ATME College of Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CS MAIL

NEWSLETTER VOLUME 10, ISSUE II, AUG 2022

Dear Readers,

It is with great pleasure that we bring you **Volume 10, Issue II** of our department newsletter **"CS MAIL"**. The current newsletter highlights the activities of the department, achievements of faculty and students during the past six months. It also features workshop organized and attended, paper publication details and other social activity undertaken from CS Department. Your valuable comments and suggestions are appreciated.

We wish all the readers an enjoyable reading.

VISION OF THE DEPARTMENT

To develop highly talented individuals in Computer Science and Engineering to deal with real world challenges in industry, education, research and society.

MISSION OF THE DEPARTMENT

- To inculcate professional behavior, Strong ethical values, innovative research capabilities and leadership abilities in the young minds & to provide a teaching environment that emphasizes depth, originality and critical thinking.
- Motivate students to put their thoughts and ideas adoptable by industry or to pursue higher studies leading to research.

PROGRAM EDUCATIONAL OBJECTIVES (PEO'S)

- Empower students with a strong basis in the mathematical, scientific and engineering fundamentals to solve computational problems and to prepare them for employment, higher learning and R&D.
- Gain technical knowledge, skills and awareness of current technologies of computer science engineering and to develop an ability to design and provide novel engineering solutions for software/hardware problems through entrepreneurial skills.
- Exposure to emerging technologies and work in teams on interdisciplinary projects with effective communication skills and leadership qualities.
- Ability to function ethically and responsibly in a rapidly changing environment by applying innovative ideas in the latest technology, to become effective professionals in Computer Science to bear a life-long career in related areas.

PROGRAM SPECIFIC OUTCOMES (PSO'S)

- Ability to apply skills in the field of algorithms, database design, web design, cloud computing and data analytics.
- Apply knowledge in the field of computer networks for building network and internet-based applications.

Message From Principal

ATMECE has emerged as a prominent institute offering quality education. All round continuous changes in infrastructure and academics standard have helped us to build a brand name. It gives me immense pleasure to introduce the **Volume 10, Issue II** of the half yearly newsletter **"CS MAIL"** of Computer Science Department. I am pleased to know that the newsletter will showcase the activities and credentials of CS&E department. I hope this will become a platform for students and staff to exhibit their talents in science and technology. On behalf of management, I appreciate the newsletter committee for their efforts in bringing out this edition.

I wish the editorial all success!!!

Regards
Dr L Basavaraj
Principal,
ATMECE

Don't wait for opportunity create it

Message From Chief Editor

Dr Puttegowda D
HoD, CS&E

Department of Computer Science & Engineering commits to work towards developing dedicated professional with a rich blend of competent, technical, managerial and social skills to contribute nation building. I am happy to inform that our department newsletter **"CS MAIL"** is being released in the month of Aug 2022. The newsletter encourage departments technical activities and also motivate students to bring out their innovative ideas , hidden talents and also provide a common platform to share their knowledge, in turn gain technical knowledge.

I wish all the readers an enjoyable reading!!!

TOPPERS

4th sem		
USN	STUDENT NAME	SGPA
4AD20CS032	KAVANA K R	9.5
4AD20CS034	LAKSHMI CHANDRASEKER	9.3
4AD21CS404	MOHAMMED ARSHAD	9.0

6th sem		
USN	STUDENT NAME	SGPA
4AD19CS003	AMOGH P	9.375
4AD19CS007	ANIRUDH NITIN BAKARE	9.25
4AD19CS042	MOHAMED FAROOQ HAGALWADI	9.0

