THE CCET ACM TECH MAGAZINE

DIGITAL OUTLET

VOLUME 4 - ISSUE 3
NOV - DEC, 2023

ACM CCET
MOBILE APP

GET IT ON PLAYSTORE

PUBLISHED BY

CCET ACM STUDENT CHAPTER
CCET, DEGREE WING
SECTOR 26, CHANDIGARH

OUR MISSION & VISION

Our Mission is to advance computing education and research, fostering innovation and collaboration globally. Through our bi-monthly digital outlet, we provide a platform for sharing knowledge and addressing societal challenges. We empower individuals within the computing community, promoting excellence and continuous learning.

Our Vision is to lead the forefront of computing's evolution, driving innovation and ethical practices that benefit all. We envision a dynamic global community where collaboration across disciplines sparks transformative solutions to society's most pressing challenges. ACM is committed to championing equitable access to computing's advantages worldwide. Through our magazine and platforms, we aim to inspire and inform, empowering computing professionals with invaluable resources and fostering a future where technology serves humanity's highest aspirations.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

VISION

To produce self-motivated and globally competent technocrats equipped with computing, innovation, and human values for ever changing world and shape them towards serving the society.

MISSION

M1: To make the department a smart centre for learning, innovation and research, creativity, and entrepreneurship for the stakeholders (students/scholar, faculty, and staff).

M2: To inculcate a strong background in mathematical, theoretical, analytical, and practical knowledge in computer science and engineering.

M3: To promote interaction with institutions, industries and research organizations to enable them to develop as technocrats, entrepreneurs, and business leaders of the future.

M4: To provide a friendly environment while developing interpersonal skills to bring out technocrat's inherent talents for their all-round growth.

TABLE OF CONTENTS

A NOTE FROM OUR MENTORS

Our mission at CCET is not only to produce engineering graduates but to produce engineering minds.

Dr. Manpreet Singh
Principal CCET (Degree Wing)

ACM CCET provides student a great opportunity to learn scientific and practical approach of computer science.

Dr. Sunil K. Singh
Professor and HOD, CSE | Faculty Mentor

Every person should be provided with an opportunity to learn and explore the field of computer science.

Er. Sudhakar Kumar
Assistant Professor, CSE | Faculty Sponsor

CCET ACM Student chapter is a group of people with similar interests and goals in computer science. Together, this platform focuses on the growth and development at not only personal but professional level also as it has a unique learning environment.

Saket Sarin
UG Scholar, 5th Semester, CSE | Chairperson, CASC

ACM-W Student Chapter of CCET aims to promote women in technology. As a member of this community, you will have the opportunity to collaborate with others who share similar interests and explore different areas of computing in order to advance in them.

Aishita
UG Scholar, 5th Semester, CSE | Chairperson, CASC-W

CCET ACM STUDENT CHAPTER

Research and Development

Student Speaker Program

Competitive Coding

Designing & Digital Art

Internship and Career Opportunity

ABOUT ACM

ACM boosts up the potential and talent, supporting the overall development needs of the students to facilitate a structured path from education to employment. Our Chapter CASC focuses on all the aspects of growth and development towards computer technologies and various different fields. Overall, we at CCET ACM Student Chapter, through collaboration and engagement in a plethora of technical activities and projects, envision building a community of like-minded people who love to code, share their views, technical experiences, and have fun.

We have been trying to encourage more women to join the computing field, so we started an ACM-W Chapter to increase the morale of women. CASC launched an app which aimed at maintaining decorum of reading among CS members and sharing their ideas.

CCET ACM-W STUDENT CHAPTER

Research and Development

Student Speaker Program

Competitive Coding

Designing & Digital Art

Internship and Career Opportunity

ABOUT ACM-W

The CCET ACM-W was founded in October 2021 with an aim to empower women in the field of computing and increase the global visibility of women in the field of research as well as development. We provide a platform for like-minded people so that they can grow together and contribute to the community in a way that shapes a better world. Our chapter was founded to encourage students, especially women, to work in the field of computing. The chapter's main goal is to create even opportunities and a positive environment for students, where they can work to develop themselves professionally. We at the ACM Student chapter aim to build a globally visible platform where like-minded people can collaborate and develop in their field of interest.

CASC ACHIEVEMENTS

ALL INDIA CYBERTHON 2023

Ruchika Thakur of CSE 3rd Year won the second prize in 4th All India Cyber Thon 2023, conducted by Chandigarh Police Association in collaboration with Infosys.

Certificate of Recognition

PRESENTED TO

Ruchika Thakur

Team: Cyber Ciphers **College:** Chandigarh College of Engineering & Technology, Sector 26, Chandigarh
Project: AI-driven Sentiment Analysis for Community Policing

For winning Second Prize in All India 4th Cyber-Thon 2023, conducted by Chandigarh Police in association with Infosys

Ketan Bansal, IPS
SP, Hqrs & Cyber, Chandigarh

Praveer Ranjan, IPS
Director General of Police Chandigarh

IPD EXPO 2023

Ref No. IIC/IPD/2023/CE/16

INSTITUTION'S INNOVATION COUNCIL

CERTIFICATE

This certificate is awarded to SAHIL GARG, Roll No. _____ of Branch CSE, for securing ~~First~~/~~Second~~/Third position/~~participating~~ in the Innovative Product Design, IPD Expo-2023 (Project Exhibition) held at Chandigarh College of Engineering And Technology (Degree Wing), Sector-26 Chandigarh, on 22nd November 2023.

Dr. Ashwani Kumar, Vice-President - IIC
Dr. D. S. Saini, President - IIC
Dr. M.S. Gujral, Principal CCET (Degree Wing)

The following students from ACM and ACM-W baaged position in Innovative Product Design Expo 2023 held at CCET, Sector 26, chandigarh on 22nd November 2023.

- Sahil Garg [CSE 2022]: 3rd position
- Kanishk Nagpal & Japan Ajit Singh Gandhi [CSE 2021]: 1st position

RESEARCH PAPERS PUBLISHED

- The paper titled "Role of Social Media in Disaster Management using NLP and Deep Learning" , authored by Pooja Rai, Sudhakar Kumar, Sunil K. Singh, Harkiran Kaur, Simran Jaggi, Varsha Arya, and Brij B. Gupta, was accepted in the proceedings of the International Conference on Artificial Intelligence, Computing, IoT and Data Analytics (AICTA-2023). The conference was organized by the Department of Computer Science and Engineering at Punjab Engineering College Chandigarh from December 18-20, 2023.

