

SEIRI

Security Education, Research, & Innovation Conference

Promoting Cybersecurity Education, Research and Innovation

 | **23rd Nov 2021**



PARTNER

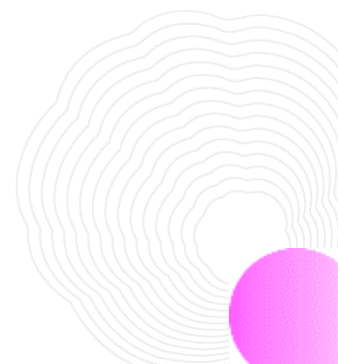


PUBLICATION PARTNER



CONTENTS

Inaugural of SERI 2021	3
Organizing Cyber Research	4
The rise of AI and automation in cyber security by Mr. Sree Hari Nagaralu, Principal Group	5
Presentation on 'Accelerating Cybersecurity Research and Innovation' by Vinayak Godse (Senior VP, DSCI)	5
Quad: Cyber Security Capabilities ... Collective efforts for Research and Education	6
National Interventions & Programs for Security Education	7
The decade of Security Discipline [2021-30] ... Agenda for Cyber Education	8
Hardware: security's frontier ... research use cases and Ideas	9
Crypto: Realizing Possibilities ... Strength of Modern Crypto	10
Distributed Security Model ... Why Does That Matter Now?	11
Security and Scale, Volume & Velocity ... Security Paradigm in Cloud	12
Cyber Maths ... Mathematics Behind Provenance, Observability, & automated reasoning concepts of security	13
Privacy: A new field ... throwing unprecedented, voluminous, complex, and intertwining problems	15
Cyber First ...This and Next Generation	16



Inaugural of SERI 2021 Ms. Rama Vedashree (CEO, DSCI)

Key messages:



**Rama
Vedashree**
CEO, DSCI

Academic institutes in India, especially the country's premier institutions such as NIT's, IIT's, and IISc, have undertaken cutting-edge research and have created pockets of innovation. To make a broader impact and engage the larger ecosystem comprising the industry, start-ups, emerging product companies, service organizations, and global R&D along with the community of researchers, academicians, and institutions, the National CoE envisaged the SERI 2021 conference.

The NCoE has been established with the vision to help incubate and facilitate technology development in some of the emerging deep tech areas, where the cybersecurity product ecosystem is scaling up. The NCoE is also focusing on bringing out future use cases that are important and strategic, for cybersecurity in India, for the academic community, industry, and the Government alike. In the past, the National CoE has hosted similar events such as the crypto innovation series, the lightweight cipher challenge, and calls for papers hosted by National CoE in the area of 5G and SCADA security. The National CoE has also supported research projects around IoT network traffic and lightweight image encryption techniques. The National CoE is also focusing on helping commercialize such research projects and reaching potential buyers in the market.

The Government is encouraging researchers, academicians, and students to take up R&D in cybersecurity. Many start-ups are now willing to begin their journey in the cybersecurity sector, and all stakeholders' adequate efforts to promote research and development will boost such efforts.

Shri Arvind Kumar – Scientist G, DG STQC & Group Coordinator Cybersecurity RnD, MeitY



**Shri. Arvind
Kumar**
MeitY, New Delhi

Each year, the SERI conference helps strengthen the earlier conversations and the numerous post deliberations taken on this platform. With the widespread adoption of digital technology and interconnected digital ecosystem, the risk of cyber threats is also increasing. To counter the challenges of novel cyber threats, a focus on cybersecurity research and development is a crucial aspect. Research institutions play a crucial role in enabling this. Similarly, upon completion of research objectives, productization of research is essential, and start-ups with a sustainable commercial model backed by cutting-edge technology are crucial. MeitY and DSCI have enabled the National Centre of Excellence (CoE) to lead the charter to develop and nurture this important ecosystem.

With advancements in technologies like 5G, lightweight crypto, IoT, more research on cybersecurity aspects needs to be carried out. The emergence of novel concepts like metaverse quantum computing will undoubtedly generate more demand for skilled and talented resources from this field.