8th sem		
USN	STUDENT NAME	SGPA
4AD18CS072	SHASHANK K	10.0
4AD19CS408	KHUTEJATUL KUBRA	9.83
4AD18CS001	ADVIYA SABA	9.67

EDITORIAL TEAM

A DREAM BECOMES A GOAL WHEN ACTION IS TAKEN TOWARD ITS ACHIEVEMENT

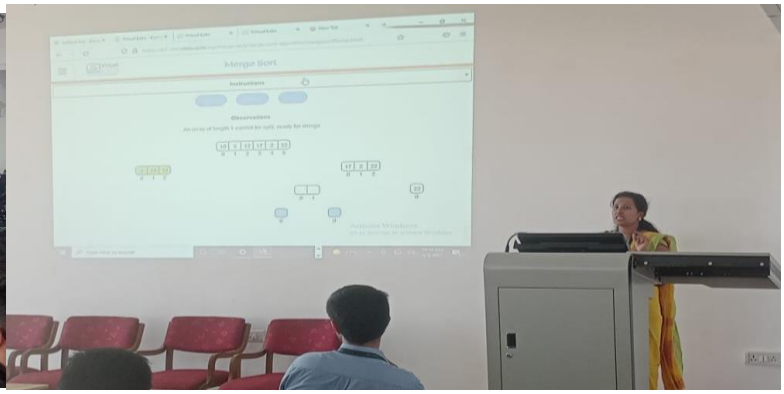
DEPARTMENT ACTIVITIES

Workshop on Awareness on Virtual Lab & Its Utilization

The Department of Computer Science and Engineering, ATME College of Engineering, Mysore organized A one-day workshop on "Awareness on Virtual Lab and its utilization" was organized for the 3rd Semester Students of Computer Science & Engineering Students on 05/03/2022.

The main aim of the workshop is to bring the awareness on the Virtual Lab and utilization in the regular curriculum. The workshop was inaugurated by Dr. Govinde Gowda M S, Dean Academics, ATME College of Engineering, Mysuru. Dr. Puttegowda D, Prof. & Head Department of Computer Science & Engineering, ATME College of Engineering, Mysuru presided over the function.

In his inaugural address, he spoke about the importance of learning and how virtual lab is contributing has a blended learning tool by enhancing the better understanding of the concepts learnt. He also insisted the students to go through the experiments of the V-labs before actually conducting the experiment in the physical lab. This will bring a better understanding and the deep learning among the concepts learnt. And also informed the students to use the virtual labs not only for the lab component but also this can be used to substitute the theory concepts learnt in the few of the courses in the regular curriculum.



Also, the students were taken to hands on session on the Virtual lab portal, where they were guided about how to use the web portal, search for experiments, choosing the experiment to conduct and its simulation.

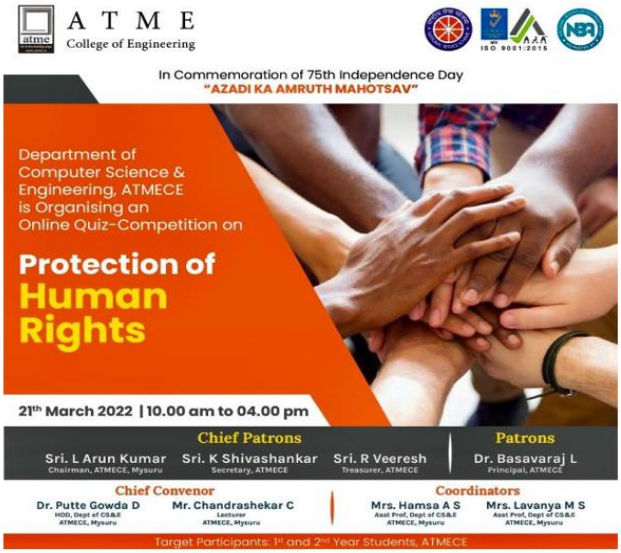
Students worked on the Virtual lab platform and had hands on experience in conducting experiments and learnt the navigation in Virtual lab Platform.

Sl.	Lab Conducted	Coordinator	Department
1	Data Structures - Merge Sorting	Sushma V	Computer Science & Engineering

PROTECTION OF HUMAN RIGHTS - Online Quiz Competition

The Department of Computer Science & Engineering in commemoration of 75th Independence Day has organized Online Quiz Competition “PROTECTION OF HUMAN RIGHTS” on 21st March 2022.