CASC ACHIEVEMENTS

- The paper titled "Pushing the Boundaries of Mortality Prediction: Advancing High-Risk Sepsis-III Patient Care through Cutting-Edge Deep Learning Techniques," authored by Deepak Mahto, Sunil K. Singh, Sudhakar Kumar, Manya, Rashmi, Varsha Arya, Kwok Tai Chui, Brij B. Gupta, was accepted in the proceedings of the International Conference on Artificial Intelligence, Computing, IoT and Data Analytics (AICTA-2023). The conference was organized by Department of Computer Science and Engineering at Punjab Engineering College Chandigarh from December 18-20, 2023.

- The paper titled "Exploring Advanced Neural Networks for Cross-corpus Fake News Detection," authored by Manya, Sunil K. Singh, Sudhakar Kumar, Deepak Mahto, SUNIL K SHARMA, Varsha Arya, Kwok Tai Chui, Brij B. Gupta, was accepted in the proceedings of the 5th International Conference on Information Management, & Machine Intelligence (ICIMMI-2023). The conference was organized by Poornima Institute of Engineering & Technology, Jaipur, Rajasthan from December 14-16, 2023.

SESSION ON TECHNICAL WRITING - WRITE IT RIGHT

November 4th, 2023

Event Details

On November 4, 2023, the CCET ACM and ACM-W Student Chapters co-hosted an insightful "Introductory Session on Technical Writing - Write it Right." This event aimed to empower participants with an understanding of technical writing's significance across various domains. Serving as a beginner's guide to research paper writing, the session provided practical guidance on navigating Google Scholar and Kaggle

Event Speaker

Aishita Sharma, the knowledgeable speaker of the event, shared valuable insights and practical tips to demystify the world of technical writing and equip participants with the skills needed for effective communication in a technical context. The collaborative effort of both student chapters ensured an enriching experience for all participants

Aishita Sharma
CO21305, CSE 2021

CODE JAM 01 SESSION

5th November, 2023

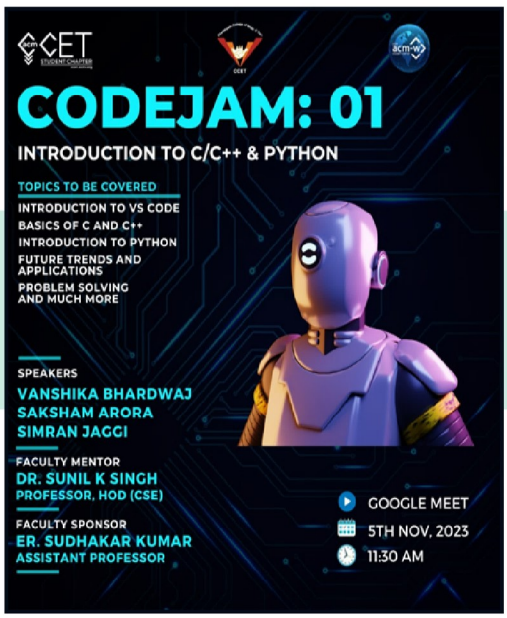
Event Details

On November 5, 2023, the CCET ACM and ACM-W Student Chapters collaboratively hosted an event called ‘CodeJam 101’ . In this event the participants were offered an excellent opportunity to learn the essential things in coding and familiarize themselves with the programming languages as well as how to code. The speakers, Vanshika Bhardwaj, Saksham Arora and Simran Jaggi, shared information and provided hands-on guidance, making this session an invaluable experience for all participants where they were able to learn coding along with trying it.

Event Speaker

- Vanshika Bhardwaj
- Saksham Arora
- Simran Jaggi

Event Gallary



TECHTALES - THE ART OF INNOVATION IN WORDS

10th November, 2023

Event Details

The CCET ACM & ACM-W Student Chapter conducted a technical writing competetion named "**Techtales - The Art of Innovation in Words**". The competition not only encouraged students to refine their writing skills but also fostered a culture of scholarly inquiry and knowledge dissemination within the department. As we reflect on the wealth of knowledge and expertise showcased during the event, it is evident that played a pivotal role in nurturing the academic and intellectual growth of our student community

APRATIM EVENTS HOSTED BY CASC

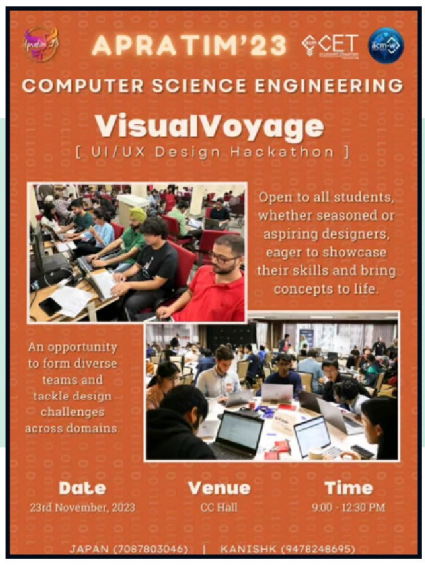
22nd - 23rd November, 2023

Events Details

The ACM & ACM-W Student Chapter recently hosted an exhilarating 12-hour hackathon "**Code Crusade"**, inviting participants to embark on a journey of innovation, collaboration, and problem-solving. The event aimed to unleash participants' coding prowess, foster new connections, and cultivate a spirit of creativity and ingenuity.

CCET ACM and ACM-W Student Chapter, recently organized a stimulating online writing event titled "**Writathon"**. This event served as a platform for participants to showcase their writing skills, creativity, and literary prowess in a digital landscape.

CCET ACM and ACM-W Student Chapter orchestrated an innovative design hackathon titled "**VisualVoyage**" as a prominent feature of the annoual Apratim 2023. This hackathon was conceived as a platform for participants to explore the frontiers of design, creativity, and problem-solving in a collaborative and competitive environment.



CREATIVITY WITH AI : HOUR OF CODE

9th December, 2023

Event Details

CCET ACM and ACM-W conducted an Hour of Code event on December 9th, 2023 as an inspiring initiative during Computer Science Education Week. Under the theme 'Creativity with AI,' participants delved into the fascinating intersection of art and technology

Event Speaker

The speaker, Utkarsh Chauhan provided valuable insights in the online event and enabled the attendees to explore the vast possibilities that coding offers.

