

**A THREE-DAY
INTERNATIONAL CONFERENCE
ON
A PRIMER ON INTELLECTUAL
PROPERTY RIGHTS....
(EMPHASIS ON COMPUTER ETHICS)**



**ORGANISED BY
DEPARTMENT OF COMPUTER SCIENCE
ANDHRA LOYOLA COLLEGE
(AUTONOMOUS)**

"A college with potential for excellence"
**Re-accredited at A+ Grade with 3.66/4.00
points**

**Vijayawada - 520008, A.P., India
www.andhraloyolacollege.ac.in**

On 9th, 10th & 11th March 2023

Message from Rector



Rev. Fr. Bala Showry. S. J.,
Rector
Andhra Loyola College
Vijayawada -5200 08

As the Rector of this institution, I believe it is essential that we understand the legal and ethical implications of our actions in the digital world. The issue of intellectual property rights and computer ethics is becoming increasingly important in our society, and it is essential that we are well-informed on these matters.

Intellectual property rights are fundamental to protect the creative work of individuals and organizations. This conference will provide a platform for us to discuss the legal framework of intellectual property rights, including copyright, patents, trademarks, and trade secrets. We will also explore the importance of respecting the rights of others and how to obtain permission to use their work.

Computer ethics is equally crucial in this digital age. We will examine the moral and ethical implications of technology and how it affects our lives. This includes the responsible use of social media, the prevention of cyberbullying and online harassment, and the protection of our privacy.

As an institution of higher learning, it is our responsibility to educate ourselves and others about these important issues. We must strive to use technology ethically and responsibly to create a better and more just society. I thank the department for taking the initiative to organize this conference.

I encourage all students and faculty members to attend this conference, and to actively participate in the discussions and activities. Together, we can create a better understanding of intellectual property rights and computer ethics and ensure a more just and ethical digital world for all.

Thank you, and I look forward to seeing you all at the conference.

Rev. Fr. Bala Showry. S. J.,
Rector
Andhra Loyola College
Vijayawada -5200 08

Message from Correspondent



Rev. Fr. Dr. M. Sagayaraj, S. J.,
Correspondent
Andhra Loyola College
Vijaywada - 5200 08

I feel greatly encouraged to see the Department of Computer Science taking initiative in conducting three-day international Conference on “**A Primer on Intellectual Property Rights (Emphasis on Computer Ethics)**” for making available yet another platform for the interested faculty, research scholars and student to learn from the deliberation during the conference. As you may know, intellectual property rights are legal protections that grant creators and innovators exclusive rights to their creations, inventions, and ideas. These rights include patents, trademarks, copyrights, and trade secrets, among others.

Intellectual property rights are important because they encourage innovation and creativity, and provide an incentive for individuals and companies to invest in research and development. By protecting these rights, society encourages individuals and companies to invest in new technologies, ideas, and creative works, which can lead to new products and services that benefit society as a whole. They also protect the interests of the creators or inventors by giving them the exclusive rights to their works, which can lead to economic benefits and increased market share.

However, there is a balance that must be struck between protecting intellectual property rights and ensuring that they do not impede innovation or harm consumers. Some individuals and organizations may use intellectual property laws to stifle competition or limit consumer choice, which can ultimately harm society's progress.

As we move forward, it is important that we continue to strike this balance and ensure that intellectual property rights are used fairly and responsibly to promote innovation, creativity, and economic growth. By doing so, we can continue to foster an environment of innovation and creativity that benefits society as a whole.

Thank you for your time and attention for participating to this conference.

Rev. Fr. Dr. M. Sagayaraj, S. J.,
Correspondent
Andhra Loyola College
Vijaywada - 5200 08

Message from Principal



Rev. Fr. Dr. G. A. P. Kishore, S. J.,
Principal
Andhra Loyola College (Autonomous)
Vijayawada – 5200 08

I am glad that our Department of Computer Science is organizing a three-day International Conference on “A Primer on Intellectual Property Rights (Emphasis on Computer Ethics)” in association with SOLETE (Society for Learning Technologies, India) to explore the intersection of these two critical topics - Intellectual Property Rights and Digital Technology – and the ways to protect and manage the intellectual property in this digital age.

As all of us know, the rapid advancement of Digital Technology has presented new challenges for the management and protection of intellectual property. The ease with which digital content can be copied and shared has made it more difficult to enforce intellectual property rights and prevent infringement.

This is where Computer Ethics come into play. As we navigate these new challenges, we must also consider the ethical implications of our actions when it comes to intellectual property. At their core, the intellectual property rights are designed to promote innovation, creativity, and economic growth. By protecting the rights of inventors, authors, artists, and other creators, intellectual property laws encourage the development of new ideas, products, and services that can create jobs, improve quality of our lives, and drive economic progress.

I sincerely hope that this Conference will discuss these critical issues in depth and find proper solutions for protecting intellectual property in this digital age while also ensuring that our actions are ethical and responsible.

Rev. Fr. Dr. G. A. P. Kishore, S. J.,
Principal
Andhra Loyola College (Autonomous)
Vijayawada – 5200 08

Message from Vice Principal



Rev. Fr. Dr. Lourdhraj Ignacimuthu S.J.,
Vice Principal,
Andhra Loyola College, Vijayawada – 5200 08

I am pleased to welcome you to this conference on intellectual property rights and computer ethics. As we all know, technology is advancing at an unprecedented rate, and it is becoming increasingly important for us to understand the legal and ethical implications of our actions in the digital world.

Intellectual property rights are essential to protecting the creativity and innovation that drives our economy. We must ensure that we respect the intellectual property rights of others, including copyright, trademarks, and patents. This means that we cannot use or reproduce the work of others without their permission, and we must also ensure that we do not infringe on their trademarks or patents.

Computer ethics, on the other hand, is about understanding the moral and ethical issues surrounding the use of technology. We must be aware of the impact our actions have on others, including online privacy, cyberbullying, and online harassment. It is our responsibility to ensure that we use technology in a responsible and ethical manner, and that we respect the rights and dignity of others.

As educators, it is important that we teach our students about these important issues. By doing so, we can help them become responsible digital citizens who understand the importance of intellectual property rights and computer ethics.

I hope that this conference will provide you with valuable insights and knowledge about these topics, and that you will be able to take this information back to your schools and communities. Together, we can help build a better and more ethical digital world.

Thank you for your attention, and I wish you all a productive and informative conference.

Rev. Fr. Dr. Lourdhraj Ignacimuthu S.J.,
Vice Principal,
Andhra Loyola College, Vijayawada – 5200 08

Message from Organizing Secretary



Dr. K. B. S. Sastry
Organizing Secretary (PIPR-2023)
Department of Computer Science
Andhra Loyola College, Vijayawada- 5200 08

I am pleased to invite you to our upcoming conference on intellectual property rights and computer ethics. As the Organizing Secretary of this event, I believe that it is essential that we understand the legal and ethical implications of our actions in the digital world.