The main objective of this event was to awaken the knowledge & the basic insights on the Protection of Human rights, which are basic rights that belong to all of us simply because we are human. They embody key values in our society such as fairness, dignity, equality and respect. They are an important means of protection for us all, especially those who may face abuse, neglect and isolation. Human rights constitute a set of rights and duties necessary for the protection of human dignity, inherent to all human beings, irrespective of nationality, place of residence, national or ethnic origin, colour, religion, language, or any other status.



SERB Sponsored 3-Day Seminar

Department of Computer Science and Engineering, ATME College of Engineering organized a 3-Day National Level Seminar on "Research Avenues in Artificial Intelligence and Allied Areas" in association with Science and Engineering Research Board (SERB), New Delhi a statutory body of the Department of Science and Technology (DST), Government of India, from 24th - 26th March, 2022.

The department has received a partial grant of Rs. 80000/- from SERB, New Delhi. This program aimed to provide opportunities to acquire research skills in the domain of AI and its allied areas such as Machine Learning, Natural Language Processing, IoT, Cloud Computing, and Cyber Security. Registration for the seminar was open to engineering students, research scholars, academicians, and industry people. In total, 61 registrations were received for the event. This included 25 faculty members, 16 research scholars, 04 industry people, 06 UG and 10 PG students. All participants received a welcome kit that included a button file, a note book, and a pen.

The 3-day Seminar event comprised of 10 plenary sessions and we invited 10 distinguished

academicians from premier institutes and universities to share their views and research experiences in AI. Each speaker was given one and half-hours time to present, followed by 5 to 10 minutes to address questionnaires. The event was conducted in both online and offline modes together.

CSEISMIC – 2022 (Two days College Level Technical Events)

The Department of Computer Science & Engineering has organized 2 days' College Level Technical events CSEISMIC - 2022 on 30th June & 1st July 2022.

Day 1: 30/06/2022

The day started with Dr. Puttegowda, Professor and Head, Department of CSE addressing the students and briefing them about the technical events. Mr. Anil Kumar C J briefed about the rules of the technical events. The following are the events conducted.

- Blind coding
- Code debugging
- Quiz
- Code relay
- Hackathon

Day 2: 01/07/2022

The day started with the Hackathon conducted from 9:30 AM to 4:00 PM, and event Code Relay from 11:00 AM to 12:30 PM.

Totally 10 teams participated in the Hackathon. Two rounds of evaluation were conducted and the Juries were DR. J V Gorabal, Professor, Department of CSE and Dr. Deepu R, Professor, Department of CSE.

The winners of the event are,

Blind Coding:
First Prize: Lakshmi C 4th semester CSE
Second Prize: Nikitha 4th semester CSE

Code Debugging:
First Prize: Muzammil Husain Shantageri 4th semester CSE
Second Prize: Mohammed Labeeb 4th semester CSE

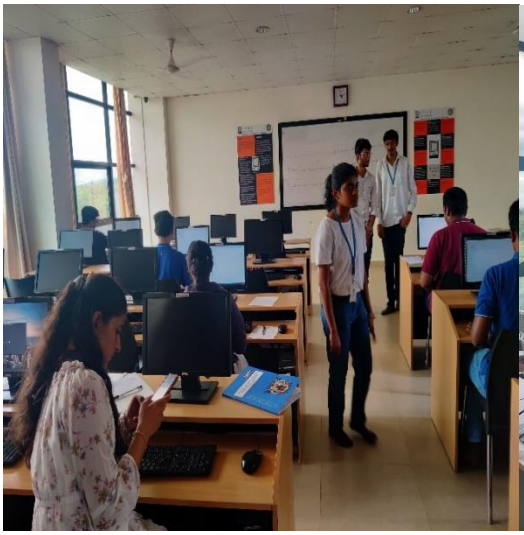
Technical Quiz:
First Prize: Mohammed Rayan Khan, Mohammed Afnan M and Hashim Farooq sheikh of 2nd semester CSE.
Second Prize: Manvitha B, Kavya L G and Kavya G D of 6th semester CSE.