Utkarsh Chauhan
CO21364, CSE 2021

DATA ANALYTICS AND CLOUD COMPUTING IN THE REALM OF CYBER SECURITY, PRIVACY, AND NETWORKING

Ayushi [MCO22384, CSE 2022]

Abstract:

The complex relationships between cloud computing, data analytics, and the important topics of networking, privacy, and cyber security are examined in this article. Strong security measures are essential as businesses move their operations to the cloud and depend more and more on data-driven insights. This article explores the history of various technologies, how they interact, and how important it is to strike a careful balance between innovation and protecting private data.

Introduction:

The combination of cloud computing and data analytics has ushered in a new era of efficiency and innovation in the digital age. Businesses use data analytics to extract insightful knowledge, and cloud computing offers the scalable infrastructure needed to handle and store enormous volumes of data. But this technical advance also presents serious privacy, networking, and cyber security risks that need to be carefully considered.

Background:

2.1 Data Analytics:

Analyzing raw data to identify patterns and make inferences is known as data analytics. Predictive modeling, machine learning, and statistical analysis are just a few of the methods used in the process. Companies use data analytics to improve decision-making, comprehend consumer behavior, and streamline workflows. Advanced analytics are becoming essential as data generation is increasing at an exponential rate.

2.2 Cloud Computing:

The way companies handle their IT resources is being revolutionized by cloud computing. Organizations move their data and apps to cloud platforms instead of depending on servers located on-site. More flexibility, scalability, and cost effectiveness are made possible by this change. There are three primary forms of cloud services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model has unique benefits with regard to control and management accountability.

Significance:

In today's digital world, the importance of data analytics and cloud computing is immense, impacting a wide range of industries from business and healthcare to education and government. Recognizing these technologies' significance

illuminates their revolutionary potential:

3.1. Improved Making of Decisions:

Data analytics: From enormous volumes of organized and unstructured data, organizations can extract insights that are useful. This enables decision-makers to make well-informed decisions devoid of gut feeling and grounded in facts.

Cloud Computing: Large datasets can be processed and analyzed with the help of cloud platforms, which offer the processing and storage capability required. Decision-makers will always have access to the processing power they require, whenever they require it, thanks to this scalability.

3.2. Effectiveness of Operations:

Data analytics: Data analytics improves operational efficiency by finding inefficiencies and optimizing processes. Organizations can increase productivity, cut expenses, and simplify processes.

Cloud computing: By providing on-demand access to computer resources, cloud services relieve businesses of the burden of maintaining and modernizing their own hardware. This lowers capital costs while also enabling more flexibility in responding to shifting business needs.

3.3. Innovation and Competitive Advantage:

Data Analytics: By spotting market trends, consumer preferences, and potential improvement areas, data analytics insights can spur innovation. Businesses that successfully use data analytics have a competitive advantage in their respective markets.

Cloud Processing: Because cloud platforms offer a scalable and flexible environment, they lay the groundwork for innovation. This enables companies to swiftly introduce new products, test out novel concepts, and adjust to shifting market dynamics.

3.4. Flexibility and Scalability:

Data Analytics: Adaptable analytics programs let businesses manage expanding datasets without compromising efficiency. As the amount, speed, and variety of data keep growing, this scalability becomes increasingly important.

Cloud computing: Due to the inherent scalability of cloud services, businesses can expand or contract in response to demand. This flexibility is especially beneficial for companies whose workloads change frequently.

3.5. Cost Savings:

Data Analytics: Data analytics helps reduce costs by finding and removing inefficiencies. Furthermore, a higher return on investment may come from operational and marketing changes that are specifically targeted and informed by analytics insights.

Cloud computing: Pay-as-you-go cloud services do away with the need for upfront capital investments in hardware and infrastructure. This economical

method enables companies to concentrate on their core skills.

3.6. International Cooperation and Accessibility:

Data Analytics: State-of-the-art analytics tools facilitate international cooperation and information exchange. Collaborating on data-driven projects allows teams to foster creativity and a diversity of viewpoints.

Cloud computing: By offering universal access to data and apps, cloud services help teams located all over the world collaborate. This accessibility encourages productive remote work and teamwork.

3.7. Security and Disaster Recovery:

Data Analytics: By spotting patterns suggestive of possible dangers, analytics tools can help with security. A company's overall security posture can be improved with proactive analytics measures.

Cloud Computing: Reputable cloud service providers make significant investments in security measures, frequently going above and beyond what can be done by individual businesses. Furthermore, cloud platforms provide strong disaster recovery options, guaranteeing the resilience of data in the event of unanticipated circumstances.

Disadvantages:

4.1. Security Issues

Combining cloud computing and data analytics creates a complicated new set of security issues. Cybercriminals find it appealing to target the enormous repositories of sensitive data kept on cloud servers. To protect against illegal access and data breaches, organizations need to put strong security measures in place, such as encryption, access controls, and frequent audits. Furthermore, in order to avoid interception and manipulation, secure networking protocols are necessary as data moves between on-premises infrastructure and the cloud.

4.2. Consequences for Privacy:

Concerns concerning personal privacy are brought up by the relationship between cloud computing and data analytics. There is a chance that massive datasets collected and analyzed by organizations will unintentionally reveal personally identifiable information. It's critical to strike a balance between following privacy laws and using data to draw conclusions. A thorough privacy strategy must include data anonymization methods, strict data access controls, and adherence to privacy laws.

4.3. Difficulties in Networking:

A key component of the smooth integration of cloud computing and data analytics is effective networking. High-speed, low-latency connections are necessary for the transfer of data between devices, cloud servers, and analytics platforms. To guarantee that data moves smoothly and without interruption, organizations need to make

significant investments in networking infrastructure. Furthermore, the requirement for optimized network architectures increases with the scale of operations.

Conclusion:

To sum up, the combination of cloud computing and data analytics has changed how businesses operate. The advantages in terms of productivity, creativity, and expandability are enormous. Nonetheless, it is impossible to overlook the difficulties presented by networking, privacy, and cyber security. Companies need to take a comprehen sive approach, incorporating state-of-the-art security measures, privacy-aware procedures, and networking solutions that are optimized.

It's critical that we approach this period of digital transformation by seeing cloud computing and data analytics as essential parts of a safe and morally sound business ecosystem, rather than merely as instruments for expansion. By doing this, businesses can protect the privacy and trust of their stakeholders while realizing the full potential of these technologies.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Avneet Kaur [CO21312, CSE 2021]

What is Artificial Intelligence?

