Adi Shankara
INSTITUTE OF ENGINEERING AND TECHNOLOGY
Ph: 0484-2463825
Email: info@adishankara.ac.in
Website: www.adishankara.ac.in

DEPARTMENT OF **ELECTRONICS AND COMMUNICATION ENGINEERING (ECE)**

EXPLORE, DREAM, DISCOVER

GENESIS

IGNITING THOUGHTS

MONTHLY NEWSLETTER

MARCH 2022 ISSUE 50

VISION

To be recognized at national and international level for excellence in education and research in Electronics and Communication Engineering.

MISSION

- Inculcating leadership qualities, adaptability and ethical values
- Imparting quality education in the field of electronics, communication, and related areas to meet the challenges in industry, academia and research
- Nurture the growth of each individual by providing a dynamic and conducive learning environment.

DEPARTMENT ACTIVITIES AND ACHIEVEMENTS

Industry Institute Interaction Program - Suyati Technologies

Manikandan A R and Libin Luvis of S5 EC (2019-23 batch) got selected for a paid internship of 10k/per month for the next phase of the project with Suyati Technologies under the industry-institute interaction program.

1. Libin Luvis: "E-commerce plugin" mentored by Arya Paul, Asst. Prof., ECE & Anuroop K B, Asst. Prof., ECE

Mr. Libin Luvis

Ms. Arya Paul

Mr. Anuroop K B

2. Manikandan A R: "Cloth detection" mentored by Dr. Bipin P R, Assoc. Professor.Dept. Of ECE.

Mr. Manikandan A R

Dr.Bipin P R

Mr. Anuroop K B, Asst. Professor, Department of Electronics and Communication won Second Prize in "Art of Teaching" competition conducted exclusively for all faculty members by GTECH (Group of Technology Companies, Kerala) in association with KTU as the University partner. The aim of this competition was to recognize teachers with creativity and innovation in teaching any engineering concept/topic.

APJ AKTU - CERD FUNDING: SHORTLISTED FOR PRESENTATION

Following projects from our department was shortlisted for presentation for student project under CERD funding by KTU

1. Project Titled "MED-MATE" proposed by Student investigators Aisha Mehrin K I, Aswani M Ravi, AUSHIN Jose Manjooran, Farhan Najeeb and Finto Shajan mentored by Ms. Aswathy N, Asst. Professor, Dept of ECE and Ms. Anju George Asst. Professor, Dept of ECE.

2. Project Titled "Dual control floor cleaning robot with sanitizing facility", proposed by Student investigators Abin P Xavier, Arjun Suraj, Govind VJ and Adeeb Abubacker mentored by Ms. Neema M Asst. Professor, Dept of ECE.

TEACHER'S ZONE

A SINGLE-PHOTON SOURCE WHICH CAN OPERATE IN ROOM TEMPERATURE PAVES THE WAY FOR PRACTICAL QUANTUM ENCRYPTION

Author: Ms Savitha Raghavan, Assistant Professor, Department of ECE

In the Optica Publishing Group journal Optics Letters, Zeng and colleagues from Australia University of New South Wales and Macquarie University describe their new single-photon source and show that it can produce over ten million single photons per second at room temperature. They also incorporated the single-photon source into a fully portable device that can perform Quantum Key Distribution (QKD). The new single-photon source uniquely combines a 2D material called Hexagonal Boron Nitride with an optical component known as a Hemispherical Solid Immersion Lens, which increases the source's efficiency by a factor of six.

Single photons at room temperature

QKD offers impenetrable encryption for data communication by using the quantum properties of light to generate secure random keys for encrypting and decrypting data. QKD systems require robust and bright sources that emit light as a string of single photons. However, most of today's single-photon sources don't perform well unless operated at cryogenic temperatures; hundreds of degrees below zero, which limits their practicality.

Although hexagonal boron nitride has previously been used to create a single-photon source that operates at room temperature until now researchers had not been able to achieve the efficiency needed for real-world application. "Most approaches used to improve hexagonal boron nitride single-photon sources rely on precisely positioning the emitter or using nano-fabrication," said Zeng. "This makes the device complex, difficult to scale and not easy for mass production."

