DIGITAL OUTLET

VOLUME 5- ISSUE 4

JULY- AUGUST 2024

PUBLISHED BY-
CCET ACM STUDENT CHAPTER
CCET, DEGREE WING , SECTOR 26
CHANDIGARH

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.

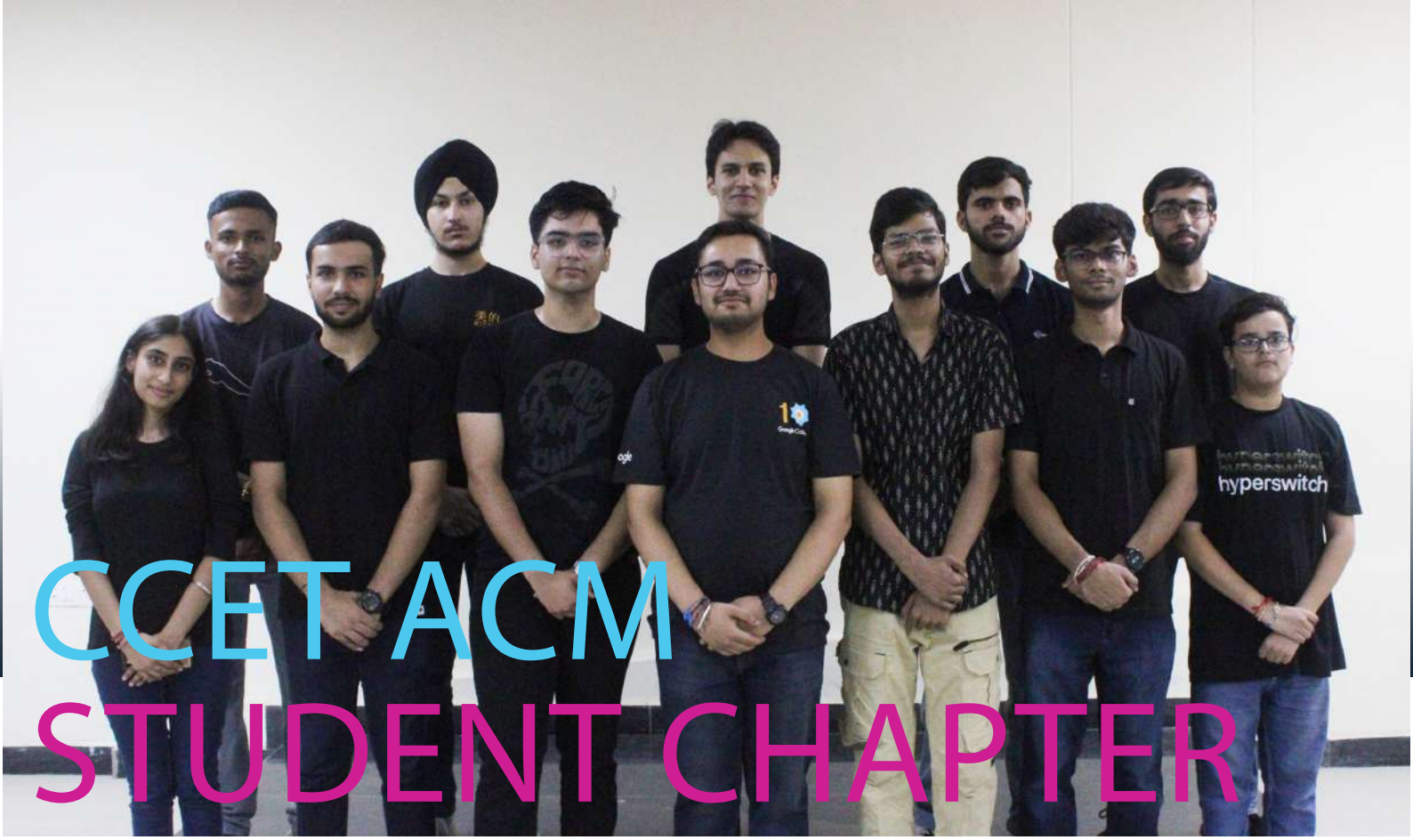
Dr. Sudhakar Kumar
Assistant Professor, CSE | Faculty Sponsor

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.

Sahil Garg
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.

Ayushi
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.

VISION

Chandigarh College of Engineering and Technology aims to be a center of excellence for imparting technical education and serving the society with self-motivated and highly competent technocrats.