Artificial intelligence (AI) is a broad discipline that includes the simulation of human-like intelligence in computers. It entails a wide range of approaches and procedures that allow computers and technologies to mimic cognitive capabilities normally associated with humans. This includes problem-solving, which entails using algorithms and computational models to solve complicated problems. AI systems are meant to learn from data using techniques like machine learning, allowing them to recognize patterns, forecast outcomes, and optimize operations. Furthermore, AI is concerned with information perception, in which robots receive and comprehend data from multiple sources, including visual and aural inputs. Reasoning is an important feature of AI systems because it allows them to analyze data, draw conclusions, and make logical inferences to help them make decisions. Natural Language Processing (NLP) is used to understand natural language, allowing robots to perceive, interpret, and synthesize human languages. Furthermore, AI systems demonstrate flexibility by adapting to new scenarios, surroundings, or data without the need for explicit programming for each case. They increase their performance over time by iterating, learning from experience, and perfecting their algorithms. The capacity of AI systems to analyze and understand data, recognize patterns, make judgements, and improve over time without explicit programming for each job is a distinguishing feature, adding to their versatility and application across a wide range of areas.

What is Machine Learning?

Machine Learning (ML) is a subfield of artificial intelligence that focuses on allowing machines to learn and develop without being explicitly programmed. It entails the creation of algorithms and statistical models that enable computers to learn patterns and insights from data and then make predictions or judgements based on that learning.

Machine learning often entails the following steps:

Data Collection: Obtaining relevant and representative data for use in training the machine learning model.

Data Preprocessing: Cleaning and preparing data for analysis by dealing with missing values, normalizing features, encoding categorical variables, and so on.

Model Training: Training the model on

the prepared dataset using different machine learning techniques (such as regression, decision trees,neural networks, support vector machines, and so on). The model learns patterns, correlations, and rules from the data during training.

Evaluation: Assessing the trained model's performance using evaluation measures to assess how effectively it generalizes to new, previously unknown data. This stage aids in the selection of the optimal model and the adjustment of its parameters.

Prediction or Inference: Using the trained model to forecast or make choices on fresh data based on what it learnt during the training phase.

Machine learning can be categorized into three main types:

Supervised Learning: Training a model on labelled data involves the algorithm learning the link between input features and the intended output. Classification and regression are two common tasks.

Unsupervised Learning: The model is given unlabeled data and is charged with detecting patterns or structures in the data, such as clustering related data points or dimensionality reduction.

Reinforcement Learning: This kind includes an agent learning to make decisions through interaction with its surroundings. The agent learns from the consequences of its actions and is rewarded or punished, with the goal of maximising cumulative reward over time.

Machine learning has a wide range of applications, including but not limited to healthcare, finance, marketing, recommendation systems, natural language processing, computer vision, autonomous cars, and others.

The ethical implications of AI and ML

The fast growth and broad adoption of Artificial Intelligence (AI) and Machine Learning (ML) technologies raises a number of ethical concerns and ramifications. Some major ethical considerations are as follows:

Bias and Fairness: AI systems might inherit biases from the training data, resulting in biassed outputs that disproportionately affect specific groups or people. It is critical to ensure fairness and bias in AI systems in order to prevent prejudice.

Transparency and Explainability: Many AI/ML models, particularly complicated ones like deep neural networks, function as "black boxes," making it difficult to comprehend how they make certain judgements. This lack of transparency raises questions about accountability and the ability of impacted parties to understand AI-driven judgements.

Privacy and Security: AI systems frequently analyse massive volumes of personal data, prompting worries about data breaches and privacy violations.

To protect user privacy, sensitive information must be safeguarded and correct data processing practises must be followed.

Job Displacement and Socioeconomic Impact: Artificial intelligence (AI) automation may result in job displacement in certain areas, thereby exacerbating economic inequities. Addressing the social impact of AI on employment and ensuring equal benefit distribution are critical.

Autonomy, Responsibility, and Liability: As AI systems become increasingly autonomous, it becomes more difficult to determine accountability and assign blame for AI-related errors or choices. It is a huge difficulty to establish legal frameworks to manage liability issues and determine who is liable for AI-related conduct.

The economic impact of AI and ML

Artificial Intelligence (AI) and Machine Learning (ML) have a significant and broad economic influence, impacting different industries and components of the global economy:

Increased Efficiency and Productivity: Across sectors, AI and ML technologies optimise processes, automate operations, and improve operational efficiency. This greater efficiency leads to cost savings and increased production, which benefits businesses and economies.

Innovation and New Business Opportunities: AI/ML promotes innovation by facilitating the creation of new goods, services, and business models. It promotes entrepreneurship and the formation of businesses focused on AI-driven solutions, hence promoting economic growth.

Labor Market Changes: While artificial intelligence and automation may result in employment displacement in some areas, they also generate new career prospects. Data scientists, machine learning engineers, and AI ethicists are in great demand, fueling growth in specialised sectors.

Improved Decision-Making: AI and machine learning help data-driven decision-making by delivering insights from massive amounts of data. This leads to more informed strategic decisions, which might lead to improved company outcomes and economic growth.

However, there are obstacles, such as the need for workforce reskilling, dealing with possible job displacement, guaranteeing ethical AI development, and bridging the digital divide across nations and sectors. To maximise the good economic effect of AI/ML while limiting any negative outcomes, policymakers, enterprises, and governments must negotiate these hurdles. Overall,

when used and handled appropriately, AI and ML have the ability to boost economic development, innovation, and competitiveness across several industries.

Conclusion

The future of Artificial Intelligence (AI) and Machine Learning (ML) offers great potential in terms of altering many aspects of society. The potential of artificial intelligence (AI) extends across industries, from healthcare, where predictive analytics might revolutionise diagnoses and personalised treatment, to transportation, where AI-powered autonomous cars could improve safety and efficiency. Machine learning algorithms have the potential to transform the way organisations run by allowing improved decision-making, higher efficiency, and the development of novel goods and services. Furthermore, by optimising resource management and assisting in environmental research, AI and ML hold the key to tackling societal concerns such as climate change. To realise this promise, however, ethical concerns, legal frameworks, and a deliberate effort to promote inclusion, justice, and openness in AI development and deployment are necessary.