Intellectual property rights are essential to protect creativity and innovation. The conference will provide valuable insights into copyright, trademarks, patents, and other legal issues related to intellectual property. We will also discuss the importance of respecting the rights of others and the importance of obtaining permission to use their work.

Computer ethics is an essential topic for discussion in our current digital age. We will explore the moral and ethical implications of technology and how it affects our lives. Cyberbullying, online harassment, and privacy concerns are just a few examples of the issues we will discuss.

As professionals, it is our responsibility to understand these issues and to educate others. This conference will provide an opportunity for us to exchange ideas and knowledge and to learn from experts in the field.

I urge you to join us for this important event and to share your insights and experiences. Together, we can help create a more just and ethical digital world.

Thank you for your attention, and I look forward to seeing you at the conference.

Dr. K. B. S. Sastry
Organizing Secretary (PIPR-2023)
Department of Computer Science
Andhra Loyola College, Vijayawada- 5200 08

Message from Convener



Mr. S. A. B. Nehru
Convener (PIPR-2023)
Andhra Loyola College
Vijayawada- 5200 08

I am delighted to welcome you all to our conference on intellectual property rights and computer ethics. As the Convener of this event, I believe that it is essential that we understand the legal and ethical implications of our actions in the digital world.

Intellectual property rights are crucial to protect creativity and innovation. This conference will provide valuable insights into copyright, trademarks, patents, and other legal issues related to intellectual property. We will also discuss the importance of respecting the rights of others and the importance of obtaining permission to use their work.

Computer ethics is a topic that affects us all in our daily lives. We will explore the moral and ethical implications of technology and how it affects our personal and professional lives. Cyberbullying, online harassment, and privacy concerns are just a few examples of the issues we will discuss.

As professionals, it is our responsibility to understand these issues and to educate others. This conference will provide an opportunity for us to exchange ideas and knowledge and to learn from experts in the field.

I urge you to take advantage of this opportunity and to share your insights and experiences with us. Together, we can help create a more just and ethical digital world.

Thank you for your attention, and I look forward to a productive and informative conference.

Mr. S. A. B. Nehru
Convener (PIPR-2023)
Andhra Loyola College
Vijayawada- 5200 08

Contents

S.No	Title of the Article	Page No
1	The Potential of AI in Medicine Chilukoti Divya Chandrika (DAI-12)	1
2	AI IN SPORTS DAI 10 - P. Rajeswari , DAI 34 - B. Sai Priyanka Singh	2
3	An Advanced CKD Detection using Deep Learning Mr Venkata Siva Narasimha G, Dr KBS Sastry, PVS Sairam	3
4	AI For Disabled K. Pragathi (Dai 18), S. Vyshnavi Bhavana (Dai 42)	4
5	Brain Tumor Detection using Deep Learning A.Radhika, A.Lakshmi Prasanna	5
6	Face Mask Prediction using deep Learning Techniques Manubolu Greeshma Priya (DPM-51), Kopanathi .Lavanya(DPM-53)	6
7	Liver Disease Prediction using Machine Learning P Dhana Lakshmi(DCM-39), Macharla Pallavi(DPM-61)	7
8	Deep Learning for Computer Vision Sk. Firoz (DCM03) , N. Dange Naveen (DCM36), N. Naga Pavan (DCM05)	8
9	Credit Card Fraud Detection Using Adaboost and Majority Voting G.Chandan Sai(DMC 47), T.Mohan Teja(DMC 45)	9
10	Driver Drowsiness Detection G.Sravani(DMC 39), K.Raja Rajeswari(DMC 40)	10
11	Enhancing Cloud Security Using Order Preserving Encryption and Audit Server Based Verification Ramanjaiah Ganji, Dr.Suresh Babu Yalavarthi	11
12	Enhancing Fastag with Software Jalaluddin Pathan	12
13	Ethics of Computer Science in Modern Era Polimetla vinay	13
14	Expression Detection using Ensemble Models LNageswari Devi, A.Sandhya Rani	14
15	Housing Price Prediction Using Linear Regression S. Yamini Durga (DMC-41), M.Niharika (DMC-50)	15
16	Intellectual Property Rights and Challenges before Higher Education Dr. Poornima Ravinathan, Dr. Chandrasekar .K	16
17	Intellectual Property In Higher Education T. NagaPrasada Rao	17
18	Mobile Addiction in Adolescents K. Anthony Raju, Rai Prakash, A. Srinivasa Rao	18

19	Phishing Web Sites Features Classification Based on Machine Learning M.Raj Kumar (DMC-48), D.Mohith (DMC-43)	19
20	Rays of Intellectual Property Rights in India and Its Progress Dr. Baby Rani Bommadevara	20
21	Risk Prediction in Deep Learning K.Aparnaa, J.Satyanarayana	21
22	Sentiment Analysis using Deep Learning Mr. S.A.B. Nehru, Mr. K Anil	22
23	Study on Computer Ethics G.Bhavana, Y.Jessy Veena , B.Deepika	23
24	Study on Deep Learning G. Pradeep kumar, G. Prasanna kumar, A. Vazra Dany	24
25	HYBRID NUMERICAL-ANALYTICAL APPROACHES FOR SOLVING NON-LINEAR AND TIME-DELAY DIFFERENTIAL EQUATION SYSTEMS: A STUDY ON RELIABILITY AND COMPUTATIONAL OPTIMIZATION D Narsimha Reddy, Dr.Syed Shahnawaz Ali, Dr. Kunderu Lakshmi Narayan	25
26	SECURITY CONCERNS WITH BODY SENSOR NETWORKS AND THEIR USE IN HEALTHCARE P. Madhuri Paul, Dr Prasadu Peddi	26-32
27	AN INTERNET OF THINGS (IOT) SECURITY STUDY INFORMED SUGGESTED MODEL OF IOT SECURITY MANAGEMENT SYSTEM Pushpa Latha Thumma, Dr Prasadu Peddi	33 - 37
28	Disrupting the Gender Binary: Transgender Representation and Resistance in "Seatbelt Crew" Jithin J, Dr. R. Ponmani Subha Chellam	38-56

THE POTENTIAL OF AI IN MEDICINE

Chilukoti Divya Chandrika (DAI-12)

Department of CS, Andhra Loyola College, Andhra Pradesh, India.

chilukotidc30@gmail.com

Abstract

Artificial intelligence (AI) is a rapidly developing field of computer science concerned with creating intelligent machines capable of performing tasks, to do things like analyze data, make predictions that require human intelligence. Now it's presented in medicine. Before the advent of AI, the medical field was also characterized by manual processes & paperwork. Doctors had to go through a laborious process of collecting & analyzing patient data. This was time-consuming and prone to errors, leads to inefficient care. Diagnoses were conducted by doctors & nurses, relying on their knowledge and experience to provide best possible care. And processes such as billing and scheduling were done by hand. With AI, the medical field has been revolutionized. AI-driven algorithms can quickly analyze data, identify patterns and detect potential disease markers. This is a tool that it can help doctors make more accurate diagnoses, medical imaging & make better decisions about treatments and preventive measures to give effective treatment for a particular patient. It can also automate processes of billing & scheduling, freeing up the time to focus on patient care. When COVID-19 pandemic disrupted the world, AI was used as a tool to develop predictive models that can help minimize the spread and used ML to make discoveries & create better vaccines. AI is finding its place in healthcare robotics by providing unique assistance in surgeries. It is used to operate in small spaces that might otherwise require open surgery. Robots can be more precise around sensitive organs & tissues, reduce blood loss, risk of infection and post-surgery pain. Robotic surgery patients reports less scarring & shorter recovery time.