MISSION

1. To provide high quality and value based technical education.
2. To establish a center of excellence in emerging and cutting edge technologies by encouraging research and consultancy in collaboration with industry and organizations of repute.
3. To foster a transformative learning environment for technocrats focused on inter-disciplinary knowledge; problem-solving; leadership, communication, and interpersonal skills.
4. To imbibe spirit of entrepreneurship and innovation for development of enterprising leaders for contributing to Nation progress and Humanity.

CASC ACHIEVEMENTS

PAPERS PUBLISHED IN IOSPRESS 2024

CCET-ACM and ACMW provide an environment with an emphasis on research and development, aiming to stay at par with recent trends and innovative approaches in the eld of computer science. Recently, research papers written by some of the bright minds of CASC were published in IET Research, a leading publishing platform by the Institution of Engineering and Technology, focusing on cutting-edge advancements in science, engineering, and technology.

1. IoT-enabled smart farming with Industry 5.0: This paper, authored by Aishita Sharma, Sunil K. Singh, Sudhakar Kumar, Ruchika Thakur, Brij B. Gupta, and Varsha Arya, explores how IoT and Industry 5.0 are revolutionizing modern agriculture. It highlights the integration of real-time data monitoring systems, cognitive systems, and digital twin technology in farming, promoting precision agriculture, enhancing crop yields, and fostering sustainability in an ever-changing global environment.

PAPER PUBLISHED IN TECHSCIENCE 2024

"Unleashing the Power of Multi-Agent Reinforcement Learning for Algorithmic Trading" by Saket Sarin, Sunil K. Singh, and others, published in Tech-Science on 15 August 2024, explores how Multi-Agent Reinforcement Learning (MARL) and Explainable AI (XAI) enhance Algorithmic Trading. The study focuses on improving decision-making in Fintech by using AI-driven agents to uncover trends, reduce risks, and provide personalized financial insights.

ESSENCE OF CODING ACM & ACM-W ORIENTATION

30th August 2024

Event Details

On August 30, 2024, an engaging orientation event was held at CCET for new entrants, led by speaker Sahil Garg and Ayushi. This event introduced students to the ACM Chapter and ACM-W, aiming to familiarize them with the organizations' objectives and activities while emphasizing the importance of coding as a fundamental skill in computer science.

The orientation featured interactive sessions where participants took part in coding challenges and collaborative problem-solving activities. Students gained insights into the significance of coding for developing innovative solutions and learned how it empowers them to tackle real-world problems. Experienced members of the ACM Chapter, including Sahil, shared valuable knowledge about various programming languages, tools, and frameworks, illustrating how coding is integral to software development, web design, and data analysis.

Through these engaging activities, the orientation underscored that coding is more than just writing lines of code; it is a creative process that nurtures logical thinking and teamwork. The newcomers were encouraged to view coding as a means to express their ideas and make meaningful contributions to the tech community.

Overall, this event successfully ignited enthusiasm among the new students, laying the groundwork for their active involvement in the ACM Chapter and motivating them to enhance their coding skills as they embark on their academic journeys in computer science.

Event Gallary

EMERGING THREATS IN CYBERSECURITY: A REVIEW OF ADVANCED PER-

Vanshika Chilkoti[MCO22392, CSE 2022]

This research attempts to provide a concise overview of Advanced Persistent Threats (APTs) within the cybersecurity domain, the focus is on their stealthy and prolonged presence in targeted systems, posing significant challenges to global organizations. Recent case studies and threat intelligence underscore the evolving tactics employed by APT groups, ranging from state-sponsored entities to criminal organizations. Motivations driving APT campaigns, such as espionage and sabotage, are explored alongside the role of emerging technologies, like artificial intelligence, in enhancing defensive strategies and empowering APT actors with more sophisticated offensive capabilities. The conclusion offers practical recommendations for organizations to strengthen their resilience against APTs, emphasizing proactive threat intelligence sharing and robust cybersecurity frameworks.

KEYWORDS:
Advanced Persistent Threats (APTs), Detection, Response, Recovery, Layered Defense Strategy, Cybersecurity Framework