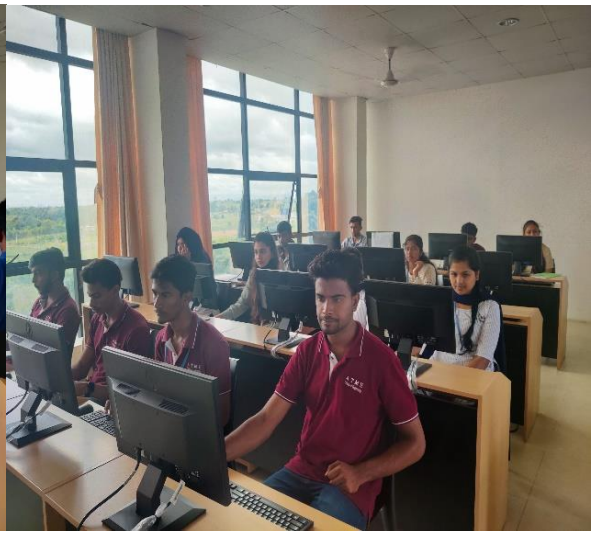
Hackathon:
First Prize: Pratheek B, Prerana N and Pramod B S of 6th semester CSE.

Second Prize: Pooja S, Sharya G and Sneha N of 2nd semester CSE.

Code Relay:

First Prize: Mithilesh A, Mohamed Farooq Hagalwadi and Mohamed Raihan of 6th semester CSE.





FACULTY PARTICIPATION

CONFERENCES

1. Sunitha Patel,Dr.Srinath S **," Automotive Imbalance Dataset Analysis and Solution using Deep Learning Algorithms",** River Publishers Series in proceedings - Intelligent Systems- Proceedings of ICIS, April 2022
2. Kiran B**," Parking space detector",** Proceedings of ICRTST, July 2022
3. Kavya P O**," Brain tumor detection using image Segmentation",** Proceedings of ICRTST, July 2022
4. Kiran B**," E-commerce product rating based on customer reviews",** Proceedings of ICRTST, July 2022
5. AnilKumar C J**," Robust human activity recognition using multimodal feature level fusion",** Proceedings of ICRTST, July 2022
6. Sneha N P**," Motorcyclist helmet rule violation detection using deep learning",** Proceedings of ICRTST, July 2022
7. Dr. Puttegowda D**," Deep learning based container for text recognition",** Proceedings of ICRTST,
   July 2022
8. Dr. J V Gorabal**," Offline Signature validation using Image processing",** Proceedings of ICRTST, July 2022
9. Raghuram A S**," Food waste management and donation app",** Proceedings of ICRTST, July 2022
10. Sushma V**," AI chatbot for collage website",** Proceedings of ICRTST, July 2022
11. Dr.Nasreen Fathima**," Traffic clearance for Ambulance using Deep learning",** Proceedings of ICRTST, July 2022
12. Anil Kumar C J**," Face recognition at Varying angles",** Proceedings of ICRTST, July 2022
13. Raghuram A S**," A review detection of offensive language using social media",** Proceedings of ICRTST, July 2022
14. Sushma V**," Credit card fraud detection using machine learning",** Proceedings of ICRTST, July 2022
15. Dr. Deepu R**," Paddy leaf disease detection using Machine Learning",** Proceedings of ICRTST, July 2022
16. Lavanya N**," Wheat variety identification using deep learning",** Proceedings of ICRTST, July 2022

17. Sushma V,**" Division and Replication of data in cloud",** Proceedings of ICRTST, July 2022

18. Sushma V,**" Plant health monitoring system using IOT",** Proceedings of ICRTST, July2022

JOURNALS

1.Dr. Naveen N. M., Mr. Sourabh G Patil, Mr. Veer Jadimath, Dr. Mahantesh C. Elemmi, Dr. Pritam Dhumale, Mr. Shreyas Deshpande**," Development of a Framework for Ideal Water Management of a Household in a Smart City Environment",** Journal of Computer Science Engineering and Software Testing,Feb 2022