The advantages of AI that AI allows healthcare professionals to better understand patterns & patient needs through in-depth data analysis. As technology continues to develop in medical applications, doctors will be able to provide better guidance. And there also be some disadvantages. Some are, AI algorithms can be trained on biased data, which can lead to inaccurate diagnoses and treatment. It can also be expensive to implement & maintain and require a lot of computing power and data. And wrong Diagnosis, threat of data loss & losing personal approach. The future of AI is Bright. In future, AI will be used to detect diseases, diagnose diseases, provide treatment, surgical procedures, predict outcomes, and even provide personalized treatments. And its use in the medical field is likely to continue to grow in future. However, it is important to ensure that AI is used responsibly and ethically in order to ensure the best outcomes for patients.

AI IN SPORTS

DAI 10 - P. RAJESWARI

DAI 34 - B. SAI PRIYANKA SINGH

DEPT. OF COMPUTER SCIENCE, ANDHRA LOYOLA COLLEGE, VIJAYAWADA

Abstract:

As a confined subject mainly based on computer science, information technology and machine learning, AI is about the simulation, extension and expansion of human intelligence. Meanwhile, the enforced AI application research is helpful to improve the human brain functions, further unleash human intelligence, and give a great boost to the overall technological and reform innovations. The application of AI in sports can both avoid sports disputes, record memorable moments of sports events, and provide directions and guidance for sports scientific research. First, it makes sports competitions more professional. In sports events, the scientific application of AI technology makes it possible to accurately observe athletes physical conditions before, during and after the game, and provide strong support when coaches make real-time adjustments to technical tactics. It also helps to develop personalized training models and promote more scientific and effective competition strategies, thus increasing the competitiveness of athletes. In this way, big data is able to provide a strong support in China's pursuit of a strong sports power. In addition, with the strong support of intelligent technology, competitive sports can also have a more ideal and efficient development prospect. Second, it further strengthens the transformation and upgrading of the sports industry. The sports sector is a sunrise industry with favourable economic and ecological returns. With the support of AI technologies, the industry will see better utilization of capitals, helping build a more scientific and innovative business model and enhance customer service experiences. This will lay a solid foundation for the high-quality development of the sports industry, helping the traditional sports industry see an intelligent upgrading and enhancing the international competitiveness of China's sports industry. Third, the introduction of AI will promote personalized physical education. Through the support of AI, big data and other information technologies, schools can establish a novel and scientific physical education ecosystem, organize students to carry out personalized sports learning and training activities, and help teachers to provide students with more scientific teaching guidance. Big data greatly facilitates the harmonious communication between schools, society and the family.

AN ADVANCED CKD DETECTION USING DEEP LEARNING

Mr Venkata Siva Narasimha G¹, Dr KBS Sastry², PVS Sairam³

¹Assistant Professor, Department of Computer Science,
Andhra Loyola College, Vijayawada.
gvsnarasimha@gmail.com

²Associate Professor, Department of Computer Science,
Andhra Loyola College, Vijayawada.
sastrykbs@gmail.com

³Associate Professor, Department of Physics,
Andhra Loyola College, Vijayawada.
alcsairam@gmail.com

Abstract: Deep learning models are based on artificial neural networks, which are designed to mimic the structure and function of the human brain. These models can learn complex patterns and relationships in large datasets, allowing them to make accurate predictions or classifications. For CKD detection, deep learning models can be trained on large datasets of clinical and laboratory data to identify patterns and risk factors associated with the disease. One approach to using deep learning for CKD detection is to develop a predictive model that can classify patients as having or not having CKD based on their clinical and laboratory data. This can be done using supervised learning, where the model is trained on a labeled dataset of patients with and without CKD. The model can then be used to predict CKD status in new patients based on their data. Various deep learning architectures, such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs), can be used for this task. Another approach is to use deep learning for image analysis of renal histology. Renal biopsy is often used to diagnose and stage CKD, and deep learning models can be trained to analyze renal tissue images and identify features associated with the disease. This approach has the potential to improve the accuracy and speed of CKD diagnosis.

Keywords: convolutional neural networks (CNNs), recurrent neural networks (RNNs), Chronic Kidney Disease (CKD).

AI FOR DISABLED

¹K. PRAGATHI (DAI 18)

²S. VYSHNAVI BHAVANA (DAI 42)

^{1,2} Dept. of Computer Science, Andhra Loyola College(Autonomous), Vijayawada-8.

Gmail: pragathikukkala@gmail.com , vyshnavibhavana21@gmail.com

Abstract

Artificial intelligence (AI) is the study of providing the ability for a computer or a robot controlled by a computer to think and do tasks which require human intelligence. Some of the AI applications are natural language processing, speech recognition, automation and machine vision. People with various impairments find it difficult to access a device and that device may go unusable for them making their daily activities even more hard. Accessibility tools and techniques is a limitation for which most of the disabled people cannot use technology without help. AI came up, finding ways to access technology for people with various disabilities, whether related to vision, hearing, mental health, learning, cognition, or mobility, can be permanent, temporary, or even situational. Necessity is the mother of Invention, disabilities designing new products with different levels of abilities in mind. Through inclusive design AI has ensuring that technology works out for everyone.

Artificial intelligence plays an important role in communication and interaction, it increases the accessibility and usability of technology to people with disabilities. Like giving voice commands to devices like Alexa, Google voice assistant, Siri etc through this disabled people can access devices like computers, mobiles comfortably and even control the whole environment just by sitting and giving voice commands. AI-based self-driving cars promise incredible freedom of mobility for house-bound individuals with disabilities and for people with motor impairments, autonomous vehicles developed by Google's Waymo, Uber, Lyft, Drive AI, and others could eliminate physical isolation and promote a more social lifestyle. Using robotic cars enables disabled people to leave the house without depending on others. Once driverless vehicles are fully integrated into society, motor impaired could ease independent mobility.

AI based solutions stand to make a real difference in the lives of people with disabilities, by providing them usability, accessibility and support in terms of using technology as well as in daily life activities. AI technology helps disabled people to gain new opportunities through accessibility, inclusion in society, and independent living which would be difficult or impossible to achieve without AI. As AI tends to grow further, it could unlock more advanced and innovative solutions for addressing the most complex challenges faced by disabled people and enabling more inclusion for them.