INTRODUCTION:
In the current digital scenario, the proliferation of cyber threats[1] is an omnipresent concern for organizations across diverse sectors. Among these threats, Advanced Persistent Threats (APTs)[2] present a particularly insidious and formidable adversary. APTs, distinguished by their sophisticated strategies, prolonged infiltration durations, and selective targeting of high-value assets, pose a significant and evolving challenge to global cybersecurity. APTs are orchestrated as covert operations by highly skilled threat actors, including nation-states, cybercriminal syndicates, and politically motivated groups. Unlike conventional cyberattacks marked by their immediacy and brevity, APTs are engineered to remain undetected within targeted networks for extended durations, often spanning months or years. This covert persistence enables APT actors to methodically surveil their victims, extract sensitive data, and execute strategic maneuvers with precision. The evolution of APT tactics and techniques is driven by various factors, including technological advancements, shifts in geopolitical dynamics, and the evolving motivations of threat actors. Recent years have witnessed a surge in APT activity across multiple sectors, with organizations in finance, healthcare, government, and critical infrastructure being prime targets. From the strategic campaigns of state-sponsored actors aimed at intellectual property theft and strategic intelligence gathering to financially motivated operations orchestrated by cybercriminal groups seeking monetary gain, the motivations driving APTs are

diverse and multifaceted. Moreover, the rapid advancement of technology has both empowered APT actors and introduced new challenges for defenders. Innovations such as artificial intelligence (AI), machine learning (ML), and automation have revolutionized cybersecurity practices, offering both offensive and defensive capabilities to adversaries and defenders. APT actors leverage these technologies to augment their attack capabilities, automate reconnaissance, and evade detection, while defenders harness AI-driven analytics, threat intelligence platforms, and behavioral analysis to identify and mitigate APT activity. Given these complexities, organizations face the daunting task of defending against APTs while safeguarding the security and integrity of their digital assets. Effective defense against APTs necessitates a multifaceted approach that encompasses proactive threat intelligence sharing, robust cybersecurity frameworks, continuous monitoring and response mechanisms, and a pervasive culture of security awareness and resilience. In light of these challenges, this article aims to provide a comprehensive analysis of the dynamic landscape of APTs in cybersecurity. Drawing upon recent case studies, threat intelligence reports, and academic research, this study will scrutinize the tactics, motivations, and ramifications of APT activity. Furthermore, it will delve into the role of emerging technologies such as AI and ML in augmenting defensive strategies and enabling more sophisticated offensive capabilities for APT actors. By shedding light on the ever-evolving nature of APTs and offering actionable recommendations for organizations to fortify their defenses, this paper seeks to inform and empower cybersecurity practitioners and policymakers in their endeavors to mitigate this persistent threat.

TACTICS AND TECHNIQUES OF APTS:

Tactics and Techniques of APTs Description

Spear Phishing Targeted emails with malicious attachments or links to install malware on victim systems.

Zero-Day Exploits Exploiting undisclosed software vulnerabilities to gain unauthorized access and deploy malware.

Watering Hole Attacks Compromising legitimate websites frequented by targets to infect visitors' devices with malware.

Credential Theft Stealing user credentials via keylogging, password spraying, or social engineering for network access.

Lateral Movement Moving laterally across networks using privilege escalation, credential reuse, or trust exploitation.

Fileless Malware Operating in memory without leaving traces on disk, often exploiting legitimate system tools for malicious activities.

Command and Control InfrastructureEstablishing covert communication channels with compromised systems for remote control and data exfiltration.

Steganography Concealing malicious code or data within innocuous files to evade detection.

Living off the Land Utilizing legitimate system tools and processes for malicious activities.

Anti-Forensic Techniques Hindering incident response and forensic investigation efforts to cover tracks.

MOTIVES BEHIND APT CAMPAIGNS:

The driving forces behind Advanced Persistent Threat (APT) campaigns are often

intricate and varied, mirroring the strategic goals and interests of the individuals orchestrating them. Among the primary motivations frequently guiding APT campaigns are espionage coupled with intellectual property theft, as well as financial gain and sabotage.

Espionage and Intellectual Property Theft:
Among the prevalent motivations propelling APT campaigns is espionage, particularly evident when undertaken by state-sponsored actors or intelligence agencies. These entities endeavor to surreptitiously infiltrate networks to acquire sensitive information, such as classified government data, proprietary technologies, or strategic business intelligence. Exploiting vulnerabilities within the networks of target organizations, APT actors conduct meticulous reconnaissance, extract valuable data, and gain insights into the activities and intentions of their adversaries. Additionally, intellectual property theft serves as a significant driver of APT campaigns, notably prevalent in sectors harboring high-value proprietary information, such as technology, defense, and pharmaceuticals. APT groups may set their sights on research and development data, trade secrets, or patented innovations, aiming to secure a competitive edge or undermine the economic interests of rival entities or nations. The pilfered intellectual property may be harnessed to expedite domestic research and development efforts, inform policy decisions, or bolster similar products or technologies in competitive markets. The repercussions of espionage and intellectual property theft executed through APT campaigns can be profound and widespread. Beyond the immediate loss of sensitive data and competitive advantages, victims may grapple with reputational damage, financial ramifications, and legal entanglements. Moreover, the theft of intellectual property has the potential to stifle innovation and economic progress, sow distrust between nations and organizations, and pose significant national security threats, particularly in strategically vital sectors.