UNDERSTANDING THE PROMISE & CHALLENGES OF EXPLAINABLE AI

Eshita Badwal [CO21316, CSE 2021]

In the ever-evolving world of artificial intelligence (AI), the development of complex, deep learning models has now become increasingly prevalent. These models have exhibited exceptional performance in various tasks, like image recognition, natural language processing, computer vision, robotics and much more. However, As AI continues to advance, the challenge of comprehending and retracing an algorithm's decision-making process becomes increasingly daunting. The algorithm's inner workings often transform into a mysterious "black box," rendering them nearly impossible to interpret. This black-box poses a serious issue. Model these days make decisions on sensitive user data (such as health records), and for none to know how this data is being used and the models processing to arrive at a decision is a major ethical and privacy concern. Even the engineers and data scientists behind the algorithm may find it challenging to decipher how a specific outcome was reached. Hence, we need an understanding about how AI systems arrive at their results to make these systems better from a privacy and reliability standpoint. This is the main motivation behind the development of Explainable AI. In essence, Explainable AI is the key to unlocking the potential of AI while ensuring transparency and accountability.

What is Explainable AI?

Explainable AI, often abbreviated as XAI, is a subfield of artificial intelligence which is mainly focused on developing AI systems that can provide understandable and transparent explanations for their decisions and predictions. In essence, XAI seeks to bridge the gap between the "black box" nature of many AI models and the need to comprehend the rationale behind AI-generated outcomes for accountability.

Why is Explainable AI Important?

Incorporating Explainable AI into an organization's operations is imperative. Blindly relying on AI models without a comprehensive understanding of their decision-making processes is not advisable and a major privacy and security concern. The significance of Explainable AI lies in its ability to elucidate the inner workings of machine learning (ML) algorithms, deep learning, and neural networks for human comprehension.

As mentioned before, machine learning models are often likened to enigmatic "black boxes" that defy interpretation. Among these, neural networks, particu-

larly those used in deep learning, pose the greatest challenge for human understanding. Another persistent concern in AI model development is the potential bias rooted in factors like race, gender, age, or location. Additionally, AI model performance may fluctuate or deteriorate when faced with production data that differs from the data used for training. This underscores the need for continuous model monitoring and management to enhance AI explain ability and assess the business impact of deploying such algorithms.

Explainable AI not only fosters trust among the end users but also enables model auditability and ensures -the effective utilization of AI. It serves as a safeguard against compliance issues, legal entanglements, security breaches, and threats to an organization's reputation arising from the deployment of AI in production. Recognizing the role of Explainable AI as an essential component of responsible AI implementation, a framework aimed at deploying AI methods on a large scale with fairness, model transparency, and accountability is necessary. To adopt AI in an ethical and responsible manner, organizations must integrate ethical principles into AI applications and processes, building AI systems founded on trust and transparency.

Challenges in Developing Explainable AI

In the pursuit of Explainable AI (XAI), there are many challenges. Firstly, there's a trade-off between the complexity and explain ability of AI models. Deep learning models, renowned for their state-of-the-art performance, inherently feature complexity that often proves too difficult to decipher. While simplifying these models may enhance interpretability, it can come at the cost of predictive accuracy. Additionally, the field grapples with the diversity of interpretability methods. There's no one-size-fits-all solution for crafting explainable AI, as researchers have introduced a range of techniques, each possessing its unique strengths and limitations. Evaluating explain ability remains a persistent challenge. Determining what constitutes a satisfactory explanation can be elusive, further complicated by varying human preferences for explanations. Finally, privacy concerns add another layer of complexity. Some XAI methods have the potential to unveil sensitive information, potentially infringing on privacy regulations, necessitating the delicate balancing of transparency and privacy. These challenges collectively underscore the ongoing evolution and significance of the Explainable AI field.

Current Approaches to Explainable AI

Researchers are actively engaged in the development of innovative techniques aimed at tackling the multifaceted challenges of Explainable AI (XAI). Notable approaches within the XAI domain encompass:

Interpretable Models: This approach involves designing AI models that inherently possess interpretability. Models like decision trees and linear regression fall into this category. These interpretable models are characterized by their transparency, making it easier for users to understand their decision-making processes. However, they often come with a trade-off in terms of predictive performance, which may not be as robust as that of more complex models.

Post hoc Explanations: Post hoc explanation techniques, such as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations), offer insights into the decision-making of complex models, even when the models themselves lack inherent interpretability. These methods provide localized, user-friendly explanations for specific model predictions, enhancing the comprehensibility of intricate AI systems.

Visualization Tools: Visualization tools are pivotal in shedding light on the opaque workings of AI models. These tools generate graphical representations of the decision-making processes, making them more accessible and understandable to humans. By visually mapping out the model's operations and decision paths, these tools empower users to grasp the rationale behind AI-generated outcomes.

Rule-Based Systems: Rule-based systems adopt a structured, transparent approach by defining explicit decision rules that are easily understandable by humans. These systems provide clear guidelines for the model's decision-making, offering transparency and accountability. When rules are based on ethical and regulatory considerations, they ensure that AI systems adhere to responsible and ethical practices.

These approaches represent a dynamic and evolving landscape within the field of Explainable AI. By combining these techniques and continually refining them, researchers are striving to make AI systems more transparent, interpretable, and trustworthy, ultimately paving the way for responsible and accountable AI applications across various domains. Explainable AI is an increasingly vital field in the development of artificial intelligence. It addresses the pressing need for transparency, accountability, and fairness in AI systems. While challenges remain in achieving the perfect balance between complexity and interpretability, researchers and practitioners are actively working to make AI more understandable and accessible to all. As we move forward in the AI era, XAI will continue to play a pivotal role in shaping the future of AI applications and ensuring that these technologies work for the benefit of humanity.

SOCIAL ENGINEERING ATTACKS

Sahil Garg [CO22358, CSE 2022]

In this modern era of digitalization, everyone has a mobile and an internet presence. Everyone has an email account, bank account with net banking enabled or using some sort of app for banking, social accounts on various social media apps such as instagram, facebook, whatsapp etc. Talking to strangers and being comfortable around them is one of the harvested characteristics of this new digitalized era for most of us. Our galleries are filled with sensitive and personal media which in our wildest thoughts, we would not like to share with the world. Hence, we have a lot of digital content to lose. Our body is still physically present but our minds are converted virtual.