BRAIN TUMOR DETECTION USING DEEP LEARNING

A.Radhika¹, A.Lakshmi Prasanna²

¹Assistant Professor, Department of Computer Science
Andhra Loyola College, Vijayawada
aradhikaalavala@gmail.com

²Assistant Professor, Department of Computer Science
Andhra Loyola College, Vijayawada
info.rafasoft@gmail.com

Abstract: Brain tumor detection is an important task in medical diagnosis, and using deep learning algorithms, particularly ensemble deep learning algorithms, can be an effective approach to achieve high accuracy in brain tumor detection. Ensemble deep learning algorithms involve combining multiple models to make more accurate predictions. The two most common types of ensemble methods are bagging and boosting. Bagging involves training multiple models on different subsets of the data, and then aggregating their predictions to make a final prediction. Boosting involves training multiple models sequentially, with each model focusing on the data that was misclassified by the previous model. To use ensemble deep learning for brain tumor detection, the first step is to gather a large dataset of brain images. This dataset should include a mix of images that contain tumors and images that do not contain tumors. The images should be pre-processed and normalized to ensure consistency across the dataset. Once the dataset is prepared, the next step is to train the ensemble deep learning model. This involves selecting the appropriate architecture for the neural network, such as convolutional neural networks (CNNs), and tuning hyperparameters such as learning rate, batch size, and number of epochs. After the model is trained, it is evaluated using a separate test dataset to determine its accuracy in detecting brain tumors. The performance of the model can be further improved by fine-tuning hyperparameters or by using data augmentation techniques to increase the diversity of the dataset.

Keywords: neural network, convolutional neural networks (CNNs), Bagging, Boosting.

FACE MASK PREDICTION USING DEEP LEARNING TECHNIQUES

¹Manubolu Greeshma Priya (DPM-51)

²Kopanathi .Lavanya(DPM-53)

^{1,2}Dept of Computer Science, Andhra Loyola College (Autonomous), Vijayawada-8

Abstract

Medical researchers around the globe provide evidence that COVID19 pandemic diseases transmitted through droplets and respirators of respiratory aerosols and wearing a face mask is an efficient infection control recommendation process. In addition, many public and private service providers demand that consumers use the service only if they wear masks properly. However, a few research studies have been found on face mask detection based on the technology of Artificial Intelligence (AI) and Image Processing. In this project , we propose, Prediction of Mask, which is a deep learning-based multi-phase face mask detection model for preventing human transmission of Two different face mask datasets along with more than 5,200 images have been utilized to train and test the model for detecting with and without a face mask from the images and video stream. Experiment results show that with 770 validation samples Face Mask achieves an accuracy of ~ 93% whereas with 276 validation samples it attains an accuracy using classification techniques many public and private service providers demand that consumers use the service only if they wear masks properly. However, a few research studies have been found on face mask detection based on the technology of Artificial Intelligence (AI) and Image Processing.

LIVER DISEASE PREDICTION USING MACHINE LEARNING

¹P Dhana Lakshmi(DCM-39), ²Macharla Pallavi(DPM-61)

^{1,2}Dept of Computer Science, Andhra Loyola College (Autonomous), Vijayawada-8

Abstract:

Machine learning is a part of man-made consciousness that utilizes an assortment of measurable, probabilistic and enhancement methods that enables PCs to "learn" from past precedents and to identify hard-to-recognize designs from huge, boisterous or complex informational indexes. This capacity is especially appropriate to restorative applications, particularly those that rely upon complex proteomic and genomic estimations. Therefore, machine learning is every now and again utilized in disease conclusion and discovery. All the more as of late machine learning has been connected to disease guess and forecast. This last mentioned approach is especially intriguing as it is a piece of a developing pattern towards customized, prescient drug. Diagnosis of liver disease at a preliminary stage is important for better treatment. It is a very challenging task for medical researchers to predict the disease in the early stages owing to subtle symptoms. Often the symptoms become apparent when it is too late. To overcome this issue, this project aims to improve liver disease diagnosis using machine learning approaches. The main objective of this research is to use classification algorithms to identify the liver patients from healthy individuals. This project also aims to compare the classification algorithms based on their performance factors

DEEP LEARNING FOR COMPUTER VISION

Sk. Firoz (DCM03) , N. Dange Naveen (DCM36), N. Naga Pavan (DCM05)
Dept. of Computer Science, Andhra Loyola College, Vijayawada, 520008

Abstract:

Computer vision is a field of artificial intelligence (AI) that enables computers and systems to derive meaningful information from digital images, videos and other visual inputs — and take actions or make recommendations based on that information. If AI enables computers to think, computer vision enables them to see, observe and understand. Computer vision works much the same as human vision, except humans have a head start. Computer vision trains machines to perform these functions so that it can quickly surpass human capabilities.

Computer vision needs lots of data. It runs analyses of data over and over until it discerns distinctions and ultimately recognize images. For example, to train a computer to recognize automobile tires, it needs to be fed vast quantities of tire images and tire-related items to learn the differences and recognize a tire, especially one with no defects.

Two essential technologies are used to accomplish this: a type of machine learning called [deep learning](#) and a convolutional neural network (CNN). Machine learning uses algorithmic models that enable a computer to teach itself about the context of visual data. If enough data is fed through the model, the computer will “look” at the data and teach itself to tell one image from another. Algorithms enable the machine to learn by itself, rather than someone programming it to recognize an image.

A CNN helps a machine learning or deep learning model “look” by breaking images down into pixels that are given tags or labels. It uses the labels to perform convolutions and makes predictions about what it is “seeing.” The neural network runs convolutions and checks the accuracy of its predictions in a series of iterations until the predictions start to come true. It is then recognizing or seeing images in a way similar to humans.

The development of self-driving vehicles relies on computer vision to make sense of the visual input from a car’s cameras and other sensors. It’s essential to identify other cars, traffic signs, lane markers, pedestrians, bicycles and all of the other visual information encountered on the road.

Keywords: Computer Vision, Artificial Intelligence, Convolutional Neural Network (CNN), Deep Learning, automation

CREDIT CARD FRAUD DETECTION USING ADABOOST AND MAJORITY VOTING

¹G.Chandan Sai(DMC 47), ²T.Mohan Teja (DMC 45)

^{1,2}Dept of Computer Science, Andhra Loyola College(Autonomous),Vijayawada-8

Abstract

Credit card fraud is a serious problem in financial services. Billions of dollars are lost due to credit card fraud every year. There is a lack of research studies on analyzing real-world credit card data owing to confidentiality issues. In this paper, machine learning algorithms are used to detect credit card fraud. Standard models are firstly used. Then, hybrid methods which use AdaBoost and majority voting methods are applied. To evaluate the model efficacy, a publicly available credit card data set is used. Then, a real-world credit card data set from a financial institution is analyzed. In addition, noise is added to the data samples to further assess the robustness of the algorithms. The experimental results positively indicate that the majority voting method achieves good accuracy rates in detecting fraud cases in credit cards.