Financial Gain and Sabotage:
In addition to espionage, APT campaigns may be motivated by financial gain or sabotage, particularly when spearheaded by cybercriminal collectives or hacktivist factions. These entities may seek to monetize their exploits through various avenues, such as ransomware attacks, financial fraud, or extortion tactics. By penetrating networks and compromising pivotal systems, APT actors can disrupt operations, extort ransom payments, or abscond with financial assets, inflicting considerable monetary losses upon targeted entities. Moreover, APT campaigns driven by sabotage might aim to undermine the operations or reputation of specific entities or industries. For instance, hacktivist groups may target governmental bodies, corporations, or ideological adversaries to protest political decisions, social injustices, or environmental concerns. These entities might disrupt services, deface websites, or expose sensitive information to further their agenda, inciting disruption, chaos, and reputational harm to their targets. The motivations steering APT campaigns are intricate and ever-evolving, mirroring the varied interests and objectives of the involved threat actors.

Whether fueled by espionage and intellectual property theft or financial gain and sabotage, APT campaigns pose formidable challenges to organizations and nations alike, accentuating the necessity for robust cybersecurity measures, the exchange of threat intelligence, and collaborative efforts on the international stage to counter their threats.

CASE STUDIES AND EXAMPLES:

Exploring real-world occurrences of Advanced Persistent Threat (APT) campaigns offers valuable insights into the methods, consequences, and lessons learned from these sophisticated cyber intrusions. By delving into notable APT incidents and the insights gleaned from them, organizations can bolster their comprehension of the ever-evolving threat landscape and fortify their defensive strategies accordingly.

Example 1: Stuxnet Worm

Among the most notorious APT campaigns is the Stuxnet[3] worm, unearthed in 2010. Stuxnet stood out as a highly intricate malware engineered to target Iran's nuclear program, particularly its uranium enrichment facilities. By exploiting various zero-day vulnerabilities in Windows operating systems and Siemens industrial control systems, Stuxnet infiltrated air-gapped networks and manipulated programmable logic controllers (PLCs) overseeing centrifuge operations. Stuxnet's repercussions were profound, causing considerable damage to Iran's nuclear infrastructure. Reports indicated the destruction of thousands of centrifuges, effectively stalling the country's nuclear ambitions. The worm's sophisticated capabilities, including its stealthy propagation methods and evasion of detection, underscored the unprecedented complexity of APT campaigns driven by nation-states.

The StuxNet Worm

Insights Drawn:

Stuxnet's impact can be analyzed through different metrics, including the number of centrifuges destroyed, the financial cost incurred for remediation efforts, and the geopolitical tensions resulting from the attack. Estimates suggest that Stuxnet obliterated approximately 1,000 to 2,000 centrifuges, leading to substantial financial losses for Iran's nuclear program. Furthermore, the incident exacerbated diplomatic tensions between Iran and the global community, triggering diplomatic consequences and heightened scrutiny of cyber warfare tactics.

Example 2: NotPetya Ransomware

Another notable APT campaign is the NotPetya[4] ransomware attack, which transpired in 2017. Initially masquerading as a ransomware[5] assault targeting Ukrainian entities, NotPetya swiftly proliferated worldwide, infecting thousands of systems across various nations and industries. The malware exploited diverse propagation techniques, including the exploitation of the EternalBlue vulnerability, previously leveraged in the WannaCry attack. The repercussions of NotPetya were catastrophic, resulting in billions of dollars in damages to businesses globally. The attack disrupted critical infrastructure, spanning shipping, healthcare, and manufacturing sectors, and led to prolonged service disruptions and data losses for numerous organizations. NotPetya's[6] indiscriminate targeting and destructive capabilities underscored the evolving threat landscape of APT campaigns, where ransomware serves as a tool for both financial extortion

and sabotage.

The NotPetya Attack Process
Insights Drawn:
The financial impact of the NotPetya attack can be quantified by assessing direct remediation costs, revenue losses due to downtime, and the reputational damage sustained by affected organizations. For instance, Maersk, a prominent shipping company, reported losses exceeding $300 million attributable to NotPetya-related disruptions, including temporary system shutdowns and extensive server and workstation reinstallation efforts.
Establishing a robust defense framework is essential in guarding against Advanced Persistent Threats (APTs), renowned for their stealthy and persistent tactics. A comprehensive APT defense strategy encompasses key pillars revolving around detection, response, and recovery, highlighting the importance of implementing layered defense strategies.