This is also an era of information overload with all the knowledge being freely available. This is one of the strengths of the internet but also in the hindsight of the praises and appreciations it is also a foe of the human. This has been a good source to learn mind manipulation and made it available to the general public much more easily. Manipulating the other person into him giving their details isn't a great deal. This has been going on since digitalization has begun. Spammers have one trick stored in their bag, manipulating the other person into believing what the spammer wants to get the necessary information out of the other person. This is exactly what happens in a social engineering attack.

In a social engineering attack, the victim is manipulated in any possible way to get hold of the credentials directly or indirectly. There are two ways of attacking a person's account - either get hold of the username and password or get hold of the security question or some other detail which would help break into account through reset password or forgot password option.

One of the attacks' that come under social engineering is a phishing attack. In this attack, a person is led to a malicious clone of a real and trusted website. There the victim is made to enter one of the two pieces of information discussed above while showing the user the trust that they have for that company and its website. Once information is entered, nothing great happens on the user's side but a lot happens on the attacker side. With this information, they attack one of the accounts' of the user which usually leads to another account and hence, the chain continues.

This attack is provoked also by sending

an SMS or a fake email or making a scam call to the victim with a lure or a fear. Using these human emotions, they drive the non-tech savvy society into social engineering attacks.

Nowadays, there is yet another way to attack a victim's accounts without the victim ever sharing any details with anyone. Well this happens with the help of browser cookies. Browsers store session cookies every time you log into your account on any website. If installation of a malicious software is successful, reading a browser's cookies and sending them over to the attacker is no big task. Once the cookies are there, they can be used to open the account without any username or password.

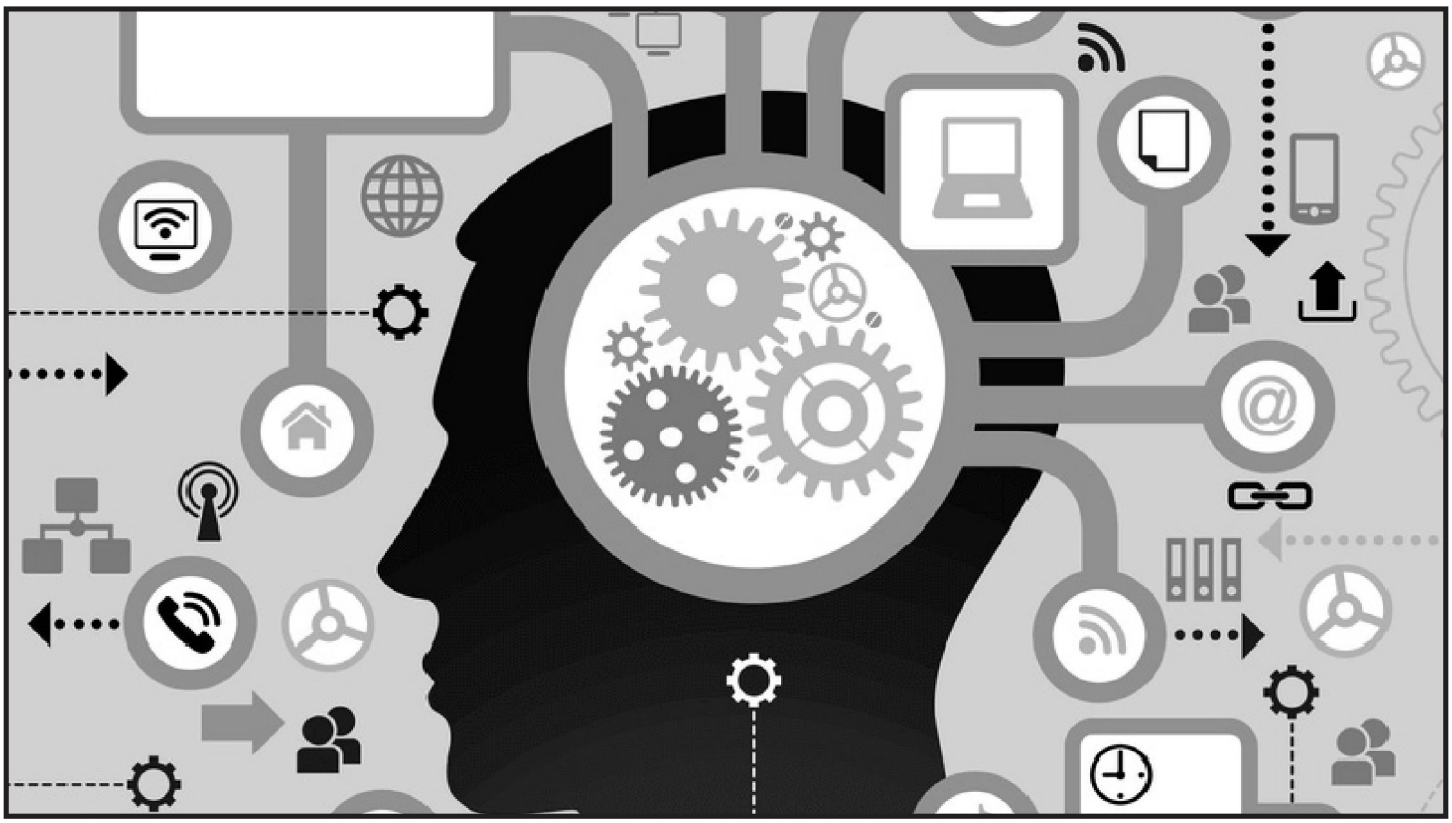
Impersonation is yet another part of this attack. Impersonation involves pretending to be someone the target knows and trusts, often through social media or other communication channels. Creating a fake social media profile of a colleague and using it to request sensitive information from others in the network.

Some of the preventive measures one should take to prevent such manipulation are followed mainly by not sharing your sensitive usernames or passwords with anyone. Any security question you may have set, such as your dog's name or your age, well this is an alert. Keeping the ears open and brain on alert especially when in public would prevent you from social engineering attacks tried in public areas.

For the online ones, prevent them by adding multi-factor authentication (MFA) to all systems and applications, you may fortify your security measures. By requiring users to give additional authentication factors, like a one-time code from a mobile app or a biometric scan, MFA adds an extra layer of security on top of passwords. Implementing multi-factor authentication (MFA) greatly lowers the danger of unwanted access, even in the event that hackers succeed in obtaining login credentials through social engineering. To lessen the effect of compromised credentials, make sure MFA is set for email accounts, cloud services, and any other important systems.