Organizing Cyber Research

- **Prof. Manjesh Hanawal** - Associate Professor, IEOR Associated faculty, CMInDS, IIT Mumbai
- **Dr. Rajat Moona** - Director, Indian Institute of Technology Bhilai, GEC Campus
- **Mr. Sachin P Lodha** - Head, TCS's Cybersecurity and Privacy research

Moderator: Prof. Manendra Agarwal - Prof. Dept. of Computer Science, Deputy Director, IIT Kanpur



Prof. Manjesh Hanawal

Director of the UNSW
Institute for Cyber Security,
University of New South
Wales, Australia



Dr. Rajat Moona

Director,
Indian Institute of
Technology Bhilai
GEC Campus



Mr. Sachin P Lodha

Head
TCS's Cybersecurity and
Privacy research



Prof. Manendra Agarwal

Prof. Dept. of CSE, Deputy
Director IIT Kanpur,
IIT Kanpur
Moderator

Cybersecurity is multidimensional; hence, we need greater collaboration amongst researchers in this field compared to others. With focussed knowledge amongst the research community regarding challenges and potential research areas, organizing the agenda for cyber research will reap much more significant benefits for society. Several areas, such as Algorithm Security, Quantum Computing Security, Infrastructure Security, etc., offer exciting possibilities for researchers. Researchers can be benefitted by exploring such niche areas. One such area is around mathematical methodologies available to protect against attacks on present-day algorithms. Other areas include the concepts of security by design, end-to-end security, and availability of infrastructure.

Organizations do well in using technologies, algorithms, and infrastructure. They are now focussing on building a secure ecosystem and understanding how to incorporate security by design practically. More knowledge about cybersecurity and its linkages will help researchers understand and find weaknesses in algorithms and systems designing. Cybersecurity research and education require collective efforts and a consolidated approach. Several initiatives are underway in the country and are doing so systematically.

Attracting talent to cybersecurity

Cybersecurity is usually portrayed as a domain of problems and challenges, whereas profound awareness is required that this domain is rich with opportunities. There is a misconception about who can enter the field of cybersecurity, and generally, it is felt that this field requires extensive technical qualifications, work experience, certifications, etc. On the contrary, the cybersecurity profession offers excellent careers, growth opportunities, and handsome pay packages. With the evolving technology landscape, the need for extensive collaboration

between the Government, academia, and researchers in the security research area has increased significantly. Such developments are also helping create more awareness around the opportunities in cybersecurity.

Using India's technology-aware workforce and strengths in the IT services industry is undoubtedly an opportunity to embrace and nurture. Organizing forums to extract real-world challenges from such professionals and gaining insights around practical scenarios is one of the factors through which our country's researchers can produce a higher quality research output. Developing a curriculum for training people about facets of security research shall provide a shot in the arm.

The Rise of AI and Automation in Cyber Security

Mr. Sree Hari Nagaralu – Leading Security and Compliance Data Science Group, Microsoft



Mr. Sree Hari Nagaralu

Leading Security and Compliance Data Science Group, Microsoft

A combination of internal and external threats has been responsible for significant data breaches in the past. Data leakage has become an enormous challenge with the rapid proliferation of data-intensive methods and technologies. There are challenges in processing signals as data processing is massive. Data science can help in solving this challenge. Machine learning can help build models which are context-based and can better protect data. However, machine learning systems themselves can be attacked; for example, model theft, data poisoning, model stealing, adversarial machine learning attacks, and transfer learning attacks are a few of the threats surrounding the use of machine learning.

Currently, there is a need for standardization of ML models and AI risk management frameworks, with extensive research needed for securing AI/ML. This can be a huge enabler for security teams as they can use mission-critical ML systems by understanding and implementing ML model security and AI safety measures. This will make it possible to scale and meet an organization's most significant challenges while minimizing vulnerability and risk.

Presentation on 'Accelerating Cybersecurity Research and Innovation'

Vinayak Godse – Senior VP, DSCI



Vinayak Godse

Senior VP, DSCI

Gap in tracking cybersecurity research and innovation

Cybersecurity is a vast field and developing a standardized way to understand and track work undertaken in different aspects shall provide a fillip to cybersecurity research and innovation. People working in a particular domain find it challenging to learn about research being undertaken in another domain. DSCI is working towards filling the gap by compiling information around research from all fields and understanding the context of research being undertaken. For this, the National CoE has built a utility named "Cybersecurity Research Network (CSRN)." The utility provides a consolidated view of research in different areas and explores

specific research undertaken on various domains. The primary benefit of this utility is that it provides consumable research that helps understand ongoing projects better.

Need for improvements in the CSRN utility

To make CSRN more valuable, it needs the active participation of all researchers working in different cybersecurity domains. Researchers need to sign up and share their work on this portal. This will enable the utility to provide information about ongoing research and innovation in cybersecurity.