2. Naveen N. Malvade, Rajesh Yakkundimath, Girish B. Saunshi, Mahantesh C. Elemmi**," Paddy variety identification from field crop images using deep learning techniques",** International Journal of Computational Vision and Robotics,Feb 2022

3. Sunitha Patel Dr. Srinath S**," Performance Evaluation of Support Vector Machine: Before and After Image Data Augmentation",** International Journal of Engineering Trends and Technology,Feb 2022

4. Sunitha Patel Dr. Srinath S**," Multi-vehicle detection in a platooning system using an image processing model with a machine learning approach",** DogoRangsang Research Journal, Feb 2022

5. Anil Kumar C J, Raghavendra B K, Dr.Raghavendra**," A Credit Scoring Heterogeneous Ensemble Model Using Stacking and Voting",** Indian Journal of Science and Technology, Feb 2022

6. Dr.

6. Nasreen Fathima Dr. Reshma Banu Dr. G F Ali Ahammed**," A Signature-based Data Security and Authentication Framework for Internet of Things Applications"**, International Journal of Electrical and Computer Engineering (IJECE),June 2022

7. Hamsa AS Sushma V**, "LID Systems for Speech Processing Systems",** International Journal of Creative Research Thoughts,June 2022

8. Sushma V, Hamsa AS**," Collabaration of blockchain in healthcare 4.0",** International Journal of Advance Research in Computer and Communication Engineering, June 2022

9. Roopa B, Pallavi V R, Raksha S, Rakshitha R**", Real-Time Face Mask Detection Using Deep Learning",** International Journal of Innovative Research in Technology,July 2022

10. Dr. Deepu R., Suman K.M., S. S. Surabhi, Nischal S., Nisarga P.**," Personality Analysis through Graphology",** International Journal of Innovative Science and Research Technology, July 2022

11. Lavanya N, Syed Suhail, Nithin DB,Syed Hameed UR Rahman**," Driver Drowsiness Detection Using Machine Learning and OpenCV",** International Journal of Innovative Science and Research Technology, July 2022

12. Sneha N P, Kavyashree D L, Kavya G T, Bhoomika S R, Chandana M V**," A Study On Camouflaged Object Detection Methods"**, International Journal of creative research thoughts (IJCRT), July 2022

13. Adviya Saba, Ayesha Sidddiqua, Bharath R, Darshan S, Hamsa AS," **Video Based Moving Vehicle Detection and Speed Estimation System using Machine Learning"**, International Journal of Innovative Research in Computer and Communication Engineering, July 2022

14. Lakshmi Durga, Deepu. R**," A self-adaptive cognitive deep learning framework for classifying graphology features to Big five personality traits",** International Journal of Advanced Technology and Engineering Exploration, July 2022

TECHNICAL ARTICLES

"Applications of Computer Science in biometrics"

Biometrics are body measurements and calculations related to human characteristics. Biometric authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological characteristics which are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor/scent, voice, shape of ears and gait. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to mouse movement, typing rhythm, gait, signature, behavioral profiling, and credentials. Some researchers have coined the term **behaviometrics** to describe the latter class of biometrics.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

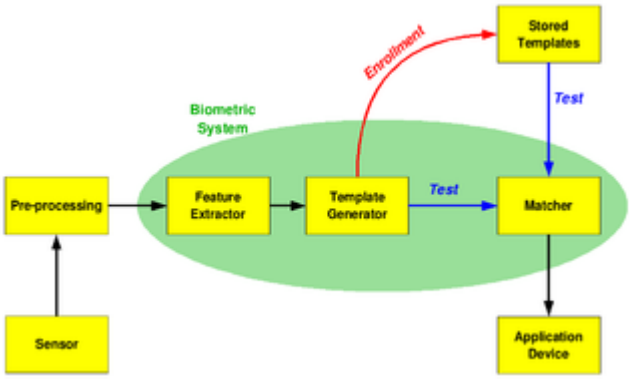
Biometric Functionality

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication. Biometric authentication is based upon biometric recognition which is a advanced method of recognising biological and behavioural characteristics of an Individual.