DRIVER DROWSINESS DETECTION

¹G.Sravani(DMC 39), ²K.Raja Rajeswari(DMC 40)

^{1,2}Dept. of Computer Science, Andhra Loyola College(Autonomous),Vijayawada-8

Abstract

The main idea behind this project is to develop a nonintrusive system which can detect fatigue of any human and can issue a timely warning. Drivers who do not take regular breaks when driving long distances run a high risk of becoming drowsy a state which they often fail to recognize early enough. According to the expert's studies show that around one quarter of all serious motorway accidents are attributable to sleepy drivers in need of a rest, meaning that drowsiness causes more road accidents than drink-driving. This system will monitor the driver eyes using a camera and by developing an algorithm we can detect symptoms of driver fatigue early enough to avoid the person from sleeping. So, this project will be helpful in detecting driver fatigue in advance and will give warning output in form of alarm and pop-ups. Moreover, the warning will be deactivated manually rather than automatically. For this purpose, a de-activation dialog will be generated which will contain some simple mathematical operation which when answered correctly will dismiss the warning. Moreover, if driver feels drowsy there is possibility of incorrect response to the dialog. We can judge this by plotting a graph in time domain. If all the three input variables show a possibility of fatigue at one moment, then a Warning signal is given in form of text and sound. This will directly give an indication of drowsiness/fatigue which can be further used as record of driver performance.

ENHANCING CLOUD SECURITY USING ORDER PRESERVING ENCRYPTION AND AUDIT SERVER BASED VERIFICATION

¹Ramanjaiah Ganji, ²Dr.Suresh Babu Yalavarthi

¹Department of Computer Science and Engineering, Research Scholar, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India.

²Professor, Department of Computer Science, J.K.C College, Guntur, Andhra Pradesh, India.

E.Mail:¹ramanjaiah@gmail.com,²yalavarthi_s@yahoo.com

Abstract:

By the use of the internet and cloud computing, customers may keep their data on the cloud and access it at any time. There is a tremendous amount of data on the computers that cloud storage services employ. To see all the data under the current system, the data owner must upload the files to a cloud server. If a data owner has the ability to edit any data, Third Party Arbitrary (TPAR) will be able to detect any altered or absent data. If the cloud-stored data remains unchanged, TPA will generate the verification report and provide it to the data owner. The management of the information and the administrations on the cloud aren't entirely moral, nevertheless. Guaranteeing the information uprightness is a requesting errand. Numerous plans like "Proofs of Retrievability" and "Provable Data Possession" have been created yet they can't bolster dynamic information i.e. they are produced to dissect static archive data. By and large a significant number of the peril models accept that having a fair data owner and they are concentrating on the exploitative cloud authority organization. In any case, there are a few shots that the customer might be untrustworthy for the getting the advantages by means of pay from the supplier. The open inspecting plan that provides information assistance and acceptable discretion in data safety matters is the main emphasis of this study. It takes into account the fact that data owners cannot view all of the uploaded files immediately. Only the data owner is able to examine files associated with a term by using keywords. Hence, when someone logs into the account of the data owner, they cannot view the file. Only after conducting a keyword search may files be accessed. The owner's data is kept secure by this suggested system.

Keywords: Cloud Computing, Data Owner, TPA, Third Party Arbitrator, OPE, Data verification, Dispute Arbitration.

ENHANCING FASTAG WITH SOFTWARE

Jalaluddin Pathan

UG student, department of CS, Andhra Loyola College, Andhra Pradesh, India.

jalaluddinpathan@yahoo.com

Abstract

Fastag was founded on 4 November, 2014 by Ministry of Road Transport and Highways. Fastag came into its complete existence by the maintenance of National Highways authority of India as of September 2019[1]. Fastag is being used as an electronic toll collection in India, since its existence. The main reason behind the introduction of fastag was to eliminate the cash payments, avoid the traffic jams at the toll gates across India, to save time from the manual process of tax collection, and to save the environment by reducing the usage of paper.

Fastag also allows users to maintain the records of toll expenses. Fastag comprises the usage of RFID (Radio Frequency Identification Device) at the toll lanes of the toll gates across India. RFID system consists of radio transponder, a transmitter, and a radio receiver. RFID system has two main devices, a tag, and a reader [2]. Tag contains a RFID transmitter, which is stucked on to the mirror of the vehicle, and the reader is placed in the toll line. Reader provides radio waves as energy to the passive tag and receives the digital data through the receiver. This has made a revolutionary change in the progress of National Highway Authority of India. Unfortunately, this system of Fastag contains some flaws which give discomfort to the vehicle owners and also makes a long-term financial effect on National Highway Authority of India. Fastag is comprised with maximum usage of hardware components. After long usage, hardware components like receivers and radio transponder wear out due to many reasons. This is an expected problem and a problem being faced now. Fastag receivers and transponders are wearing out due to some conditions. Considering the failure rate of RFID, National Highway Authority of India, has introduced portable RFID receivers, and if the portable devices wear out, entry into particular line needs to be prohibited and the vehicles need to be sent into the line using the manual process. The NHAI technical staff has to collect the toll tax manually by feeding the vehicle registered number in the system which is the old practice. This creates trouble to both the vehicle owners and also to the NHAI staff. This problem can be fixed by appending a software solution to the present hardware system. Since software does not wear out [3], relying on software is wiser than relying on hardware. The usage of QR system can completely end the above problems and enhance the Fastag system in a productive and easy way, by considering all the problem facers in present fastag system. This research paper consists of deep report of present Fastag architecture, problem faced by people using fastag, and the solution to the problems, and its advantages.

ETHICS OF COMPUTER SCIENCE IN MODERN ERA

Polimetla vinay ,Student
Andhra Loyola College ,Vijayawada
Mail id -vinaypolimetla7286@gmail.com
Mob:-9966416421

Abstract

Advancement of computer technology has proved as double edged knife, simultaneously it helps in the development and became curse in our lives in the name of betterment. Improvement in computer science and technology since twenty years and created ethical dilemmas, some similar to many other professionals and some unique to the computer field

In past years alone society experienced computer virus, interruption of power, and invasions of privacy, cyber- pornography, phishing, and many thefts. This paper brings out the basic instructional issues and provides primary ways to professionals who demand both technical knowledge and the ability of understanding of ethical principles and skills.

Finally, this paper comes out with a valuable framework for the study of ethics and social principles and skills in summarized form.

Keywords: Computing Ethics, Computer abuse, Ethical principles and skills, Cyber laws

EXPRESSION DETECTION USING ENSEMBLE MODELS

LNageswari Devi¹, A.Sandhya Rani²

¹Assistant Professor, Department of Computer Science

Andhra Loyola College, Vijayawada

lankenageswari@gmail.com

²Assistant Professor, Department of Computer Science

Andhra Loyola College, Vijayawada

rani.amarlapudi@gmail.com

Abstract: Expression detection is a common application of machine learning that involves identifying the emotions or sentiments expressed by individuals in images, videos, or text. Ensemble models are a popular approach to improving the performance of expression detection models by combining the predictions of multiple models. Ensemble models work by training multiple models on the same dataset, but with different variations in the model architecture or training process. These models are then combined in a way that maximizes their collective predictive power. In this paper, an ensemble model used the multiple models are trained and their predictions are combined using a meta-model. The meta-model is trained on the outputs of the base models, and the final prediction is made by the meta-model. To use ensemble models for expression detection, a dataset of labeled images or videos can be used to train multiple models using different architectures or training techniques. For example, one model could be trained on raw pixel data, while another could be trained on extracted features. These models can then be combined using one of the ensemble methods described above to improve the accuracy of the overall prediction. Ensemble models have been shown to be effective in improving the accuracy of expression detection models, and are commonly used in industry and research applications. However, it is important to note that ensemble models can be computationally intensive and require careful tuning of hyper-parameters to achieve optimal performance.