Quad: Cyber Security Capabilities ... Collective efforts for Research and Education

- **Ms. Aditi Chaturvedi** - Head, Law and Policy, Koan Advisory Group
- **Ms. Sonia Arakkal** - Policy Fellow, Perth US Asia center
- **Mr. Pranay Kotasthane** - Deputy Director, Takshila Institute

Moderator: Mr. Deepak Maheshwari - Public Policy Consultant

Utilizing capabilities or platform of Quad to counter cybersecurity challenges



**Ms. Aditi
Chaturvedi**

Head, Law and Policy,
Koan Advisory Group



**Ms. Sonia
Arakkal**

Policy Fellow,
Perth US Asia centre



**Mr. Pranay
Kotasthane**

Deputy Director,
Takshila Institute



**Mr. Deepak
Maheshwari**

Public Policy
Consultant
Moderator

Quad countries understand that self-sufficiency is not enough to counter global challenges. Embracing technology safely and securely needs interventions to tackle the growing threats in the global cyber supply chain. However, the global supply chain is heavily influenced by a regional Asian power. Thus, there is a need to build measures to provide better assurance over supply chain cybersecurity. At the same time, it is imperative to devise a strategy to develop an alternate supply chain utilizing the strengths of each of the Quad nations. Given such common purpose and concerns, the Quad can succeed in pursuing its agenda. Quad has a broader agenda to work on, including critical technologies and strengthening bilateral relations. However, multilateral/bilateral cooperation discussions are presently at a fundamental level. Moreover, the alignment of interests and values differs between Quad countries; for example, a popular video app considered an internal security threat in India did not have a similar perception of the other countries. Likewise, a large telecom conglomerate was under suspicion in all countries except India. Given their shared interests, many measures are being introduced to swiftly establish a shared understanding and approach to regional and global challenges and concerns. Technologies such as 5G, cybersecurity and semiconductors, etc., are emerging points of focus where such recognition of mutual interests will facilitate collaboration.

Quad countries may focus on the following areas to enhance cooperation:

- Start trusting each other's systems and enhance cooperation to build a trusted ecosystem.
- Develop interventions for collaboration amongst researchers, such as a Quad Centre of Excellence (QCoE).
- Explore opportunities for enhancing cooperation on key cybersecurity areas, for example, hardware security.
- Create platforms to enable the younger generation to have open conversations on critical challenges and solutions.
- Look beyond any traditional limitations such as varied geopolitical views established in the past to focus on intellectual knowledge sharing and cooperation.

National Interventions & Programs for Security Education

- **Prof. Vijay Varadharajan** - Global Innovation Chair in Cybersecurity, University of Newcastle, Australia
- **Mr. Rangeet Choudhury** - Principal Research Group Head - RnD, Microsoft India
- **Prof. V. Kamakoti** - Professor, Department of Computer Science, IIT Madras

Moderator: Ms. Rama Vedashree - CEO, DSCI



**Prof. Vijay
Varadharajan**
Global Innovation Chair
in Cybersecurity,
University of Newcastle,
Australia



**Mr. Rangeet
Choudhury**
Principal Research
Group Head - RnD,
Microsoft India



**Prof. V
Kamakoti**
Professor,
Department of
Computer Science,
IIT Madras



**Ms. Rama
Vedashree**
CEO,
DSCI
Moderator

With the fast pace of digitalization, information is being targeted by complex attacks. Along with cyber threats such as ransomware attacks, dark web utilization by cybercriminals is also becoming common. While cyber threats and attackers are upgrading themselves, cybersecurity defenders and budding professionals rely on content and curriculum, which is dated. To keep pace with the adversary or attempt to leap forward, Cybersecurity education and awareness, certifications, and formal education in security need a regular upgrade. A national-level security program that can provide enhanced visibility on the talent pipeline while enabling a quick resolution of issues hampering the cyber talent pipeline will go a long way in unifying pockets of innovation in the country today. A few years ago, the Government of India launched the Information Security Education and Awareness (ISEA) project for cybersecurity awareness, capacity development, and education. It has a user-friendly section for children, students, government officials, police, system administration, and women. The journey of ISEA pans

across different phases where the program has focussed on capacity building in Information Security and generating qualified human resources to meet the ever-evolving challenges through education. In the private sector, there have been several initiatives too. For example, Microsoft and DSCI have partnered on programs to train women engineers and train CXO's government employees, and create a pool of master trainers in cybersecurity. A coordinated system to consolidate gains is highly desirable in the future.

