere) computing of a more natural kind or even human-machine symbiosis as Licklider already envisioned in the 1950"s.

REFERENCES

[1] ISWC'99: Proc. 3rd Int'l Symp. on Wearable Computers, San Francisco, CA, USA, Oct. 18-19 1999. IEEE CS Press. ISBN 0-7695-0428-0.

[2] IWAR'99: Proc. 2nd Int'l Workshop on Augmented Reality, San Francisco, CA, USA, Oct. 20-21 1999. IEEE CS Press. ISBN 0-7695-0359-4.

[3] ISAR'00: Proc. Int'l Symp. Augmented Reality, Munich, Germany, Oct. 5-6 2000. IEEE CS Press. ISBN 0-7695-0846-4.

[4] ISWC'00: Proc. 4th Int'l Symp. on Wearable Computers, Atlanta, GA, USA, Oct. 16-17 2000. IEEE CS Press. ISBN 0-7695-0795-6.

[5] ISAR'01: Proc. 2nd Int'l Symp. Augmented Reality, New York, NY, USA, Oct. 29-30 2001. IEEE CS Press. ISBN 0-7695-1375-1.

[6] ISWC'01: Proc. 5th Int'l Symp. on Wearable Computers, Zürich, Switzerland, Oct. 8-9 2001. IEEE CS Press. ISBN 0-7695-1318-2.

[7] ISMAR'02: Proc. 1st Int'l Symp. on Mixed and Augmented Reality, Darmstadt, Germany, Sep. 30-Oct. 1 2002. IEEE CS Press. ISBN 0-7695-1781-1.

[8] ISMAR'03: Proc. 2nd Int'l Symp. on Mixed and Augmented Reality, Tokyo, Japan, Oct. 7-10 2003. IEEE CS Press. ISBN 0-7695-2006-5.

[9] ISMAR'04: Proc. 3nd Int'l Symp. on Mixed and Augmented Reality, Arlington, VA, USA, Nov. 2-5 2004. IEEE CS Press. ISBN 0-7695-2191-6.

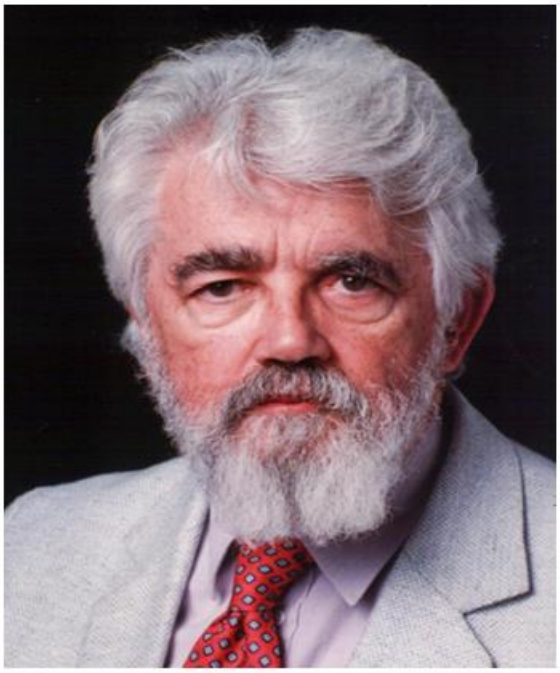
John McCarthy

G. S. S. Khyati Priya, 17JG1A1222, Department of IT, 3rd year

Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam

John McCarthy (September 4, 1927 – October 24, 2011) was an American computer scientist and cognitive scientist. McCarthy was one of the founders of the discipline of artificial intelligence. He coined the term "artificial intelligence" (AI), developed the Lisp programming language family, significantly influenced the design of the ALGOL programming language, popularized timesharing, invented garbage collection, and was very influential in the early development of AI.

McCarthy spent most of his career at Stanford University. He received many accolades and honours, such as the 1971 Turing Award for his contributions to the topic of AI, the United States National Medal of Science, and the Kyoto Prize.



Early life and education

John McCarthy was born in Boston, Massachusetts, on September 4, 1927, to an Irish immigrant father and a Lithuanian Jewish immigrant mother, John Patrick and Ida (Glatt) McCarthy. The family was obliged to relocate frequently during the Great Depression, until McCarthy's father found work as an organizer for the Amalgamated Clothing Workers in Los Angeles, California. His father came from the fishing village of Cromane in County Kerry, Ireland. His mother died in 1957.

