acm CCET STUDENT CHAPTER
ccet.acm.org

CCET acm-w STUDENT CHAPTER

Chandigarh College of Engg. & Tech.
CCET

DIGITAL outlet

THE CCET ACM TECH MAGAZINE

DISCOVER INSIDE

- BLOCKCHAIN AND ADVANCED DATA SCIENCE -
- ADVANCEMENTS IN THREAT INTELLIGENCE SHARING AND COLLABORATIVE DEFENSE FOR ENHANCING CYBERSECURITY RESILIENCE -

ACM CCET MOBILE APP

GET IT ON PLAYSTORE

VOLUME 4, ISSUE 2
September - October, 2023

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

PAPERS PUBLISHED IN ICSPN-2023

The papers written by the brilliant minds of the ACM and ACM-W Student chapter of CCET were published in the proceedings of the 3rd International Conference on Cyber Security, Privacy, and Networking (ICSPN-2023). The conference, held virtually, took place during September 28-30, 2023, in Dubai, UAE. Following were the details of the papers:

1. The paper titled "**Ransomware Resilience: Advancements in Detection and Mitigation Strategies for Real-world Threats,**" authored by Chandra Kumari Subba, Sudhakar Kumar, Sunil K. Singh, Mehakpreet, Saket Sarin, and Avneet Kaur.

2. The paper titled "**Deep Learning for Enhanced Spam and Phishing Detection**," authored by Kanishk Nagpal, Dr. Sunil K. Singh, Sudhakar Kumar, Japan Ajit Singh Gandhi, and Kartik.


Springer

3rd International Conference on Cyber Security, Privacy and Networking (ICSPN-2023)

Certificate of Participation

This is to certify that paper entitled "**Ransomware Resilience: Advancements in Detection and Mitigation Strategies for Real-World Threats**" authored by "**Chandra Kumari Subba, Sudhakar Kumar, Sunil K. Singh, Mehak Preet, Saket Sarin, and Avneet Kaur**" has presented in the 3rd International Conference on Cyber Security, Privacy and Networking (ICSPN-2023) organized during September 28-30, 2023 in Dubai, UAE (Virtual mode).

ICSPN-2023 Organizing Committee


Springer

3rd International Conference on Cyber Security, Privacy and Networking (ICSPN-2023)

Certificate of Participation

This is to certify that paper entitled "**Deep Learning for Enhanced Spam and Phishing Detection**" authored by "**Kanishk Nagpal, Sunil K. Singh, Sudhakar Kumar, Japan Ajit Singh Gandhi, Kartik**" has presented in the 3rd International Conference on Cyber Security, Privacy and Networking (ICSPN-2023) organized during September 28-30, 2023 in Dubai, UAE (Virtual mode).

ICSPN-2023 Organizing Committee

ORIENTATION AND CODE JAM SESSION

18th September, 2023

Event Details

CCET ACM and ACM-W Student Chapter organized an informative orientation session and an exciting coding event on September 18, 2023. The orientation session, led by speaker Aishita Sharma, welcomed attendees to the new academic year and introduced the dynamic new executive board. Attendees also gained insight into the diverse teams within ACM and ACM-W. Following the orientation, an engaging coding jam session was hosted, featuring activities aimed at promoting knowledge exchange among participants.

Utkarsh Chauhan led a captivating presentation and interactive discussions, enhancing the event with expertise and insights. With participation from over 100 enthusiastic students from various study branches, the event exceeded expectations, fostering a successful gathering and enriching the experience for all attendees.

Event Gallary

INTRODUCTION TO HACKTOBERFEST 2023

6th October, 2023

Event Details

On October 6, 2023, the CCET ACM and ACM-W student chapters hosted an informative event titled "Introduction to Hacktoberfest 2023." The event featured a presentation by Ruchika Thakur, the webmaster for CASC-W, providing attendees with insights into the open-source ecosystem. The event covered four key highlights:

1. Introduction to Open Source
2. Hacktoberfest - Background and Celebration
3. Git and GitHub: Tools driving open-source projects
4. Hands-on Session

Event Speaker

Attendees delved into Git and GitHub, essential tools for open-source projects, gaining practical insights and enhancing their skills through a hands-on session. With active participation across various disciplines, the event fostered an interactive and enriching experience for all.