The Decade of Security Discipline [2021-30] ... Agenda for Cyber Education

- **Prof. Ryan Ko** - Professor (Cloud Security Pioneer), University of Queensland, Australia
- **Dr. Deepak Garg** - Dean, International relations & Corporate Outreach; HOD, Computer Science & Engineering, Bennett University
- **Prof. Sugata Sanyal** - Professor, School of Technology & Computer Science, Tata Institute of Fundamental Research

Moderator: Dr. Sriram Birudavolu - CEO, Cybersecurity Centre of Excellence, DSCI Hyderabad



**Prof. Ryan
Ko**

Professor (Cloud
Security Pioneer),
University of
Queensland, Australia



**Dr. Deepak
Garg**

Dean, International relations &
Corporate Outreach; HOD,
Computer Science & Engineering,
Bennett University



**Prof. Sugata
Sanyal**

Professor,
School of Technology &
Computer Science,
Tata Institute of
Fundamental Research



**Dr. Sriram
Birudavolu**

CEO, Cybersecurity
Centre of Excellence,
DSCI Hyderabad
Moderator

Cybersecurity is an essential enabler of digital transformation, and a lack of focus on cybersecurity can severely impact an organization. However, the field of cybersecurity is dealing with a perception problem. Usually, it is assumed by the masses that cybersecurity is synonymous with hacking, while few people understand that cybersecurity involves ensuring the security of digital systems. The need of the hour is to elaborate on how cybersecurity is intertwined with technological evolutions and is an integral part of modern technologies such as blockchain, AI/ML, autonomous IoT, etc. Likewise, the current cybersecurity curriculum provides essential building blocks to help students with fundamentals from a technology perspective but misses out on the bigger picture around its relationship with other fields. In the case of certification programs, much more needs to help professionals connect the dots with existing and upcoming technologies. The frequency of occurrence and sophistication of cyber threats in an increasingly volatile, uncertain, complex, and ambiguous world needs concerted efforts in education. Most courses are available today either offer a theoretical view or are tool-centric, thus leaving a knowledge gap where the practical application of these concepts is not well understood. Where practical aspects are covered, the depth of the scenarios is not adequate to help build a broader perspective. An active relationship between academicians, researchers, and professionals in an interdisciplinary domain will undoubtedly help create viable and sustainable solutions. This can certainly be aided by establishing platforms to share research and ideas. Developing future-ready education can make a huge difference and will be an important enabler for our society to embrace the benefits of digital transformation securely.

Hardware: Security's Frontier ... Research Use Cases and Ideas

- **Dr. Shivam Bhasin** – Co-PI & Thrust (iii) Lead Research for Advanced Hardware Evaluation Techniques for Modern Systems with Security and Privacy Features, NTU, Singapore
- **Prof. Vijaypal Singh Rathore** – Assistant Professor, IIT Jabalpur
- **Dr. S. Picek** – Assistant professor Radboud University, The Netherlands

Moderator: Prof. Debdeep Mukhopadhyay – Professor, IIT Kharagpur

Hardware security is an up-and-coming field of research around security. Classically, people get



Dr. Shivam Bhasin

Co-PI & Thrust (iii) Lead Research For Advanced Hardware Evaluation Techniques for Modern Systems with Security and Privacy Features, NTU, Singapore



Prof. Vijaypal Singh Rathore

Assistant Professor, IIT Jabalpur



Dr. S. Picek

Assistant professor Radboud University, The Netherlands



Prof. Debdeep Mukhopadhyay

Professor, IIT Kharagpur
Moderator

more bothered by a software attack, but gradually the industry is beginning to understand the importance of hardware security. Similarly, the security fraternity is primarily focused on protecting operating systems and applications.

Connected devices are used in a wide range of applications. They contain different types of valuable assets, which have been the target of increasing cyber-attacks, exploiting inherent weakness at the hardware level. Various attacks reported in the last few months have focused on the importance of hardware security. Hardware brings in new prose in terms of performance, enabling various cryptographic solutions and different cloud contexts such as hardware sharing with multiple entities. The whole security of AI is running on various low-level devices.