McCarthy was exceptionally intelligent, and graduated from Belmont High School two

It was at Caltech that he attended a lecture by John von Neumann that inspired his future endeavours.

McCarthy initially completed graduate studies at Caltech before moving to Princeton University. He received a Ph.D. in mathematics from the institution in 1951 as a student of Solomon Lefschetz.

Academic career

After short-term appointments at Princeton and Stanford University, McCarthy became an assistant professor at Dartmouth in 1955.

A year later, McCarthy moved to MIT as a research fellow in the autumn of 1956.

years early. McCarthy was accepted into Caltech in 1944.

McCarthy showed an early aptitude for mathematics; during his teens he taught himself college mathematics by studying the textbooks used at the nearby California Institute of Technology (Caltech). As a result, he was able to skip the first two years of mathematics at Caltech. McCarthy was suspended from Caltech for failure to attend physical education courses.

In 1962, McCarthy became a full professor at Stanford, where he remained until his retirement in 2000. By the end of his early days at MIT he was already affectionately referred to as "Uncle John" by his students.

McCarthy championed mathematical logic for artificial intelligence.

Contributions in computer science

John McCarthy is one of the "founding fathers" of artificial intelligence, together with Alan Turing, Marvin Minsky, Allen Newell, and Herbert A. Simon. McCarthy coined the term "artificial intelligence" in 1955, and organized the famous Dartmouth conference in summer 1956. This conference started AI as a field. (Minsky later joined McCarthy at MIT in 1959.)

In 1958, he proposed the advice taker, which inspired later work on question-answering and logic programming.

McCarthy invented Lisp in the late 1950s. Based on the lambda calculus, Lisp soon became the programming language of choice for AI applications after its publication in 1960

In 1958, McCarthy served on an ACM Ad hoc Committee on Languages that became part of the committee that designed ALGOL 60. In August 1959 he proposed the use of recursion and conditional expressions, which became part of ALGOL.

Around 1959, he invented so-called "garbage collection" methods to solve problems in Lisp.

He helped to motivate the creation of Project

In 1961, he was perhaps the first to suggest publicly the idea of utility computing, in a speech given to celebrate MIT's centennial: that computer time-sharing technology might result in a future in which computing power and even specific applications could be sold through the utility business model (like water or electricity). This idea of a computer or information utility was very popular during the late 1960s, but faded by the mid-1990s. However, since 2000, the idea has resurfaced in new forms (see application service provider, grid computing, and cloud computing).

In 1966, McCarthy and his team at Stanford wrote a computer program used to play a series of chess games with counterparts in the Soviet Union; McCarthy's team lost two games and drew two games (see Kotok-McCarthy).

From 1978 to 1986, McCarthy developed the circumscription method of non-monotonic reasoning.

In 1982 he seems to have originated the idea of the "space fountain", a type of tower extending into space and kept vertical by the outward force of a stream of pellets propelled from Earth along a sort of conveyor belt which returns the pellets to Earth (payloads would ride the conveyor belt upward).

MAC at MIT when he worked there, and at Stanford University, he helped establish the Stanford AI Laboratory, for many years a friendly rival to Project MAC.

McCarthy was instrumental in creation of three of the very earliest time-sharing systems (Compatible Time-Sharing System, BBN Time-Sharing System, and Dartmouth Time Sharing System). His colleague Lester Earnest told the Los Angeles Times: "The Internet would not have happened nearly as soon as it did except for the fact that John initiated the development of time-sharing systems. We keep inventing new names for time-sharing. It came to be called servers ... Now we call it cloud computing. That is still just time-sharing. John started it.

Awards and honours

- Turing Award from the Association for Computing Machinery (1971).
- Kyoto Prize (1988).
- National Medal of Science (USA) in Mathematical, Statistical, and Computational Sciences (1990).
- Inducted as a Fellow of the Computer History Museum "for his co-founding of the fields of Artificial Intelligence (AI) and timesharing systems, and for major contributions to mathematics and computer science". (1999)
- Inducted into IEEE Intelligent Systems' AI's Hall of Fame (2011), for the "significant contributions to the field of AI and intelligent systems".

STUDENT'S HUB

We know it takes dedication and courage to learn new skills and explore new career opportunities. We are committed to providing you with all the resources and support you need to achieve your learning goals and advance your career.