APT DEFENSE FRAMEWORK:
Detection serves as the frontline defense against APTs, enabling organizations to identify and thwart malicious activities early on. Continuous monitoring of network traffic, endpoint devices, and system logs, coupled with advanced threat detection technologies like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) solutions, enhances the ability to promptly detect APT activities.
Timely and decisive response is crucial for minimizing the impact of APT incidents. A well-defined incident response plan delineates procedures and escalation protocols for effectively handling APT incidents. Incident prioritization, containment of compromised systems, forensic analysis, and collaboration with relevant stakeholders facilitate swift response efforts, limiting the spread of APT attacks and restoring normal operations promptly. Following an APT attack, recovery efforts involve restoring affected systems and data to their pre-incident state. A robust recovery strategy encompasses measures such as data backups, disaster recovery plans, and system restoration procedures. Regular backups of critical data and resilient infrastructure architectures aid in minimizing data loss and expediting the recovery process in the face of APT-related disruptions. A layered defense strategy, also known as defense-in-depth, is essential for combating the multifaceted threats posed by APTs. Deploying multiple security controls across various layers of the IT infrastructure creates multiple barriers against APT infiltration and propagation. Network segmentation, access controls, endpoint protection, application whitelisting, and encryption are key components of a layered defense strategy. By diversifying defensive measures and incorporating both preventive and detective controls, organizations can mitigate the risk of APT attacks bypassing individual security measures, bolstering overall resilience against sophisticated threats.
FUTURE SCOPE:
Looking forward, the future of APTs is poised for transformation, driven by technological advancements and the constant innovation of malicious actors. Emerging trends such as artificial intelligence (AI) and machine learning (ML) are anticipated to significantly impact both APT capabilities and defense

strategies. AI-driven systems for threat detection and response offer the promise of real-time insights into APT activities, empowering organizations to adopt proactive defense measures. Additionally, the expanding adoption of Internet of Things (IoT) devices and cloud computing infrastructures presents new avenues for APT adversaries to exploit. Therefore, the future of APT defense will rely on continuous innovation, collaboration, and adaptation to address evolving threats effectively.

CONCLUSION:

To conclude, the threat landscape posed by Advanced Persistent Threats remains dynamic and challenging, necessitating proactive and comprehensive defense approaches. Through the implementation of robust detection, response, and recovery mechanisms, supported by layered defense strategies, organizations can enhance their resilience against APT attacks. Furthermore, as APT tactics evolve and technology continues to advance, ongoing vigilance and adaptation will be essential. By staying informed about emerging threats, harnessing innovative technologies, and fostering collaboration across the cybersecurity community, organizations can better mitigate the risks associated with APTs and safeguard their critical assets and operations in today's rapidly evolving digital landscape.

Credits

Editorial Mentor Board

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

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

Sahil Garg
CASC Student Chairperson
(2024 - 2025)

Ayushi
CASC-W Student Chairperson
(2024 - 2025)

Saket Sarin
CASC Student Chairperson
(2023 - 2024)

Aishita
CASC-W Student Chairperson
(2023 - 2024)

Lead Editors

Rima Kumari
CSE 2022

Rajneesh
CSE 2022

Content Editor

Nipun Singh
CSE 2022

Deepika Goyal
CSE 2022

Feature Editors

Ayushi
CSE 2022

Saksham Arora
CSE 2022

Simran Jaggi
CSE 2022

CASC Board

Sahil Garg
Chairperson

Saksham Arora
Vice Chair

Samar Partap Singh
Secretary

Trannum
Membership Chair

Divyansh Manro
Treasurer

Harshit Vashist
Webmaster

Rajneesh
Design Head

Jaiveer Singh
External PR Head

Nipun Singh
Editorial Head

Yuvraj
Executive Head

Dikshant Rajput
Social Media Mnager

Jasjeet Singh
Event Manager

CASC-W Board

ayushi
Chairperson

Simran Jaggi
Vice Chair

Vanshika Chilkoti
Secretary

Vanshika Singla
Membership Chair

Janvi Sharma
Treasurer

Japjot Singh Nanda
Webmaster

Rima Kumari
Design Head

Ravina Mittal
External PR Head

Deepika Goyal
Editorial Head

Anoop Pant
Social Media Manager

Deependra Singh
Event Manager

"Scientists explore the mysteries of what exists, while engineers bring to life what once only existed in dreams."

Theodore von Kármán
Pioneering Aerospace Engineer and Physicist

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