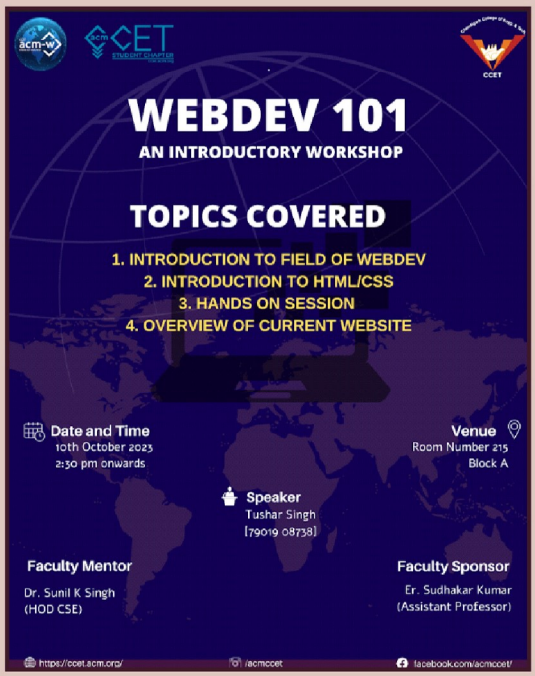
Ruchika Thakur
CO21352, CSE 2021

WEBDEV 101: AN INTRODUCTORY WORKSHOP

10th October, 2023

Event Details

On October 10, 2023, the CCET ACM and ACM-W student chapters collaborated to host an engaging web development workshop titled "WebDev 101: An Introductory Workshop." The event aimed to provide participants with a comprehensive understanding of web development, laying a solid foundation for web design and coding.



Event Speaker

Tushar Singh, the Webmaster for CASC, served as the event host, guiding attendees through essential skills required for creating visually captivating web pages and nurturing their design aesthetics. The workshop employed a well-rounded approach, integrating theoretical knowledge with hands-on coding sessions, ensuring participants gained both understanding and practical experience in web development.

Tushar Singh
CO21362, CSE 2021

BLOCKCHAIN AND ADVANCED DATA SCIENCE

Ayushi [MCO22384, CSE 2022]

Blockchain technology has been called the future of data science. But before jumping into how blockchain is helping in the advancement of data science we need to understand what the different terms mean.

Blockchain is a decentralized or distributed ledger that consists of multiple nodes. Since this is a decentralized system, the nodes are connected without any central server. This ledger can be accessed by anyone with a simple internet connection and is spread all across the globe. It stores an ever-growing list of records. These records are called blocks which are then linked together to form a chain of links. Just like its name, blockchain technology combines these blocks and revolves around the concept of a series of interconnected blocks. The initial idea for this technology was coined in 2008 but in recent years, it has gained a lot of popularity.

Data science on the other hand is the study of data to extract meaningful insights for business. It involves carefully collecting and analyzing the data to reach conclusions that would help in advancing the business. It combines a lot of practices such as computers, statistics, mathematics, artificial intelligence, machine learning, advanced analytics, etc. It analyses a large amount of data. It is very important in the modern world for smooth functioning and predicting future patterns. A big data set is of no use to a company or a huge corporation if there is no conclusion taken from it. Data scientists take this data, analyze it, and come to conclusions that are useful to the company.

We need to understand that in today's world data analysis and data science plays a vital role. The world's technology is advancing at a fast pace and with the rise of social sites and the whole world being on the internet, we get huge amounts of data. To utilize this explosive amount of data systematically, we need advancements in the data science field as well.

The increasing amount and diversity of data have also encouraged researchers to make business decisions by analyzing the big data generated. This has also caused the rapid development of the data science industry. However, there are still many challenges to be solved, especially data security and

privacy. Data security and privacy are very important and if any of the two is compromised then it would create a lot of problems.

Blockchain technology helps in this. The technology is decentralized and praised for its anonymity, security, and other characteristics. It has the power to change the way we share our information and how we access it. Blockchain technology can overcome some limitations in data science and promote the development of data science.

Blockchain technology can solve the trust problem in the Internet environment, to promote the rapid development of big data and the digital economy. The convergence of blockchain technology with data science can help in the advancement and provide various advantages.