Securing email, the main medium used by phishing attempts, is frequently the first step in defending against social engineering assaults. Use cutting-edge email filtering systems that use machine learning and artificial intelligence to identify and stop dangerous emails. To detect phishing attempts, these systems examine sender behavior, content, and recognized threat indicators. To further confirm the authenticity of incoming emails, use email authentication protocols like DMARC (Domain-based Message Authentication, Reporting, and Conformance). DMARC makes sure that only authorized organizations are able to send emails using

your domain, which helps avoid domain spoofing, a prevalent technique in phishing attempts.Promote the use of secure channels for communication, particularly when handling sensitive data. Employ secure messaging services for internal and external communication, and ensure that emails are encrypted from beginning to end. An additional degree of security is added by using secure channels, which makes it more difficult for hackers to intercept or alter communications. Additionally, train staff members on the value of confirming someone's identity before disclosing sensitive information—even through channels that are considered reliable—to avoid falling for deception or impersonation schemes. Well, with these measures and adequate knowledge about social engineering attacks, it is very difficult to fall prey to these. Use your wits in public places, keep ears open, and brain on alert mode. Human psychology is very powerful when used ethically can do a lot good else is a weapon of mass destruction.



CYBER SECURITY AND PRIVACY

Vanshika Bhardwaj [CO21366, CSE 2021]

Introduction

Businesses are increasingly embracing Industry 4.0 (I4.0), which includes Internet of Things (IoT) and Industrial Internet. In order to increase efficiency and productivity, industrial units are connected via the internet. But a major obstacle faces these internet-enabled industries: serious Cyber Security (CS) threats. CS becomes essential for maintaining organizational competitiveness in the I4.0 environment. Cybercriminals can take advantage of vulnerabilities in networks and occasionally even devices due to the increased connectivity between smart devices and networks in this era. Such cyberattacks affect society and the mentalities of the impacted countries in addition to interfering with organizational operations.

As reported in Cisco's 2018 CS annual report, 31% of organizations experienced cyberattacks on operational technology, and 38% anticipated a shift in cyber-attacks from the Information Technology to the Operational Technology level. The report emphasized that 75% of experts regarded CS as a priority, while only 16% believed their companies were adequately prepared to face CS challenges. Insufficient awareness of CS threats and lacking technical and managerial skills were cited as contributing factors. CS is gaining prominence in Europe and international organizations, with bodies like the International Electrotechnical Commission (IEC) issuing guidelines on CS and privacy implementation. Similarly, the European Skills, Competences, Qualifications, and Occupations (ESCO) has compiled standards and guidelines to aid the European digital market in addressing CS challenges. Despite these initiatives, daily reports continue to highlight security threats, especially within the context of I4.0.

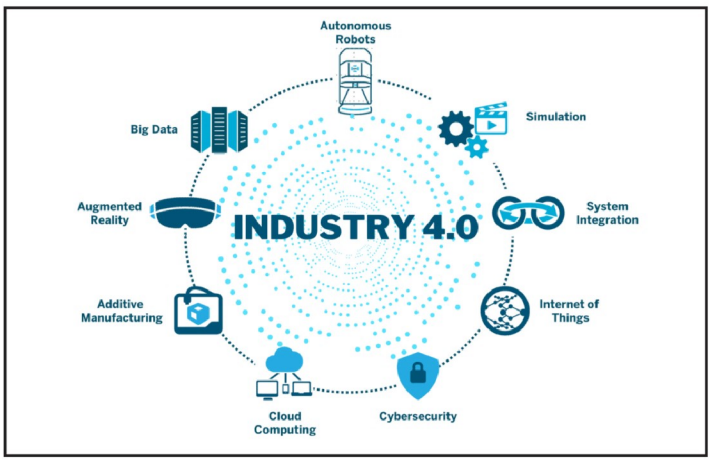
This underscores the need for in-depth research on cyber-security, particularly within the I4.0 paradigm. A comprehensive review of potential security threats targeting Industrial Internet of Things (IIoT), along with associated consequences and countermeasures, is essential. IIoT encompasses interconnected sensors, tools, and devices linked to industrial computer applications, impacting areas such as manufacturing, production, and energy management. The study's focus on IIoT is driven by its

potential for data collection, distribution, and analysis, offering avenues for productivity enhancement and economic benefits.

This emphasizes how important it is to conduct thorough research on cyber-security, especially in the context of the I4.0 paradigm. It is crucial to thoroughly examine all possible security risks aimed at the Industrial Internet of Things (IIoT), as well as the repercussions and protective measures that follow. Industrial Internet of Things (IIoT) affects industries like manufacturing, production, and energy management. It consists of networked sensors, tools, and devices that are connected to industrial computer applications. The study's emphasis on IIoT is motivated by its capacity for data distribution, collection, and analysis, which presents opportunities for raising productivity and reaping financial rewards.

Industry 4.0

An enormous revolution in the industry has been brought about by the term I4.0, also known as industrial internet. It started in Germany when the government there encouraged computerization in the manufacturing sector. The goal of I4.0 was to use the internet to link all participants and enable them to share information with one another. The concept is predicated on a cyber-physical system, which is a system of computer components working together in a planned and regulated manner. I4.0. Offers increased business gains and significantly increased productivity. It has affected nearly every aspect of life, and supporters of Industry 4.0 see it as the third innovation wave. In order to provide a better understanding, we will go over a few definitions of I4.0 from recent literature below. "The industrial internet is an IoT, machines, computers, and people that reshapes the business and consumer landscape by enabling intelligent industrial operations through the use of advanced data analytics for transformative business outcomes." Value chain organization technologies and concepts are referred to as "I4.0" collectively.



Industrial Internet of Things (IIOT)

The internet of things (IoT) is a network of interconnected devices that exchange data with one another. IIoT is what happens when the same IoT is used in industrial settings. I4.0 and IIoT have been used interchangeably by researchers. Nonetheless, we consider IIoT to be one of I4.0's pillars.

"Industrial Internet: a portmanteau for the Internet of Things' industrial applications, also referred to as the IIoT" "IoT technologies used in manufacturing is known as the IIoT." "Every object, or 'thing,' is embedded with a sensor and able to automatically communicate its state with other objects and automated systems within the environment. This is the scenario that the Internet of Things represents." In a virtual network, every object is a node that is constantly sending out a lot of data about itself and its surroundings. "IoT" refers to the general expansion of network access and computational capabilities to things, devices, sensors, and other items that are not usually thought of as computers. These "smart objects" have connectivity to distant data collection, analysis, and management capabilities; they also require little human interaction in the creation, sharing, and consumption of information.