That is why, today, we are launching the new **Student Hub** experience to all of our existing and new students. The Student Hub provides you with an effective way to connect with fellow students and receive support and guidance from knowledgeable mentors.

Our goal in launching this new experience is to help you acquire valuable and in-demand skills, and to successfully complete you are challenging Nano degree programs. These are intensive programs, and as you proceed through your curriculum, you will need to set ambitious goals, and achieve important milestones. We are excited to offer new resources that will help you do exactly that.

We have had hundreds of conversations with students about their mentorship and community experience at **SPIKE**. We have analyzed years of data to understand which behaviors produced the most successful outcomes for our students. We have experimented, iterated, tested, and trialed a whole range of solutions. In addition, we have created something special for you. Today marks the culmination of a company-wide effort to offer a powerful new set of resources that will help support your learning goals, and power your success.

SPIKE INAUGURATION:

SPORTS

Sport's is very important in everyone's life. Some people will have more passion towards sports and participation in sports should always be encouraged. Participation in sport makes us fit, active and healthy. It will develop our social and communication skills. We can explore to new places and people when we go for an competition. It will teach the importance of time in our life because every minute is important in a game. "Healthy mind lives in Healthy body" is so true because for a man to be successful his physical, as well as mental state should be well. Our college "Gayatri Vidya Parishad" helps their students to prove their strength in sports by encouraging them in several activities such as:

హోరా..హోరీ

- బాల్‌బ్యాడ్మింటన్ జట్టు ఎంపికలు ప్రారంభం
- జీఎమ్మార్ ఇంజనీరింగ్ కళాశాలలో పోటీలు
- నేడు పురుషుల జేఎన్‌టీయూకే జట్టు ఎంపిక

జేఎన్‌టీయూ బాల్‌బ్యాడ్మింటన్ మహిళా జట్టును అభినందిస్తున్న ఫిస్కస్ ప్రసాద్, ఇతర ప్రముఖులు

క్రీడలతోనే మానసిక ఉల్లాసం

STUDENT'S CORNER

Special Talents of students:

1. **Swetha Sree Poosarla** (17JG1A1241) of 3rd IT is a micro artist won **Bharat Gaurav kala shiromani** India's most prestigious award for her chalk art.

2. V. Bala Tripura Sundari (17JG1A1251) of 3rd, IT is a vena artist and classical singer. She is completed her 1st year in **Karnatic Classical** from Hyderabad University with first class.

3. B.Bhavani (16JG1A1208) of 4th IT represented ALL INDIA INTER UNIVERSITY NETBALL TOURNMENT held on February 2019.

4. Priya Bhavana V N Dwaram (18JG1A1241) of 2nd IT is a classical singer. She completed her **diploma** in Karnatic Music with first class in 2018. She received Founder's Day award by Visakha Music and Dance Academy as an **Upcoming Artist Young Talent Award Vocal** on 03/03/2019.

NPTEL Certifications

- **National Program on Technology Enhanced Learning (NPTEL) is to create course contents in engineering and science in order to devise and guide reforms that will transform India into a strong and vibrant knowledge economy.**

Well, many students of Gayatri Vidya Parishad had actively learned and succeeded in their respective courses.

Some of their scores—

1. **K. Pavani(17JG1A1227) of 3rd IT -90% in Introduction to R programming**
2. **E. Vasantha(17JG1A1220) of 3rd IT – 90% in Java Programming**
3. **J. Bavya Sri Sai(17JG1A1226) of 3rd IT – 89% in Java Programming**

Code Chef of GVPCEW:

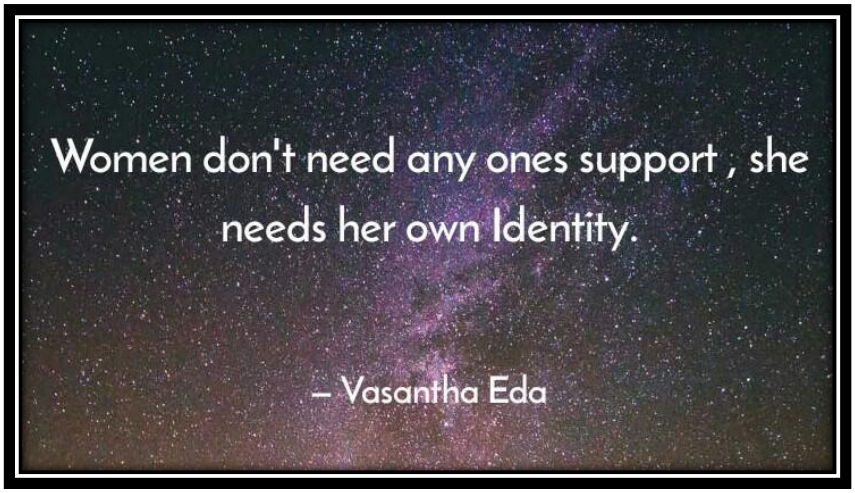
Fourth year IT:

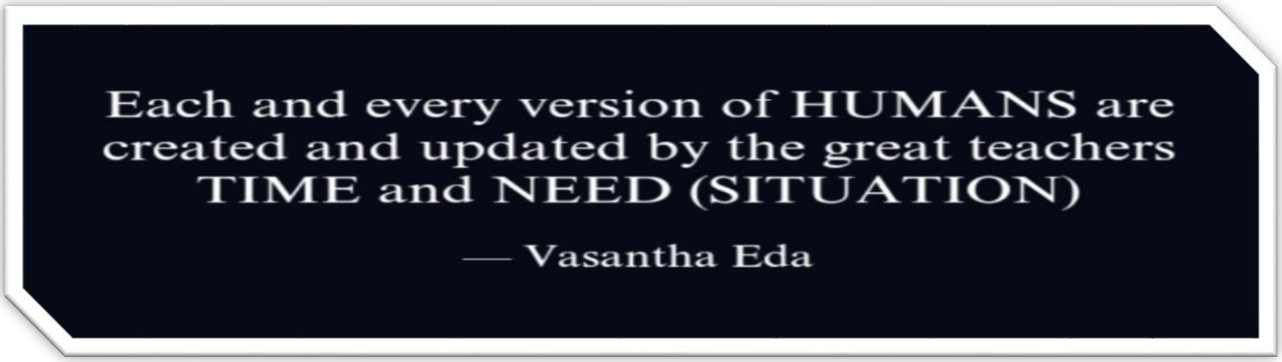
- **Surekha(16JG1A1236) – 24399 hackos**
- **Haritha(16JG1A1242) – 22396 hackos**
- **Kundana (16JG1A1240) - 22000 hackos**
- **Vaibhavi(16JG1A1247) – 20000 hackos**

Third year IT:

- **J. Bavya Sri Sai(17JG1A1226) – 5570 hackos**
- **E. Vasantha(17JG1A1220) – 4363 hackos**
- **P. Sai Prathyusha(17JG1A1236) – 3894 hackos**
- **V. B. T. Sundari (17JG1A1251) - 3805 hackos**

QUOTES BY STUDENT:





SPIKE EVENTS

Spike is our student's hub for IT people; it encourages students to participate in events, cultural activities, coding contests, field visits, etc. To make students to explore on new things and gain knowledge. It will help students to gain communicational skills and coding skills that are very important for a student in life.

Some events were conducted by our spike members are:

Riffle Riddles 1.0:

It is a general competition to test the logical thinking of the students and to make a fun full session with students to interact more.

G. Neha (16JG1A1220) -1st prize

B. Uttara (16JG1a1210) – 2nd prize

CH. Bhavani (17JG1A1214) – 1st prize

J. Bavya Sri Sai (17JG1A1226) – 2nd prize

Codes and coders 1.0:

It is a coding contest for students, participating in this competitions make student's to know there capability in their skills and try to improve their coding by more practice and understanding. To encourage students they take top 2 contestants and gave prizes.

N. Surekha (16JG1A1236) – 1st prize

B. Govindamma (16JG1A1207) – 2nd prize

V. B. T. Sundari (17JG1A1251) - 1st prize

J. Bavya Sri Sai (17JG1A1226) – 2nd prize

Code Hackers 1.0:

It is also a coding contest held by our SPIKE members among all 2nd 3rd and 4th students to make focus on coding and try to solve more problem in hacker rank. The winners are:

P. Aswini Supraja (16JG1A1205)

K. Pavani (17JG1A1227)

M. Manasa (18JG1A1225)

Industrial Visit:

We went to Center of Excellence in Maritime & Shipbuilding (CEMS), it is an institute there they provide courses for some technologies which are using in factories and industries. There we learn new things and got to know about more information about the technology using in industries. There are some courses like robotics, virtual reality, communicational signals and frequencies, etc.

EDITORIAL TEAM