Due to privacy problems, security issues, and the asymmetric flow of data, there are many limitations to the advancement of data science. Blockchain technology would promote the rapid employment of the economy as well as big data.

There are five benefits when we combine blockchain technology and data science. These are as follows :

1. Increased security and privacy

As stated earlier, privacy and data security are things that cannot be compromised and if they are, it would lead to some bad consequences. We need to understand that if a large amount of data is stored in a centralized location then there is always a risk of that data being lost or leaking of data. Blockchain technology offers a decentralized system and thus helps in overcoming this problem. This combination of data science and blockchain technology is most used in the healthcare industry and it should also be applied elsewhere.

2. Increased credibility and transparency

The convergence of the two technologies decreases human intervention. Both the resource owner and the subject making the access request can easily detect inappropriate authorization or access denial, thanks to publicly auditable evidence of misconduct. The combination of blockchain and data science can also improve the transparency of the industry.

3. Data analysis

The data that is stored in the blockchain is in a structured form and is complete which helps in further analysis. Blockchain not only makes big data even bigger but also contributes by making big data more secure and valuable, as blockchain big data is structured and ready for big data analytics. Data scientists can use these real-time, traceable, better-integrated

data for real-time analysis and optimization to achieve a global optimization model. This would also help in obtaining huge computing data.

4. Data Sharing

The blockchain technology has solved this problem to a certain extent. In the healthcare industry, data security plays an important role. Blockchain technology can be used in the field of healthcare to achieve a delicate balance between privacy and the accessibility of electronic medical records. This makes the system more trustworthy and efficient. Blockchain breaks the data into smaller silos but gives it more value.

5. Protection of Data sovereignty

No such way exists to find out who violates the data or who leaks it. Blockchain can further standardize the use of data and refine the scope of authorization, to protect the relevant rights and interests of data. When users try to access data sets, the verified smart contracts or transactions verify that users have access to the data, thereby ensuring the rights of data.

Some challenges like scalability, consensus upgrade, and intensified competition do exist but research is being done to overcome those. In conclusion, the convergence of blockchain technology in data science can lead to advancement in the field of data science.

ADVANCEMENTS IN THREAT INTELLIGENCE SHARING AND COLLABORATIVE DEFENSE MECHANISMS FOR ENHANCING CYBERSECURITY RESILIENCE

Tushar Singh [CO21362, CSE 2021]

INTRODUCTION

The ever-evolving cybersecurity landscape presents numerous challenges for organizations and individuals alike. To effectively combat these threats, collaborative defense and threat intelligence sharing have emerged as crucial strategies for enhancing cybersecurity resilience. This article delves into the multifaceted realm of collaborative defense and explores the benefits and challenges of threat intelligence sharing. By elucidating the shifting threat landscape and tracing threats from nuisances to sophisticated campaigns, this article highlights the need for organizations to pool their resources and expertise to stay ahead of adversaries. Additionally, it examines various types of threat intelligence and the advantages they offer in proactive threat detection. The article also addresses privacy concerns and the importance of standardization in sharing sensitive information. By striking the right balance between sharing actionable insights and protecting individual privacy, organizations can maximize the effectiveness of collaborative defense efforts. Through this exploration, it becomes evident that collaborative defense and threat intelligence sharing re essential components of a comprehensive cybersecurity strategy in today's interconnected world.

II. COLLABORATIVE DEFENSE MECHANISMS

In the face of escalating cyber threats and the limitations of traditional approaches, collaborative defense mechanisms have gained prominence as a proactive strategy to enhance cybersecurity resilience. Collaborative defense involves harnessing collective knowledge and resources across traditional boundaries to strengthen the overall security posture. This section explores three key elements of collaborative defense: real-time information exchange, proactive threat detection, and coordinated incident response.

A. Real-time Information Exchange

Real-time information exchange forms the cornerstone of collaborative defense. It enables swift sharing of threat intelligence across diverse entities, transcending geographical, sectoral, and organizational boundaries. By seamlessly and instantaneously sharing threat data, participating organizations can collectively anticipate and respond to emerging threats. This dynamiceco-system of mutual support fosters a proactive approach to cybersecurity, en-

abling organizations to fortify their defenses and stay ahead of adversaries. The section examines the underlying technologies and platforms that facilitate real-time information exchange, emphasizing the importance of interoperability and secure communication channels.