Zeng and colleagues set out to create a better solution by using a solid immersion lens to focus the photons coming from the single-photon emitter, allowing more photons to be detected. These lenses are commercially available and easy to fabricate.

The researchers combined their new single-photon source with a custom-built portable confocal microscope that can measure the single photons at room temperature, creating a system that can perform QKD. The single-photon source and confocal microscope are housed inside a robust package that measures just 500 x 500 millimetres and weighs around 10 kilograms. The package is also engineered to deal with vibration and stray light.

"Our streamlined device is easier to use and much smaller than traditional optical table setups, which often take up entire labs," said Zeng. "This allows the system to be used with a range of quantum computing schemes. It could also be adapted to work with existing telecommunications infrastructure."

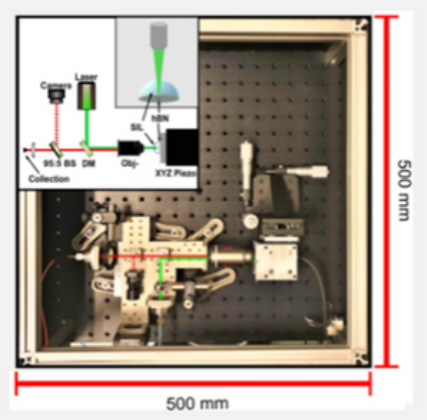

Fig: The single-photon source and confocal microscope are housed inside a robust package that measures just 500 x 500 millimeters and weighs around 10 kilograms.

Demonstrating quantum cryptography

Tests of the new single-photon source showed that it could achieve a single-photon collection rate of 107 Hz while maintaining excellent purity -- meaning each pulse had a low probability of containing more than one photon. It also showed exceptional stability over many hours of continuous operation. The researchers also demonstrated the system's ability to perform QKD under realistic conditions, showing that secured QKD with 20 MHz repetition rates would be feasible over several kilometers.

As the researchers have established proof that their portable device can perform complex quantum cryptography, they plan to perform further testing of its robustness, stability, and efficiency during encryption. They also plan to use the new source to perform QKD in real-world conditions, rather than inside the lab. "We are now ready to transform these scientific advances in quantum 2D materials into technology ready products," said Igor Aharonovich, who led the project.

Referances:

- Single-photon source paves the way for practical quantum encryption: New source is compact and operates at room temperature." Science Daily, 23 March 2022.
- H. X. J. Zeng, M. A. P. Nguyen, X. Ai, A. Bennet, A. Solntsev, A. Laucht, A. Al-Juboori, M. Toth, R. Mildren, R. Malaney, I. Aharonovich “Integrated Room Temperature Single Photon Source for Quantum Key Distribution,” Opt. Lett., 47, 7 (2022).

CYBER SECURITY

Author: Ms. Anna Paul, S8 ECE A

Cyber security is a fast-paced sector, with the growth of the internet, the dependence on computers has increased exponentially, and both the hackers and security providers seek to outsmart one another.

What is Cyber Security / Information Technology (IT) security?
The practice of protecting sensitive information and critical systems from digital attacks is known as Cyber security. It's designed to prevent threats to networked systems and applications, whether they come from within or outside of an organization.

Why Cyber Security?
Cyber security is crucial because it protects all sorts of information from being damaged or stolen by cyber attackers who wish to steal it and use it for malicious purposes. In today's world, People save massive amounts of data on laptops and other internet-connected gadgets. Sensitive data, personal information, governmental, and industrial data, protected health information (PHI), intellectual property, and personally identifiable information (PII) are all examples. The more we rely on the internet, the more we need good cyber security in all its forms.

Benefits of Cybersecurity
1. Protects Personal Information
2. Allows Employees to Work Safely
3. Better Website Security
4. Denies Spyware and prevents Adware
5. Assists in Remote Working
6. Enhanced Data Management

Different Types of Cyber Security Attacks
Some of the most common cyber security attacks are:

1. Phishing - It's a method of obtaining an individual's personal and sensitive information via email by impersonating a trustworthy entity in electronic communication. Identity theft is the goal of phishing, and personal information such as usernames, passwords, and credit card numbers can be used to steal money from user accounts. Vishing is the use of a telephone as a means of committing identity theft (voice phishing). Smishing is another type of phishing in which clients are enticed using SMS.