- Universality means that every person using a system should possess the trait.
- Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time. More specifically, a trait with *good* permanence will be reasonably invariant over time with respect to the specific matching **algorithm**.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- Performance relates to the accuracy, speed, and robustness of technology used (see performance section for more details).
- Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.

- Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.
-

Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security. No single biometric will meet all the requirements of every possible application.



The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. The third step is the testing step. This process may use a smart card, username, or ID number (e.g. PIN) to indicate which template should be used for comparison. *Positive recognition* is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

Biometric Island examining facial image 2D and 3D, voice timbre, and verifying handwritten signature

Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in

identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for *positive recognition* (so that the user does not have to provide any information about the template to be used) or for *negative recognition* of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition, such as passwords, PINs, or keys, are ineffective.

The first time an individual uses a biometric system is called *enrollment*. During enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the

Multimodal biometric system

Multimodal biometric systems use multiple sensors or biometrics to overcome the limitations of unimodal biometric systems. For instance, iris recognition systems can be compromised by aging irises and electronic fingerprint recognition can be worsened by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken passcode).

Performance

The discriminating powers of all biometric technologies depend on the amount of entropy they are able to encode and use in matching. The following are used as performance metrics for biometric systems:

- **False match rate** (FMR, also called FAR = False Accept Rate): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.
- **False non-match rate** (FNMR, also called FRR = False Reject Rate): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected.
- **Receiver operating characteristic** or relative operating characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FMR and the FNMR. In general, the matching algorithm performs a decision based on a threshold that determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FMR but increase the FNMR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

- **Equal error rate** or crossover error rate (EER or CER): the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.
- **Failure to enroll rate** (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low-quality inputs.
- **Failure to capture rate** (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- **Template capacity**: the maximum number of sets of data that can be stored in the system.

Adaptive biometric systems

Adaptive biometric systems aim to auto-update the templates or model to the intra-class variation of the operational data. The two-fold advantages of these systems are solving the problem of limited training data and tracking the temporal variations of the input data through adaptation. Recently, adaptive biometrics have received a significant attention from the research community. This research direction is expected to gain momentum because of their key

promulgated advantages. First, with an adaptive biometric system, one no longer needs to collect a large number of biometric samples during the enrollment process. Second, it is no longer necessary to enroll again or retrain the system from scratch in order to cope with the changing environment. This convenience can significantly reduce the cost of maintaining a biometric system. Despite these advantages, there are several open issues involved with these systems. For mis-classification error (false acceptance) by the biometric system, cause adaptation using impostor sample. However, continuous research efforts are directed to resolve the open issues associated to the field of adaptive biometrics.

Recent advances in emerging biometrics

In recent times, biometrics based on brain (electroencephalogram) and heart (electrocardiogram) signals have emerged. An example is finger vein recognition, using pattern-recognition techniques, based on images of human vascular patterns. The advantage of this newer technology is that it is more fraud resistant compared to conventional biometrics like fingerprints. However, such technology is generally more cumbersome and still has issues such as lower accuracy and poor reproducibility over time.

On the portability side of biometric products, more and more vendors are embracing significantly miniaturized biometric authentication systems (BAS) thereby driving elaborate cost savings, especially for large-scale deployments.

Animal biometrics

Rather than tags or tattoos, biometric techniques may be used to identify individual animals: zebra stripes, blood vessel patterns in rodent ears, muzzle prints, bat wing patterns, primate facial recognition and koala spots have all been tried.

Privacy and discrimination

It is possible that data obtained during biometric enrollment may be used in ways for which the enrolled individual has not consented. For example, most biometric features could disclose physiological and/or pathological medical conditions (e.g., some fingerprint patterns are related to chromosomal diseases, iris patterns could reveal sex, hand vein patterns could reveal vascular diseases, most behavioral biometrics could reveal neurological diseases, etc.). Moreover, second generation biometrics, notably behavioral and

electro-physiologic biometrics (e.g., based on electrocardiography, electroencephalography, electromyography), could be also used for emotion detection.