B. Proactive Threat Detection

Proactive threat detection is another crucial aspect of collaborative defense. By leveraging data analytics, machine learning, and artificial intelligence, organizations can identify potential threats before they materialize. Collaborative defense allows for the pooling of diverse analytical capabilities and expertise, strengthening the effectiveness of threat detection mechanisms. Through collaboration, organizations can analyze large datasets, identify patterns indicative of potential threats, and share actionable insights with other entities. This proactive approach empowers organizations to thwart attacks before they cause significant damage, reducing the impact on their systems and networks.

C. Coordinated Incident Response

Effective incident response is a cornerstone of cybersecurity resilience. In a collaborative defense framework, shared threat intelligence enables organizations to orchestrate synchronized response efforts. By leveraging real-time information exchange and proactive threat detection, organizations can minimize the impact of breaches and accelerate recovery. Collaborative incident response frameworks establish clear lines of communication, predefined roles, and a unified approach to mitigating and containing cyber incidents. By collectively managing the aftermath of an attack, organizations can significantly reduce downtime, financial losses, and reputational damage.

III. THREAT INTELLIGENCE SHARING

A. Types of Threat Intelligence

• Technical Indicators of Compromise: This type of threat intelligence includes specific artifacts or patterns that indicate a compromise or potential threat.

• Behavioral Patterns: Threat intelligence based on behavioral patterns helps identify malicious activities and anomalies in network traffic or user behavior.

• Strategic Insights: This type of threat intelligence focuses on understanding the motivations, tactics, and goals of threat actors.

B. Benefits of Threat Intelligence Sharing

• Accelerated Threat Detection: Collaborative sharing of threat intelligence enables organizations to detect threats more quickly, reducing the time to respond and mitigate potential damage.

• Improved Incident Response: By sharing threat intelligence, organizations

can enhance their incident response capabilities,enabling faster and more effective remediation.

• Enhanced Situational Awareness: Collaborative threat intelligence sharing provides a broader perspective on the threat landscape, enabling organizations to proactively adapt their defenses.

C. Challenges of Threat Intelligence Sharing

• Trust and Information Accuracy: Establishing trust among participants and ensuring the accuracy of shared threat intelligence can be challenging due to concerns about data quality and reliability.

• Cultural and Organizational Barriers: Different organizations may have varying levels of willingness to share information, and cultural barriers can hinder effective collaboration.

• Privacy and Legal Considerations: Sharing sensitive threat intelligence requires careful consideration of privacy laws, data protection regulations, and legal frameworks.

IV. TECHNOLOGICAL ENABLERS

In the evolving landscape of cybersecurity, the successful implementation of collaborative defense mechanisms relies on a range of technological enablers that ensure secure and efficient information sharing. This section of the article explores two pivotal enablers: blockchain technology and privacy-preserving techniques.

A. Blockchain and Secure Data Sharing

Blockchain technology offers inherent properties of transparency, immutability, and decentralization, making it a promising tool for secure data sharing in collaborative defense. By leveraging blockchain, participating organizations can establish trust and verify the authenticity of shared threat intelligence. The decentralized nature of blockchain ensures that no single entity
has control over the shared information, enhancing the overall security and integrity of the data. Additionally, blockchain has the potential to automate sharing agreements through smart contracts, ensuring compliance with predefined rules.

B. Privacy-Preserving Techniques

Threat intelligence sharing involves sensitive information, necessitating the implementation of privacy-preserving techniques. These techniques enable organizations to share valuable intelligence while safeguarding individual privacy. By employing anonymization, encryption, and access
control mechanisms, organizations can protect sensitive data and ensure that only authorized entities have access to it. Privacy-preserving techniques strike a balance between collaboration and privacy, allowing organizations to share critical information without compromising individual privacy rights. The successful implementation of collaborative

defense mechanisms heavily relies on these technological enablers. Blockchain technology provides a secure and transparent platform for sharing threat intelligence, while privacy-preserving techniques ensure the protection of sensitive information. By leveraging these enablers, organizations can establish trust, enhance data integrity, and foster effective collaboration in the fight against cyber threats.