2. Denial of Service (DoS) Attacks - It's a cyber attack in which the network is chocked and, in some cases, collapsed as a result of pointless traffic overwhelming the network, and thus obstructing legitimate network activity.

3. Man-in-the-middle (MitM) attacks - This type of attack entails the cybercriminal intercepting conversations or data transmissions between multiple people. A cyber attack using an unsecured Wi-Fi network to intercept data sent from the victim's machine to the network is an example.

4. Social Engineering - This sort of attack uses human interactions to persuade users to breach security processes. To improve the possibility of the victim clicking on a link or downloading a file, cybercriminals frequently mix social engineering assaults with others, such as phishing.

5. SQL Injection - SQL stands for Structured Query Language. A SQL injection attempts to perform actions on data in a database and potentially steal it. It entails injecting malicious code via SQL statements and exploiting the flaws in data-driven programs.

6. Insider threats - It can include current or former workers, business partners, contractors, or anyone who has had access to systems or networks in the past and has abused their access permissions. Traditional security solutions such as firewalls and intrusion detection systems, which focus on external threats, may be blind to insider threats.

Cybersecurity Techniques

Some of the most common cyber security techniques are:

1. Authentication - It's a process of identifying an individual and guaranteeing that the person is the same who he or she claims to be. On the Internet, a username and password are common ways of authentication. With the rise in reported cases of identity theft via the internet, organizations have implemented additional authentication measures such as One Time Password (OTP), which is a password that can only be used once and is sent to the user via SMS or email at the mobile number or email address provided during the registration process.

2. Encryption - It's a method of transforming data into an unreadable form before sending it over the internet. Only the person who has access to the key is able to read it and convert it into a readable format. Encryption is formally described as a method of locking data by transforming it into complicated codes using mathematical techniques. Even the most powerful computer will take years to crack the code because it is so intricate. This secure code can be safely transmitted to the destination over the internet.

3. Digital Signatures - Digital signatures are used to not only validate data but also to authenticate it. Encrypting the data using the sender's private key creates the digital signature. The encrypted data is linked to the original message and forwarded to the intended recipient through the internet. With the sender's public key, the receiver can decrypt the signature. The original message is now compared to the decrypted message. If both are the same, the data has not been tampered with, and the sender's authenticity has been validated because only the owner's private key can encrypt the data, which can then be decrypted by his public key.

4. Antivirus - A special program called an anti-virus is used to prevent malicious codes from entering your system. It's designed to safeguard the system from viruses. It not only prevents the malicious code from entering the system but also identifies and eliminates the malicious code that has already been installed.

5. Steganography - A method for concealing secret messages in a document file, image file, program or protocol, etc. such that, the embedded message is invisible and can be retrieved using special software. Only the sender and receiver are aware of the secret message hidden in the image. The benefit of this method is that these files are difficult to suspect.

Counter Cybersecurity Initiatives in India

To counter cyber security attacks, the Government of India have many some initiatives which are listed below:

1. **National Crime Records Bureau (NCRB)** - NCRB shall endeavor to empower Indian Police with Information Technology and Criminal Intelligence to enable them to effectively & efficiently enforce the law & improve public service delivery. This will be accomplished through national and international collaboration with police forces, advancements in crime analysis technology, and the development of IT capabilities and IT-enabled solutions.
2. **National Cyber Coordination Center (NCCC)** - The proposed cyber security and e-surveillance body in India is the National Cyber Coordination Center. It'ss purpose is to screen communication metadata and coordinate other agencies' intelligence-gathering efforts. A cyber-attack prevention strategy, cyber-attack investigations, training, and other elements of NCCC include, among others, a cyber-attack prevention plan, cyber-attack investigations, and training.
3. **Crime and Criminal Tracking Networks and Systems (CCTNS) project of India** - It's a project under the National e-Government Plan (NeGP) that intends to build a statewide networking infrastructure for the creation of IT-enabled advanced tracking systems centered on "crime investigation and detection" (PTI, 2013). The CCTNS aims to make data and information collection, storage, retrieval, analysis, transmission, and exchange easier at police stations as well as between police stations, State Headquarters, and Central Police Organizations. CCTNS would give a comprehensive database for crimes and offenders, making it easier for law enforcement to track down a criminal who was traveling from one location to another.
4. **Computer Emergency Response Team-India(CERT-In)** - The Department of Information Technology established the Indian Computer Emergency Response Team in 2004. CERT-In was established with the goal of responding to computer security incidents, reporting vulnerabilities, and promoting appropriate IT security practices across the country. It is also in charge of overseeing the IT act's administration (CERT-In, 2014)

Recent Trends in CyberSecurity

1. **Automotive Hacking on the rise** - Today's vehicles are loaded with automated software that provides seamless connectivity for drivers in areas such as cruise control, engine timing, door locks, airbags, and advanced driver aid systems. These automobiles connect using Bluetooth and WiFi, which exposes them to a number of vulnerabilities and hacker threats. With more automated vehicles on the road, the usage of microphones for eavesdropping and gaining control of the vehicle is predicted to increase in 2022. Self-driving or autonomous vehicles rely on a more complicated process that necessitates stringent cybersecurity safeguards.
2. **Potential of Artificial Intelligence (AI)** - With AI being implemented across all market areas, this technology, together with machine learning, has resulted in significant improvements in cybersecurity. In the development of automated security systems, natural language processing, facial detection, and autonomous threat detection, AI has played a critical role. It is also being used to create smart malware and attacks in order to get around the most up-to-date data security mechanisms. Threat detection systems with AI can forecast new assaults and immediately inform administrators of any data breaches.
3. **Mobile is the New Target** - In thelast few years, there was a cyber security trends predict a significant increase (50 percent) in mobile banking malware or attacks, making our mobile devices a target for hackers. Individuals are more at risk from all of our images, financial transactions, emails, and communications. A smartphone virus or malware may attract the attention of cybersecurity trends at any time

4. **Cloud is Also Potentially Vulnerable** - With more and more businesses moving to the cloud, security measures must be constantly checked and updated to protect data from leaks. Despite the fact that cloud programs of Google or Microsoft are well-equipped with security on their end, the user end is still a major source of erroneous mistakes, malicious software, and phishing assaults.
5. **Data Breaches: Prime target** - Organizations all over the world will continue to be concerned about data. Protecting digital data, whether for an individual or a business, is the primary priority right now. Any tiny hole or bug in your system browser or program might be used by hackers to gain access to vital data. New stringent regulations have been enacted. The General Data Protection Regulation (GDPR) went into effect on May 25, 2018, providing individuals in the European Union with data protection and privacy (EU). Similarly, the California Consumer Privacy Act (CCPA) went into effect on January 1, 2020, to protect consumer rights in the state of California is in effect since , Jan 20
6. **IoT with 5G Network: The New Era of Technology and Risks** - The Internet of Things will usher in a new era of interconnectivity with the arrival and growth of 5G networks (IoT). This communication across numerous devices exposes them to outside influence, assaults, or an unknown software bugs, making them vulnerable attacks, or software bugs. Even Chrome, the world's most popular browser, which is sponsored by Google, has been proven to have severe flaws. 5G architecture is a relatively new technology in the market, and it necessitates extensive research to identify security flaws and make the system secure from external assault. Every stage of the 5G network could result in a slew of network assaults that are unaware of. To prevent data breaches, manufacturers must create sophisticated 5G hardware and software with extreme caution.
7. **Automation and Integration** - With the amount of data growing by the day, it is imperative that automation must be implemented to provide more sophisticated management of the data. Professionals and engineers are under increasing pressure to produce rapid and effective solutions in today's demanding work environment, making automation more useful than ever. To design more safe software in every element, security metrics are incorporated within the agile process. Large and complicated online applications are even more difficult to secure, necessitating the inclusion of automation and cyber security as essential concepts in the software development process.
8. **Targeted Ransomware** - Targeted ransomware is another critical cybersecurity trend that we can't be to ignored. Industries, particularly in western countries, rely largely on specialized software to manage their daily operations. These ransomware targets are more targeted, such as the Wanna Cry ransomware attack on NHS hospitals in England and Scotland, which infected over 70,000 medical devices. Though ransomware often threatens to reveal the victim's data until a ransom is paid, it can also impact huge organizations or countries.
9. **State-Sponsored Cyber Warfare** - There will be no truce between the western and eastern powers in their quest for supremacy. Though the attacks are rare, they have a big impact on an event such as elections, such as tensions between the US and Iran or Chinese hackers. With more than 70 elections expected this year, the criminal activity would likely increase throughout this period. High-profile data breaches, as well as political and industrial secrets, are expected to be the top cybersecurity trends in 2022.
10. **Insider Threats** - One of the most common causes of data breaches is human mistakes. A single bad day or purposeful loophole can bring a whole corporation down, resulting in millions of dollars in stolen data. According to Verizon's research on data breaches, which provides strategic insights on cybersecurity trends, employees were directly or indirectly responsible for 34% of all attacks. As a result, be sure to raise awareness among employees to ensure that data is protected in every way possible.