Cyber Security

Cyber security is the use of various methods to protect networks, computers, software, and data from attacks or unwanted access. It also includes protecting an organization's cyberspace from threats to its security, both from within and without. Researchers and practitioners worldwide are paying close attention to the field of cyber security, or CS. The literature's many definitions of computer science demonstrate the complexity of this field. The act of "preserving the integrity, confidentiality, and timely availability of information in Cyberspace" is one definition of computer science (CS).

Cyber-Physical System

Cyber-Physical Systems, or CPSs, are networks of physical objects that communicate with computational components. A central computing and communication hub controls, organizes, regulates, and integrates the functions of the physical and engineered structures that make up these systems. They improve the capabilities of physical systems by enabling the fusion of communication and computation with physical processes.

A different definition defines CPS as "a system consisting of interacting physical and digital components, whether centralized or distributed, providing a combination of sensing, control, computation, and networking functions to influence real-world outcomes through physical processes" . A cyber-physical system is described as "a collection of cyber-physical devices incorporating computing hardware and software that govern mechanical activity through networking, connectivity, and embedded processing" by another viewpoint. These devices have sensors that allow them to sense their surroundings and other objects, and actuators that allow them to interact with their

surroundings." For the purpose of managing interconnected systems, CPS is recognized as a disruptive technology that bridges the gap between physical assets and computational capabilities. CPS differs from conventional I/O systems in that it interacts with the physical environment in real time. Although CPS and ICT systems manage information and/or data, CPS is primarily concerned with managing physical processes.

Cyber Security Characterization for Industry 4.0

System vulnerabilities: System vulnerabilities are flaws in the system that hackers can take advantage of to undermine the security of Cyber-Physical Systems (CPS). Vulnerabilities in the information system, security protocols, audits, controls, or implementation that could be exploited by possible threats are all included in the NIST definition of vulnerability. Every component in the Industrial Internet of Things (IIoT) exhibits different vulnerabilities. Application servers, communication infrastructure, HCIs, RTUs, and even sensors and actuators are all susceptible to these vulnerabilities. The existence of multiple pathways within networks, insufficient security measures, and a lack of isolation between unrelated networks are the fundamental causes of these vulnerabilities.

Cyber Attacks: According to NIST, cyber-attacks are incidents that negatively impact individuals, assets, or organizational operations through the use of similar techniques like disclosure, DoS attacks, unauthorized access, or information modification. Active mode attacks and passive mode attacks are the two types of these attacks. Active mode attacks (such as denial-of-service and compromised key attacks) modify system resources or interfere with system functions. Passive mode attacks, on the other hand, seek to take advantage of victim information without altering it.

Risk: According to NIST, risk is defined as the degree to which a cyberattack could affect an organization's operations, assets, or people, as well as the probability that the threat will materialize. Information systems' availability, confidentiality, and integrity are all affected by these security threats. The likelihood of security risks increases in the context of Industry 4.0 (I4.0), where a multitude of interconnected devices, including the cloud, are common. As such, it becomes imperative to proactively identify the risks related to each component and put in place efficient preventive and mitigating actions. Maintaining organizational competitiveness and avoiding the potentially higher costs associated with risks require this proactive approach.

Countermeasures: Countermeasures are methods and strategies used to stop, deter, and lessen possible attacks in order to lessen the damage that results. Identifying possible threats and evaluating the associated risks are the

responsibilities of industries operating within the Industrial Internet of Things (IIoT) infrastructure. Industries should set up efficient avoidance and detection procedures to protect their assets from cyberattacks. Using multiple layers of defense to implement a defense-in-depth strategy, controlling and managing remote access appropriately, and strengthening the perimeter—which entails separating sensitive nodes from common nodes—are some overarching protection strategies.

Credits

Editorial Mentor Board

Dr. Sunil K. Singh
(Mentor)
Professor and HoD
Department of CSE

Mr. Sudhakar Kumar
(Co-Mentor)
Assistant Professor
Department of CSE

Saket Sarin
CASC Student Chairperson
(2023 - 2024)

Aishita
CASC-W Student Chairperson
(2023 - 2024)

Akash Sharma
CASC Student Chairperson
(2022 - 2023)

Anureet Chhabra
CASC-W Student Chairperson
(2022 - 2023)

Lead Editors

Japan Ajit Singh
CSE 2021

Kanishk Nagpal
CSE 2021

Content Editor

Eshita Badwal
CSE 2021

Ayushi
CSE 2022

Feature Editors

Priyanshu
CSE 2021

Saksham Arora
CSE 2022

Vanshika Chilkoti
CSE 2022

Sneha
ECE 2022

CASC Board

Saket Sarin
Chairperson

Kanishk Nagpal
Vice Chair

Shivam Goyal
Secretary

Saksham Arora
Membership Chair

Kartik
Treasurer

Tushar Singh
Webmaster

Japan Ajit Singh
Design Head

Palvasha Bansal
External PR Head

Eshita Badwal
Editorial Head

Utkarsh Chauhan
Executive Head

Briti Singla
Social Media Mnager

Vanshika Chilkoti
Event Manager

CASC-W Board

Aishita
Chairperson

Mehak Preet
Vice Chair

Vanshika Bhardwaj
Secretary

Sahil Garg
Membership Chair

Harkiran Kaur
Treasurer

Ruchika Thakur
Webmaster

Priyanshu
Design Head

Ritika Gupta
External PR Head

Ayushi
Editorial Head

Avneet Kaur
Social Media Manager

Simran Jaggi
Event Manager

“Any sufficiently advanced technology is equivalent to magic.”

Arthur C. Clarke
Author

acmccet@gmail.com

/acmccet

http://ccet.acm.org/

CCET ACM Student chapter

/acmccet

/acmccet

ccet-acm-student-chapterZ

CCET Details
Department of CSE
CCET, Degree Wing
Sector - 26, Chandigarh

Contact Us
For general submissions and feedback, contact us.
Website: www.ccet.ac.in

CCET STUDENT CHAPTER

CCET acm-w STUDENT CHAPTER

Chandigarh College of Engg. & Tech.
CCET