The key applications for real-life hardware security are centered around IoT devices. We often encounter such devices which use our data. While security for IoT devices is rarely built-in, it becomes important in the case of critical or safety-oriented applications. Another research problem in hardware security involves a hardware and AI perspective. Hardware security is a very newly known problem. It is the marriage of algorithms and hardware itself. When we run something using hardware, it is bound to have some footprints which are of interest to attackers. Researchers and industry are now looking to collaborate to fight problems in hardware security by sharing their learning and exploring what security by design must mean in real life. Another challenge arises due to the nature of the fabrication process of chips. The development of ICs requires different tools, from the design to the production stage. This introduces a broad attack spectrum on which several attacks are possible. Hardware that integrates security, protection,

and authentication is essential. Enhancing hardware functionality, performance, reliability, design, and verification from a security-enhanced perspective is a crucial goal of the invention, manufacturing, and deployment.

Crypto: Realizing Possibilities ... Strength of Modern Crypto to Realize Digitization/ Innovation Possibilities

- **Prof. Sourav Sen Gupta**, Lecturer-School of Computer Science, NTU Singapore
- **Dr. SK Hafizul Islam**, Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani
- **Mr. Ajit Hatti, Founder**, PureID

Moderator: Dr. Gaurav Varshney - Assistant professor, IIT Jammu

Today, people prefer using online applications that project themselves as end-to-end encrypted over traditional circuit-switched phone calls, primarily due to concerns over standard calls being



**Prof. Sourav
Sen Gupta**

Lecturer-School of
Computer Science,
NTU Singapore



**Dr. SK Hafizul
Islam**

Department of
Computer Science and
Engineering,
Indian Institute of
Information
Technology Kalyani



**Mr. Ajit
Hatti**

Founder,
PureID



**Dr. Gaurav
Varshney**

Assistant professor,
IIT Jammu
Moderator

vulnerable to interception. Cryptography has played a significant role in enabling such trust to be created in the eye of the end-user. Likewise, innovation possibilities around API security and interconnectivity with numerous entities have been fundamental in revolutionizing the entire payment ecosystem. Similar to the examples above, we know of numerous consumer-centric applications and technology that expose data to many interconnected systems. Thus, democratizing technology in the future will lean heavily on the developments in the crypto space.

Today, we are looking at information exchange between various environments and systems. At the same time, there is confusion around the concept of security and privacy and the role of cryptography in such a scenario. Privacy involves limiting results provided to another entity/application, and security is about protecting personal information. This confusion is primarily because there is a trend to focus on behavior-based patterns or personal factors such as biometrics and move away from using PKI. Such movements may reap benefits in the short run; however, there will be challenges in the future as biometric security gets embedded deeper in the ecosystem and is used for key functions such as authentication. The most daunting of all shall be the enormous cost of replacing and upgrading such systems. At the same time, storing such sensitive data will add more burden on organizations. Thus, there is a need to explore

leveraging the strengths of modern crypto to enable applications that help build better confidence amongst users and are feasible for organizations to support operationally.

Another important aspect to consider is the availability of skilled professionals in the crypto space. Currently, the workforce is not an issue for the crypto industry as a large community of researchers exists in India. Measures to improve and add to the current infrastructure and provide

Distributed Security Model ... Why Does That Matter Now?

- **Prof. Anwitaman Datta** - Associate Professor, Distributed Security Research Interest, NTU, Singapore
- **Dr. Surya Nepal** - Group Leader and Sr. Principal Research Scientist, Distributed Systems Security CSIRO, Australia
- **Dr. Pradeepthi K.V** - Assistant Professor, C R Rao Advanced Institute of Mathematics, Statistics and Computer Science and, University of Hyderabad Campus

Moderator: Floyd D'Costa - Founder, Block Armour



Prof. Anwitaman Datta

Associate Professor,
Distributed Security
Research Interest,
NTU, Singapore



Dr. Surya Nepal

Group Leader and Sr. Principal
Research Scientist,
Distributed Systems Security
CSIRO, Australia



Dr. K.V. Pradeepthi

Assistant Professor, C R Rao
Advanced Institute of
Mathematics, Statistics and
Computer Science, University
of Hyderabad Campus



Floyd D'Costa

Founder, Block Armour
Moderator

If we consider the broad environment today, there are three key trends.

1. The rapid adoption of cloud computing accelerated due to various digital transformation programs by the Government and companies.
2. The proliferation of billions of IoT devices.
3. Remote work environment.