There are three categories of privacy concerns:

1. Unintended functional scope: The authentication goes further than authentication, such as finding a tumor.
2. Unintended application scope: The authentication process correctly identifies the subject when the subject did not wish to be identified.
3. Covert identification: The subject is identified without seeking identification or authentication, i.e. a subject's face is identified in a crowd.

Danger to owners of secured items

When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off a man's finger when attempting to steal his Mercedes-Benz S-Class.

Attacks at presentation

In the context of biometric systems, presentation attacks may also be called "spoofing attacks".

As per the recent ISO/IEC 30107 standard, presentation attacks are defined as "presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system". These attacks can be either impersonation or obfuscation attacks. Impersonation attacks try to gain access by pretending to be someone else. Obfuscation attacks may, for example, try to evade face detection and face recognition systems.

Several methods have been proposed to counteract presentation attacks.

Surveillance humanitarianism in times of crisis

Biometrics are employed by many aid programs in times of crisis in order to prevent fraud and ensure that resources are properly available to those in need. Humanitarian efforts are motivated by promoting the welfare of individuals in need, however the use of biometrics as a form of surveillance humanitarianism can create conflict due to varying interests of the groups involved in the particular situation. Disputes over the use of biometrics between aid programs and party officials stalls the distribution of resources to people that need help the most. In July 2019, the United Nations World Food Program and Houthi Rebels were involved in a large dispute over the use of biometrics to ensure resources are provided to the hundreds of thousands of civilians in Yemen whose lives are threatened. The refusal to cooperate with the interests of the United Nations World Food Program resulted in the suspension of food aid to the Yemen population. The use of biometrics may provide aid programs with valuable information, however its potential solutions may not be best suited for chaotic times of crisis. Conflicts that are caused by deep-rooted political problems, in which the implementation of biometrics may not provide a long-term solution.

Cancelable biometrics

One advantage of passwords over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. If the electronic biometric identifier is stolen, it is nearly impossible to change a biometric feature. This renders

the person's biometric feature questionable for future use in authentication, such as the case with the hacking of security-clearance-related background information from the Office of Personnel Management (OPM) in the United States.

Cancelable biometrics is a way in which to incorporate protection and the replacement features into biometrics to create a more secure system. It was first proposed by Ratha.

"Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. If a cancelable feature is compromised, the distortion characteristics are changed, and the same biometrics is mapped to a new template, which is used subsequently. Cancelable biometrics is one of the major categories for biometric template protection purpose besides biometric cryptosystem." In biometric cryptosystem, "the error-correcting coding techniques are employed to handle intraclass variations." This ensures a high level of security but has limitations such as specific input format of only small intraclass variations.

Several methods for generating new exclusive biometrics have been proposed. The first fingerprint-based cancelable biometric system was designed and developed by Tulyakov Essentially, cancelable biometrics perform a distortion of the biometric image or features before matching. The variability in the distortion parameters provides the cancelable nature of the scheme. Some of the proposed techniques operate using their own recognition engines, such as Teoh and Savvides whereas other methods, such as Dabbah take the advantage of the advancement of the well-established biometric research for their recognition front-end to conduct recognition. Although this increases the restrictions on the protection system, it makes the cancellable templates more accessible for available biometric technologies.

Proposed soft biometrics

Soft biometrics are understood as **not strict biometrical** recognition practices that are proposed in favour of identity cheaters and stealers.

Traits are physical, behavioral or adhered human characteristics that have been derived from the way human beings normally distinguish their peers (e.g. height, gender, hair color). They are used to complement the identity information provided by the primary biometric identifiers. Although soft biometric characteristics lack the distinctiveness and permanence to recognize an individual uniquely and reliably, and can be easily faked, they provide some evidence about the users identity that could be beneficial. In other words, despite the fact they are unable to individualize a subject, they are effective in distinguishing between people. Combinations of personal attributes like gender, race, eye color, height and other visible identification marks can be used to improve the performance of traditional biometric systems. Most soft biometrics can be easily collected and are actually collected during enrollment. Two main ethical issues are raised by soft biometrics. First, some of soft biometric traits are strongly cultural based; e.g., skin colors for determining ethnicity risk to support racist approaches, biometric sex recognition at the best recognizes gender from tertiary sexual characters, being unable to determine genetic and chromosomal sexes; soft biometrics for aging recognition are often deeply influenced by ageist stereotypes, etc. Second, soft biometrics have strong potential for categorizing and profiling people, so risking of supporting processes of stigmatization and exclusion.