CONCLUSION

In conclusion, collaborative defense mechanisms and threat intelligence sharing are essential components in enhancing cybersecurity resilience. By leveraging the collective strength of diverse entities, organizations can effectively detect and respond to dynamic cyber threats. The practice of sharing threat intelligence offers numerous benefits, including accelerated threat detection, improved incident response capabilities, and enhanced situational awareness. However, there are also challenges to overcome, such as privacy concerns and the need for standardized information sharing frameworks. Looking ahead, the future of collaborative defense holds transformative potential. Integration with autonomous systems and the utilization of artificial intelligence and machine learning algorithms can enable proactive defense strategies and empower organizations to stay ahead of adversaries. Cross-sector collaboration and the development of AI-driven predictive threat intelligence are also promising directions for the field. To navigate the evolving threat landscape, organizations must continue to invest in collaborative defense initiatives, refine their strategies, and foster a culture of information sharing. By doing so, we can collectively strengthen ourcybersecurity defenses and ensure a safer digital environment for all.

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

Simran Jaggi
CSE 2022

Vanshika Chilkoti
CSE 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

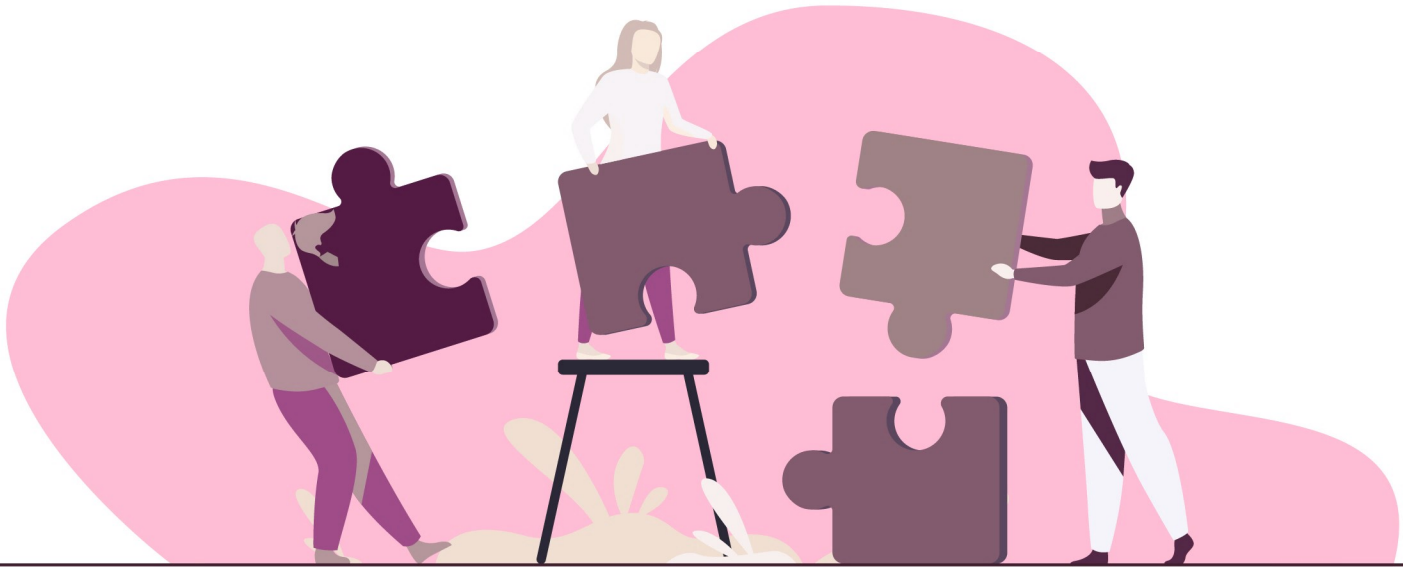
Priyanshu
Design Head

Ritika Gupta
External PR Head

Ayushi
Editorial Head

Avneet Kaur
Social Media Manager

Simran Jaggi
Event Manager



“Technology makes what was once impossible possible. The design makes it real.”

Michael Gagliano

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