These trends have resulted in a highly distributed IT environment which has overwhelmed traditional perimeter-based tools that businesses/organizations usually rely on. Security management requirements of modern-day organizations are thus becoming daunting. Such turmoil is aiding cyber adversaries as we witness a growing number of cyber-attacks. Typically, a distributed environment consists of trusted servers, trusted users, trusted administrators, untrusted clients, untrusted communication media, and intermediary systems. Traditional perimeter-based defenses are no longer sufficient as IoT, BYOD, and remote working bring are no longer within the purview of perimeter-based defenses. Several factors such as providing ubiquitous access to users, providing secure and reliable access to vendors and third parties, and dealing with heterogeneous environments are presenting challenges that are too

overwhelming for traditional methods to tackle. Centralization of security does not enable the current work environment.

Another important aspect for organizations to deal with is the value of assets in a distributed environment. Not all assets are of equal importance to the organization. This prioritization of the assets is critical to achieving success in a distributed environment. Zero trust is one of the referenced approaches in a distributed model, and it establishes a new norm where every transaction must be verified. As the physical perimeter has changed, focussing on identity as the main parameter can enable organizations to rethink perimeter-based security. The concept of NFT (Non-fungible tokens) is equivalent to identity and can be thought of as identity in distributed security models. Similarly, blockchain is a good case study for distributed security models. Further research is needed in blockchain applications for distributed security models.

Security and Scale, Volume & Velocity ... Security Paradigm in Cloud

- **Prof. Gaurav Somani** - Assistant Professor- CSE, Central University of Rajasthan
- **Dr. Sanjeet Kumar Nayak** - Assistant Professor, IIIT Kancheepuram
- **Dr. Rajkumar Buyya** - Distinguished Professor and Director of the Cloud Computing and Distributed Systems (CLOUDS) Laboratory, University of Melbourne, Australia

Moderator: Prof. Sateesh Kumar Peddoju - Associate Professor, IIT Roorkee



Dr. Gaurav Somani
Assistant Professor-CSE
Central University of Rajasthan



Dr. Sanjeet Kumar Nayak
Assistant Professor,
IIIT Kancheepuram



Dr. Rajkumar Buyya
Distinguished Professor
and Director of the Cloud
Computing and
Distributed Systems
(CLOUDS) Laboratory,
University of Melbourne,
Australia



Prof. Sateesh Kumar Peddoju
Associate Professor,
IIT Roorkee
Moderator

In the past, application development used to be a challenging task. With improvement in automation capability and cloud-enabled infrastructure, it is becoming easier. For example, the emergence of several low codes and no-code platforms has brought newer methods to bring applications to life. This is another example of the several uses of cloud-based technology. Since the last few years, data sharing amongst various applications and global systems has also significantly increased. The use of cloud computing has enabled us to achieve this. When we consider the security of a cloud environment, it is about basic elements such as infra, application, and access and the scale of operations and transactions. A higher number of transactions would require a faster means to analyze data associated with every transaction and securely enable each.

We need to consider security aspects at all levels of cloud architecture. There is a thin line between cloud security and traditional security from an approach perspective. In the cloud environment, the cloud service providers (CSP) take away physical security responsibility. However, what is important and primarily responsible for cloud-related breaches are the aspects for which cloud technology users are responsible. Ensuring proper access control plays an important role in cloud security. Logging and monitoring are equally important for cloud security. We usually consider cloud security from an SLA perspective and perceive that adding controls in the agreement shall provide complete coverage from a security standpoint; however, the core challenge around securely provisioning and configuring cloud services is the user's prerogative. To avoid data breaches in the first place, organizations must deploy strong access controls. In the case of DDoS attacks, CSPs/ISPs can play an important role. They can help in stopping the attack from its origin. Also, statistical methods can help in logging and monitoring. There needs to be more discussion on the shared responsibilities between the CSP and customers. Velocity, scalability, and security are all equally important goals for the cloud. These can only be attained when security teams embrace a cloud-centric security paradigm that leverages developments around automation and machine learning, thereby transitioning to a system where human dependency (and errors) can be minimized. This requires further development around security reasoning and decision-making technologies that can keep pace with the rapidly changing cloud security paradigm.