STAFF ACHIEVEMENTS

Dr.Bobby Mathews, HOD

- Participated in a Faculty Development Program (FDP); "Artificial Intelligence & Machine Learning"; from 28/02/22 to 05/03/22 conducted by KMCT College of Engineering, Calicut.
- Selected as Technical Member for the Evaluation Panel - Darsana - IGNITE 2022.

Dr. VT Gopakumar

- Submitted Proposals for funding of around 14 lakh/10 lakh at MSME, Govt of India
  - Secure Industrial and Home Automation using human veins
  - AI based road accident reduction and fast settlement of road accidents.

Mr. Jayesh T P

- Participated in Faculty Development Program on "Artificial Intelligence & Machine Learning" from 28/02/2022 to 05/03/2022 conducted by KMCT College of Engineering for Women.

Ms. Aswathy N

- Published Paper titled; "Review on role of nanoscale HfO2 switching material in resistive random access memory device" Emergent Materials; Springer Nature; February 2022.

Ms. DIVYA V CHANDRAN

- Participated in Faculty Development Programme on "Artificial Intelligence & Machine Learning from 28/02/2022 to 05/03/2022 conducted by KMCT College of Engineering for Women.
- Published a paper titled; "Vegetation Scanning Using LiDAR-Based Drone"; International Journal of Scientific Research in Computer Science, Engineering and Information Technology; Feb 2022.

STUDENT ACHIEVEMENTS

BATCH	NAME	PROGRAM	CONDUCTED
2021-25	SREERAG	Cyber security	Simply learn
2021-25	SREYAS KUMAR C V	Data Science for Beginners	BOARD INFINITY
2021-25	SREYAS KUMAR C V	Responsive Web Design	Free Code Camp
2021-25	NAZILA K N	Data Science	NASSCOM
2021-25	UTHARA C P	Data Science for Beginners	Future skills
2021-25	GAYATHRI VISWANATH	Deep leaning	NIT
2020-24	NOEL MATHEW SHILLOW	5 day internship on introduction to Autocad	Techmaghi

EDITORIAL BOARD

DR BOBBY MATHEWS C
HEAD OF DEPARTMENT(HOD).
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

MS ANJANA S
ASSISTANT PROFESSOR
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

MS NEETHA K
ASSISTANT PROFESSOR
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

MS HRIDAYA U MALLIA
S7 ECA

MS KAVYA G PADIYAR
S7 ECB

MR SAMUEL SABU THOMAS
S5 ECB

MS RESHMI R
S5 ECB

MS TITYA RAMCHANDRAN
S3 ECB

MS SEREEN SABU
S3 ECB

MS DILNA DAVISAL
S3 ECA

MS ASWATHY MANOJL
S3 ECA