Keywords: Expression detection, Ensemble model, Deep Learning.

HOUSING PRICE PREDICTION USING LINEAR REGRESSION

¹S.Yamini Durga (DMC-41)

²M.Niharika (DMC-50)

^{1,2}Dept. of Computer Science, Andhra Loyola College (Autonomous), Vijayawada-8

Abstract:

Investment is a business activity on which most people are interested in this globalization era. There are several objects that are often used for investment, for example, gold, stocks and property. In particular, property investment has increased significantly. Housing price trends are not only the concern of buyers and sellers, but it also indicates the current economic situation. There are many factors which has impact on house prices, such as numbers of bedrooms and bathrooms. Even the nearby location, a location with a great accessibility to highways, expressways, schools, shopping malls and local employment opportunities contributes to the rise in house price. Manual house predication becomes difficult, hence there are many systems developed for house price prediction. We have proposed an advanced house prediction system using linear regression. This system aim is to make a model which can give us a good house pricing prediction based on other variables. We are going to use Linear Regression for this dataset and hence it gives a good accuracy. This house price prediction project has two modules namely, Admin and User. Admin can add location and view the location. Admin has authority to add density on the basis of per unit area. User can view the location and see the predicted housing price for the particular location.

INTELLECTUAL PROPERTY RIGHTS AND CHALLENGES BEFORE HIGHER EDUCATION

Dr. Poornima Ravinathan

Asst. Professor, Department of Political science
Andhra Loyola College, Vijayawada

Dr. Chandrasekar .K

Associate professor,
Department of chemistry,
School of applied sciences and humanities,
Vignan university, Vadlamudi,

Abstract

With the implementation of NEP-2020, the chances of innovation and new technologies keep rising as the policy focuses mainly on research at the early stages of study. This positively will bring in controversies if the work is not registered under intellectual property rights. This gives the research fraternity full control of their respective work and that can bring in lot of new life saving schemes without much issues. This study will focus on the odds that present education policy offer in comparison to the new NEP which is expected to fill in the gap as it progresses in long run with respect to research and IPR. It's not only the scientific community that has to be accounted here, apart from them researchers from other platform like literacy, journalism, social sciences do as well the odds in all these areas and how important it is to have their work documented has to be emphasised.

The fact that IPR for any inventor is the highly coveted asset that can potentially reap a financial pay out to the owner has to be emphasised and inculcated in the young minds at the higher education level where they can choose research as an potential carrier similar to engineering and medicine. IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. This can actually make the research community cherish for their discoveries and flourish with more innovations and technologies.

The contributions from the funding agency to the institution to the licencing authority and to the individual or the original contributor has not to be underestimated when the technology heads towards commercialisation and with increasing contribution challenges and potential conflict of % sharing too increases. This can be sorted out with the advent of IPR which has to been approved by the Indian government. This could be credited to the National IPR Policy approved by the Union Cabinet in May 2016, which was the first ever IPR policy framed by the Government of India.

The main focus of this Policy is towards promoting innovation and creativity, particularly amongst entrepreneurs and in higher education institutions. The Policy brief specifically mentions synergising all forms of IPR, concerned statutes and agencies for tapping the creativity and innovative energies in India with a special emphasis on start-ups and educational institutions.

The main aim of this paper is to highlight the need for the Indian universities and our Research and Development organizations to address, propose and develop policies relating to the IPRs. Secondly, to present some reflections about the need for additional emphasis on university instruction in IP issues and the training of scholars to undertake research in the area. This can end up in new startups which paves way for new national and international ventures to increase the economy.

INTELLECTUAL PROPERTY IN HIGHER EDUCATION

T.NagaPrasada Rao – Head Of The Dept Cs

t.nagaprasadarao@gmail.com - +91 9866803938

AG & SG Siddhartha Degree College of Arts & Science

Vuyyuru Krishna Dist A.P 521165

Abstract:

The importance of intellectual property (IP) in today's world cannot be overstated and, indeed, it is receiving a great deal of attention worldwide. To advance the cause of the rights and wrongs of the laws that promote and protect intellectual property at the national and international levels, education in intellectual property is required and must be advocated. We must make individuals, industries, and governments aware of the concept of intellectual property, and only then can they take positions on the issue in order to effect change. This paper explains the concept of intellectual property rights and provides a detailed overview of the state of IP education worldwide. The discussion divides the globe on the basis of economic distinctions between nations and studies the question in the context of their developmental levels: developed, developing, or underdeveloped.

Intellectual property should be a day-to-day business decision due to its value, but increasingly, a number of institutions are still not aware of the importance. Intellectual Property (IP) and its value are often not adequately appreciated. In the increasingly knowledge-driven economy, IP is a key consideration in day-to-day business decisions because new ideas and products appear almost daily in the market, which results in continuous innovation and research. Therefore, this paper will focus on the importance of IP for universities of technology and also further demonstrates how IP can become an economic tool and the challenges faced by these universities in implementing an IP system.

Keywords—Intellectual property, institutions, challenges, protection, IP Education and Government

MOBILE ADDICTION IN ADOLESCENTS

K. Anthony Raju¹, Rai Prakash², A. Srinivasa Rao³

¹Student, Department of Computer Science
Andhra Loyola College, Vijayawada
tonykondaveetirajusj@gmail.com

²Student, Department of Computer Science
Andhra Loyola College, Vijayawada
prakashrai72718@gmail.com

³Student, Department of Computer Science
Andhra Loyola College, Vijayawada
addakatlasrinivasarao@gmail.com

Abstract: India counts 38% of all networked devices by 2022, compared to 26% in 2017. Statistics acknowledge that adolescents have a high ratio of usage of smart devices. This count increased during the COVID pandemic as most of them ought to attend classes online. At the same time, it has become considerably tricky for parents and guardians to monitor screen time. There were noticeable cases of Smartphone addiction leading to death, yet limited research has been done to address this serious issue. In this context, we began our study with 250 students on addictive usage associated with their academic performance. We found that 75.7% of adolescents buy the maximum number of devices as they deem that it speaks of their economic status in society. 61.6% of them believe smartphones are only their source of entertainment. The saddening conclusion is that most of them are educated about EMR (Electromagnetic Radiation) that their devices release and yet are driven to sleep with their Smartphones. Though the purpose of smart devices is more of academics for most users, most of the time is poured into gaming and other entertainment leaving them with poor academic results and inadequate time to spend on academics. Thus, dependence on Smartphones may be a definite risk factor for poor academic performance. Longitudinal research could be used to confirm our study and supply evidence for directionality.