Cyber Maths ... Mathematics Behind Provenance, Observability, & automated reasoning concepts of security

- **Dr. Vireshwar Kumar** – Assistant Professor in the Department of CSE, IIT Delhi
- **Dr. Anindita Banerjee** – Adjunct Scientist Corporate R&D, C-DAC Pune
- **Dr. Shweta Agarwal** – Associate Professor-CSE, IIT Madras

Moderator: Prof. Saumitra Sanadhya - Associate Professor, IIT Jodhpur



**Dr. Vireshwar
Kumar**

Assistant Professor in
the Department of CSE,
IIT Delhi



**Dr. Anindita
Banerjee**

Adjunct Scientist
Corporate R&D,
C-DAC Pune



**Dr. Shweta
Agarwal**


Associate
Professor-CSE,
IIT Madras



**Prof. Saumitra
Sanadhya**

Associate Prof,
IIT Jodhpur
Moderator

Securing computers, connected devices, and data becomes increasingly complex each day. Mathematics plays a key role in preventing and modeling security breaches, and today several cybersecurity tools and algorithms are based on mathematical concepts. Mathematician Simon Singh once said that the 3rd world war would be a "mathematicians war" as mathematicians will have control over the next great weapon, "Information." Decision-making for cybersecurity involves several factors, context, etc., making it difficult for humans to evaluate and make recommendations/ decisions in real-time. There are scenarios today where thousands and millions of situations arise. Despite the best-trained security professional behind a tool, there is room for error, as not all data can be processed/understood. Such dependency on human factors




can be countered well with applied mathematical concepts in cybersecurity. Among several maths applications in cybersecurity, cryptography is the most widely used. Cryptography is as ancient as civilizations. While evaluating a cryptographic solution, it is important to understand its origin and evolution. Further, some shortcomings are equally important to factor in. First, human intelligence - there is no proof that crypto cannot be broken. Second, Quantum technology - even though we don't have large-scale quantum computers now, the threat from Quantum technology is real and needs more research towards the development of quantum-safe technology. This need has become more significant given the geopolitical developments in the past few years. Third, there is a possibility to have certain backdoors. Crypto security and cryptanalysis are some of the significant threats of super-polynomial algorithms.

Quantum analysis and quantum secure communication need quantum algorithms. There are several mathematical problems. Primarily, post-quantum crypto will be dominated by the Lattice problem, isogeny code-based problems, multiple polynomial equations, and several others. We have some algorithms proven on paper and some algorithms sufficiently robust to enable implementation on existing systems. There are specific methods such as formal verification and program verification, by which we can prove that these are secure. Securing crypto is a time-consuming and challenging task that takes significant effort. Standardization has been initiated across a few industries; for example, the telecom standards institute, Cloud Security Alliance (CSA), and NIST are all focusing on this area and devoting significant resources. Various white papers are available on the standardization process of quantum implementation, which can be referred to.

Security observability has the objective of enhancing protection through better monitoring. Observability parameters can be further fed with external and internal intelligence to determine the actual root cause of an alert and help organizations remediate it. These are also valuable for the verification of expected application performance. Instead of reacting to events that can cause disruption, observability tools can identify areas that should be addressed before significant incidents, and outages occur. For security observability to be genuinely successful, advanced analytical and data models are required.

Another important concept is provenance, primarily with its application to protect data integrity. Security provenance deals with providing mechanisms through which unwanted or unexpected changes to data can be detected. Recommended controls to be applied are determined by the context of threats, and these are mathematically processed. Similarly, we have already seen how automated reasoning uses mathematical proofs of correctness for complex systems. For example, by using automated reasoning, policies and network architecture configurations can be analyzed for locating unintended configurations that could potentially expose vulnerable data. To enable this model to work efficiently, a lot of data needs to be explored, which helps build better context around the user and the activity or transaction.



Privacy: A new field ... throwing unprecedented, voluminous, complex, and intertwining problems

- **Prof. Monica Whitty** – Director of the UNSW Institute for Cyber Security, University of New South Wales, Australia
- **Prof. Mohan Kankanhalli** – Dean of NUS School of Computing, Lead Principal Investigator, NUS Centre for Research in Privacy Technologies (NCRiPT), National University of Singapore
- **Prof. Sushmita Ruj** – Senior Research Scientist, CISRO's Data61 and UNSW Sydney check spelling on image

Moderator: Prof. Manoj Prabhakaran – Professor – CSE, IIT Mumbai



Prof. Monica Whitty

Director of the UNSW Institute for Cyber Security, University of New South Wales, Australia



Prof. Mohan Kankanhalli

Dean of NUS School of Computing, Lead Principal Investigator, NUS Centre for Research in Privacy Technologies (NCRiPT), National University of Singapore