Data protection of biometric data in international law

Many countries, including the United States, are planning to share biometric data with other nations.

In testimony before the US House Appropriations Committee, Subcommittee on Homeland Security on "biometric identification" in 2009, Kathleen Kraninger and Robert A Mocny commented on international cooperation and collaboration with respect to biometric data, as follows:

To ensure we can shut down terrorist networks before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Just as we are improving the way we collaborate within the U.S. Government to identify and weed out terrorists and

other dangerous people, we have the same obligation to work with our partners abroad to prevent terrorists from making any move undetected. Biometrics provide a new way to bring terrorists' true identities to light, stripping them of their greatest advantage—remaining unknown.

According to an article written in 2009 by S. Magnuson in the National Defense Magazine entitled "Defense Department Under Pressure to Share Biometric Data" the United States has bilateral agreements with other nations aimed at sharing biometric data. To quote that article:

Miller [a consultant to the Office of Homeland Defense and America's security affairs] said the United States has bilateral agreements to share biometric data with about 25 countries. Every time a foreign leader has visited Washington during the last few years, the State Department has made sure they sign such an agreement.

Likelihood of full governmental disclosure

Certain members of the civilian community are worried about how biometric data is used but full disclosure may not be forthcoming. In particular, the Unclassified Report of the United States' Defense Science Board Task Force on Defense Biometrics states that it is wise to protect, and sometimes even to disguise, the true and total extent of national capabilities in areas related directly to the conduct of security-related activities. This also potentially applies to Biometrics. It goes on to say that this is a classic feature of intelligence and military operations. In short, the goal is to preserve the security of 'sources and methods'.

India's national ID program

India's national ID program called Aadhaar is the largest biometric database in the world. It is a biometrics-based digital identity assigned for a person's lifetime, verifiable online instantly in the public domain, at any time, from anywhere, in a paperless way. It is designed to enable government agencies to deliver a retail public service, securely based on biometric data (fingerprint, iris scan and face photo), along with demographic data (name, age, gender, address, parent/spouse name, mobile phone number) of a person. The data is transmitted in encrypted form over the internet for authentication, aiming to free it from the limitations of physical presence of a person at a given place.

About 550 million residents have been enrolled and assigned 480 million Aadhaar national identification numbers as of 7 November 2013. It aims to cover the entire population of 1.2 billion in a few years. However, it is being challenged by critics over privacy concerns and possible transformation of the state into a surveillance state, or into a Banana republic. The project was also met with mistrust regarding the safety of the social protection infrastructures. To tackle the fear amongst the people, India's supreme court put a new ruling into action that stated that privacy from then on was seen as a fundamental right. On 24 August 2017 this new law was established.

Malaysia's MyKad national ID program

The current identity card, known as MyKad, was introduced by the National Registration Department of Malaysia on 5 September 2001 with Malaysia becoming the first country in the world to use an identification card that incorporates both photo identification and fingerprint biometric data on a built-in computer chip embedded in a piece of plastic.

Besides the main purpose of the card as a validation tool and proof of citizenship other than the birth certificate, MyKad also serves as a valid driver's license, an ATM card, an electronic purse, and a public key, among other applications, as part of the Malaysian Government Multipurpose Card (GMPC) initiative, if the bearer chooses to activate the functions.

BETTER ENVIRONMENT,BETTER TOMORROW..

“GO GREEN, BREATHE CLEAN”

Dear Readers,

Your advice or suggestions will be much appreciated and are most welcome!!!

Please mail your articles to csdept@atme.in

Setting goals is the first step in turning the invisible into visible