Keywords: Smartphone addiction, academic performance, adolescents

PHISHING WEB SITES FEATURES CLASSIFICATION BASED ON MACHINE LEARNING

¹M.Raj Kumar (DMC-48), ²D.Mohith (DMC-43)

^{1,2} Dept. of Computer Science, Andhra Loyola College (Autonomous), Vijayawada-8

Abstract:

Phishing is one of the most common and most dangerous attacks among cybercrimes. The main aim of these attacks is to hack the user information by accessing the credentials that is used by individuals and any of the organizations. Phishing web sites contain various hints among their contents and web browser-based information. The victim's confidential data is expected by the phishing sites by deriving them to surf a phishing web sites that resembles to legitimate websites, which is one of the criminal attacks prevailing in the internet. Phishing websites is similar to cyber threat that is targeting to get all the credential-based information accessed from the credit cards and social security numbers. The purpose of this project is to perform Extreme Learning Machine (ELM) based classification. There are different types of features based on web pages. Hence, to prevent phishing attacks we must use a specific web page feature. Here, a model based on Machine Learning techniques like Naïve Bayes is used to detect phishing web pages.

RAYS OF INTELLECTUAL PROPERTY RIGHTS IN INDIA AND ITS PROGRESS

Dr. Baby Rani Bommadevara, HOD, Department of Economics,
Andhra Loyola College, Vijayawada.
b.babyrani@gmail.com
9948102726

Abstract

Intellectual property is defined as property created by the human mind and intellect. Any essential progress of human knowledge, such as artistic, academic, specialized, or logical development, is managed by Intellectual Property (IP). The creator's lawful rights to validate their invention are granted under Intellectual Property Rights (IPR). Intellectual property rights (IPR) are critical to a country's development. This paper looks at Intellectual Property Rights and the relation they have with economic growth. Its aim is to analyze the impact of a strong IP regime on the economic development of a nation. . Today, IP rights are recognized as an important economic mechanism, an 'intellectual currency' of sorts, that encourages research and development (R&D), creation and innovation in several significant ways. So innovation is important for economic growth, but IPR protection is important for innovation, this way IPR protection becomes important for the economic growth too.

Keywords: Intellectual Property Rights, IPR Protection, Economic Growth, Innovation, R&D

RISK PREDICTION IN DEEP LEARNING

K.Aparnaa¹, J.Satyanarayana²

¹Assistant Professor, Department of Computer Science
Andhra Loyola College, Vijayawada
koppolu.aparna@gmail.com

²Assistant Professor, Department of Computer Science
Andhra Loyola College, Vijayawada
js.narayan25@gmail.com

Abstract: Risk prediction is a critical task in many fields, including healthcare, finance, and insurance. Deep learning has shown great promise in accurately predicting risk, but there are many challenges associated with applying deep learning to risk prediction. This paper presents an overview of recent advances in deep learning for risk prediction, including the use of convolutional neural networks, recurrent neural networks, and attention mechanisms. We also discuss important considerations when applying deep learning to risk prediction, such as data quality, feature selection, and interpretability. Finally, we highlight some of the current limitations and future directions for research in this area. Overall, deep learning has the potential to significantly improve risk prediction in many domains, but careful attention must be paid to the specific challenges and considerations associated with each application.

Keywords: Deep Learning, Risk prediction, disease prediction.

SENTIMENT ANALYSIS USING DEEP LEARNING

Mr. S.A.B. Nehru ¹, Mr. K Anil ²

¹Assistant Professor, Department of Computer Science
Andhra Loyola College, Vijayawada
sabnehr@gmail.com

²Assistant Professor, Department of Computer Science
Andhra Loyola College, Vijayawada
anilkasula66@gmail.com

Abstract

Sentiment analysis, also known as opinion mining, is the task of identifying the sentiment or emotion expressed in a given text. It has numerous applications in various fields such as marketing, customer feedback analysis, and political analysis. In this paper, we propose the use of radial basis function networks (RBFNs) for sentiment analysis. RBFNs are a type of artificial neural network that are particularly suited for function approximation and pattern recognition tasks. They consist of an input layer, a hidden layer with radial basis functions as activation functions, and an output layer. The RBFNs are trained using a supervised learning algorithm, such as backpropagation. We evaluate the proposed RBFN-based sentiment analysis method on a standard sentiment analysis dataset and compare it with other popular machine learning methods such as support vector machines (SVMs) and naive Bayes (NB) classifiers. The results show that the RBFN-based method outperforms the other methods in terms of accuracy, precision, and recall. In addition, we investigate the effect of different parameters such as the number of hidden nodes, the width of the radial basis functions, and the regularization parameter on the performance of the RBFN-based method. The experiments show that the performance of the RBFN-based method is sensitive to these parameters and that the optimal values depend on the characteristics of the dataset. Overall, our results demonstrate that RBFNs are a promising approach for sentiment analysis and that they can outperform other popular machine learning methods. Further research is needed to explore the use of RBFNs in other natural language processing tasks and to investigate the interpretability of the learned models.

Keywords: support vector machines (SVMs) and naive Bayes (NB), radial basis function networks (RBFNs).

STUDY ON COMPUTER ETHICS

G.Bhavana ¹, Y.Jessy Veena ², B.Deepika³

Students, Department of Computer Science

Andhra Loyola College, Vijayawada

¹gulipallibhavana@gmail.com, ²yadalajessyveena@gmail.com,

³deepikaswameru@gmail.com

Abstract: Computer ethics is a branch of applied ethics that deals with the ethical issues that arise from the use of computer and technology. It involves the study of moral, social and legal issues related to the use of computers and technologies. The field of computer ethics has become more integrated into our daily life.

In 1950, MIT professor Norbert Wiener published "The human use of human beings", which considered for the first time a series of ethical issues, questions and topics within Computer Science. Some of the key issues in Computer ethics include privacy, security, intellectual property and access to information. Privacy concerns arise from the collection and use of personal data by companies and governments. Security issues arise from cyber-attack and the need to protect information. Theft are the unauthorised distribution of digital content, copyrighted content and intellectual property is an on-going issue online, with everything from art and entertainment media to software and innovative products shared illegally online. Access to information issues arise from digital divide and the need to ensure that everyone has equal access to information.