Prof. Sushmita Ruj

Senior Research Scientist, CISRO's Data61 and UNSW Sydney



Prof. Manoj M. Prabhakaran

Professor- CSE, IIT Mumbai
Moderator

The protection of private data is a key responsibility for organizations today. Millions of applications are dealing with the data of billions of people. This presents a unique opportunity for newer ways to form privacy-preserving applications that are secure to use. Limiting the scope of data collection and preventing use beyond defined applications requires an effective strategy and deploying appropriate technology. Establishing a framework for data collection and protecting sensitive raw data in a secure environment are key goals for organizations. Zero-Knowledge proofs and Homomorphic Encryption are commonly used cryptographic techniques to ensure data privacy for several industry sectors. Zero-knowledge proofs are being used for generating evidence for personal attributes and transactions to preserve identity.

Meanwhile, Homomorphic encryption ensures privacy by allowing computations on encrypted data. Likewise, Trusted Execution Environments (TEEs) can be leveraged for protecting data in isolated hardware before an application can process it. This protects data just before, during, and after processing from attacks focusing on memory dumps, root user compromises, and other malicious exploits.

Privacy is not just a technical problem; it is also a socio-technical problem. There are a lot of contradictions in the privacy domain. While professionals in this domain talk about the importance of privacy and the role of security, users are convinced easily to give away their sensitive information to a random web portal in exchange for "free" services.

Data can be created and can be inherited by virtue of transactions. When we have a lot of data, we can do something useful with it, such as using AI/ML to extract insights from data.

Organizations are naturally inclined towards collecting more data as it can benefit them in several ways. At the same time, capable adversaries can breach any level of security. Hence, it is important to make it expensive to pursue organizations' valuable data. Healthy interaction between various parties and researchers may help better understand privacy needs. Methods to use technology to check compliance of any established rules for access to multiple classifications of data that an organization may have control over the need to evolve further to meet the requirements of a connected world.

Cyber First ...This and Next Generation

- **Prof. Farukh Kazi, Dean** - Research, Development and Consultancy, Veermata Jijabai Technological Institute (VJTI)
- **Prof. Tal Pavel** - Founder & Director, The Institute for Cyber Policy Studies, Israel
- **Prof. Muttukrishnan Rajarajan** - Director & Prof., Security Engineering & Institute of Cyber Security - University of London

Moderator: Ms. Kirti Seth - CEO, Sector Skill Council for IT/ITES, NASSCOM



**Dr. Farukh
Kazi**

Dean- Research,
Development and
Consultancy
Veermata Jijabai
Technological Institute
(VJTI)



**Prof. Tal
Pavel**

Founder & Director,
The Institute for Cyber
Policy Studies, Israel



**Prof. Muttukrishnan
Rajarajan**

Director & Prof.
Security Engineering &
Institute of Cyber
Security-University of
London



**Ms. Kirti
Seth**

CEO, Sector Skill
Council for IT/ITES,
NASSCOM
Moderator

The current decade is focused on three significant phenomena driven by the evolution of and adoption of Cloud, AI & ML, and Cybersecurity. To reap the benefits of digitalization, security shall need to be a fundamental enabler. To improve the overall cybersecurity posture, we must focus on enhancing security education. Cybersecurity education must start from the initial stage of primary education. For example, children nowadays use tablets smartphones for education and entertainment. They have other gadgets and technology around them. Older people are also part of the vulnerable group targeted by cybercriminals, and this is the most affected group. Ensuring that they are taught about cyber threats and risks will help introduce cybersecurity concepts.

Cybersecurity is an umbrella term, and several perspectives can be enclosed under it. Investments in making cybersecurity education and awareness mainstream will help improve the overall security posture. This shall also meet an important societal goal. Education and cyber awareness will also help individuals, organizations, and governments leverage technology for

innovation with higher confidence. We require significant effort to train and prepare students to understand cybersecurity and its interlinkages with other domains to achieve this. We also need a substantial attempt to update the curriculum to help students understand common cybersecurity threats. For the current generation, cybersecurity is an after-thought. To change this in the future, we need to orient the next generation to develop a cybersecurity engineering mindset and demystify concepts around security by design. The more significant challenge in cybersecurity is human behavior and psychology. Organizations must carefully analyze the user's behavior of their applications and services and accordingly create opportunities for collaboration with researchers and academicians to design more effective and less burdensome controls for technology users.



Security Education, Research, & Innovation Conference

Promoting Cybersecurity Education, Research and Innovation

Get in touch with us

Address : 4th Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303

Email : ncoe@dsci.in