STUDY ON DEEP LEARNING

G. Pradeep kumar ¹, G. Prasanna kumar ², A. Vazra dany³

Students, Department of Computer Science

Andhra Loyola College, Vijayawada

¹pradeepkumaraj04 @gmail.com, ²prasannakumar@gmail.com , ³loyoliteapc19@gmail.com

Abstract:

Deep learning is a sub set of the Machine learning which is essentially a neural network with three or more layers Deep learning is an emerging area of machine learning (ML) research. It comprises multiple hidden layers of artificial neural networks. The deep learning methodology applies nonlinear transformations and model abstractions of high level in in large databases. The recent advancements in deep learning architectures within numerous fields have already provided significant contributions in artificial intelligence. This article presents a state of art survey on the contributions and the novel applications of the deep learning. The following review chronologically presents how and in what major applications deep learning algorithms have been utilized. Furthermore, the superior and beneficial of the deep learning methodology and its hierarchy in layers and nonlinear operations presented and compared with the more conventional algorithms in the common applications. The state of the art survey further provides a general overview on the novel concept and the ever increasing advantages and popularity of deep learning.

Keywords: Deep learning, Machine Learning, Applied Deep Learning

HYBRID NUMERICAL-ANALYTICAL APPROACHES FOR SOLVING NON-LINEAR AND TIME-DELAY DIFFERENTIAL EQUATION SYSTEMS: A STUDY ON RELIABILITY AND COMPUTATIONAL OPTIMIZATION

¹D Narsimha Reddy , ²Dr.Syed Shahnawaz Ali, ³Dr. Kunderu Lakshmi Narayan

¹Research Scholar, Sri Satya Sai University, Sehore M.P. (India)

²Research Guide, Sri Satya Sai University, Sehore M.P. (India)

³Professor of Mathematics VJIT, Hyderabad

Abstract

Non-linear and time-delay systems of differential equations frequently arise in modeling complex phenomena across disciplines such as physics, engineering, and biological sciences. These systems present significant challenges due to their intricate dynamics, lack of closed-form solutions, and sensitivity to initial conditions. This study explores innovative hybrid numerical-analytical methodologies to address these challenges. The proposed approaches combine numerical techniques, such as reduction to first-order systems and block schemes, with analytical insights to improve the stability, accuracy, and computational efficiency of solutions.

Special emphasis is placed on time-delay systems and non-linear dynamics, with applications in domains such as predator-prey models, mechanical oscillators, and coupled reaction-diffusion systems. The hybrid framework is validated through comprehensive benchmarks, demonstrating its ability to handle complex systems with superior convergence and reduced computational overhead. By bridging numerical precision and analytical rigor, this research provides a robust and scalable solution framework for tackling non-linear and time-delay differential equation systems, advancing the state of computational mathematics.

Key Words: Hybrid numerical-analytical methods, On-linear differential equations, Time-delay systems, Computational optimization

SECURITY CONCERNS WITH BODY SENSOR NETWORKS AND THEIR USE IN HEALTHCARE

P. Madhuri Paul¹, Dr Prasadu Peddi²

¹Research Scholar, Dept of computer science, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan.

²Assistant Professor, Dept of computer science and Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University

madhuripaul.2020@gmail.com

ABSTRACT

The concept of Body Sensor Systems (BSNs), which may be widely used in healthcare applications across the board, is shown in this study. It looks at systems and related applications for medical problems and discusses crucial difficulties and BSN metrics. With recent advancements in the computer technologies of Wireless Sensor Networks (WSNs) and Embedded Systems, tiny health monitoring devices have shown to be fundamentally realistic. Yet, BSN offers the tools for evaluating low-cost devices that can detect the surrounding environment and have wireless capabilities, making it appropriate to further the issue. Sooner or later, it will be possible to witness the integration of a significant portion of wireless networks with current, particular medical technology and other fields. These sorts of devices often provide correspondence capabilities based on radio frequency. Each sensor in a sensor network is made up of three different types of subsystems: a sensor subsystem that can sense the environment, a second subsystem that aids in applying calculations to the information that has been detected, and a third subsystem that manages message exchange with nearby sensors. Little wireless computers called Wireless Sensor Networks (WSNs) detect, analyse, and transmit environmental stimuli like temperature, among others.

Keywords: BSN, Bio-sensor, Radio Frequency, WSN

1. Introduction

A Wireless Body Sensor Network (WBSN) is a kind of autonomous system designed to track a person's everyday activities. It is made up of intelligent sensor nodes that don't interfere with normal activities and may be used to identify chronic illnesses like diabetes, asthma, and heart attacks and to alert patients in case of an emergency.

These networks provide potential services in a variety of domains, including business, research, industry, and military. The sensor nodes in the WBSN have uses in consumer

electronics, Special Forces (fire fighters, bomb diffusers, military, astronaut monitoring, etc.), entertainment, and sports training. We can use the internet to remotely monitor activities, motions, and crucial human body signs with the use of WBSNs. Hence, it aids in cost savings. The demand for these devices is rising steadily, and various requirements, including security, fault assurance, dependability, and quality of service (QoS), must be met. due to fluctuating bandwidth, varied topologies, and restricted resources like memory and battery power. All of the aforementioned

demands have not been entirely met by WBSNs.

Moreover, WSNs' most reliable aspect, particularly in the healthcare industry, may be expanded. In the next years, smart spaces that are equipped with WSNs will be able to feel the surrounding environment and take various preventative measures depending on the presence of people. As a result, the system may become ubiquitous, where each person will have a module for assessment that can handle the various smart spaces that are accessible in the system and even aid to avoid other health concerns. While it is believed that the programme employed IP as a protocol, connecting the BSN in the hospital setting seems to be difficult [4].

In comparison to the current method, the other integrated IP that is present within smart sensor nodes offers benefits in the context of self-configuration and data gathering. But, it does so at the expense of communication overhead. It also includes the present behaviour that we may anticipate such systems to exhibit. A wireless sensor network is made up of an excessive number of WSN devices that work together to achieve a single goal. The sensors that are integrated into the human body will collect various biological changes with the ultimate purpose of tracking the patient's state of wellness wherever they may be. [5].

2. Literature Survey

From the year 2000, the improvement of medical facilities has led to a five-year rate rise in life expectancy. According to the World Health Organization, the current elderly population will grow by 8.5% by 2050, making about 20% of the global population. This is the major reason why so many nations are prepared to implement

these healthy ageing policies, which will enable senior people to live an active and independent life. With the rapid increase in the older population in the next years, it is now more crucial than ever to make significant efforts to investigate advanced technologies and ideas, such as elderly care in the smart IoT. In order to satisfy the needs of the aged, a broad variety of solutions are provided by offsetting the predicted mitigating and deficient repercussions [15]. Several major, medium, and small initiatives have also been established with the intention of handling the requirements of the aged and setting specific goals. In terms of examining the primary Internet of Things-based services and apps that have previously been released for keeping track of older people's health in distant areas. The need to monitor the elderly is to pay attention to them using various methods, allowing them to benefit and find it easier to go about their daily lives by using applications in various fields, such as social networks, health, nutrition, safety, localization, navigation, cancer detection, glucose level, etc.

A system has been developed that gives an application for remote monitoring and also includes daily, weekly, and monthly reports. This method gives the agent's (third party's) information on the elderly to anybody, including medical professionals, carers, or members of any emergency unit. This system may compile agent feedback in order to provide users with personalised experiences that will enhance their performance. Data integrity, confidentiality, and authenticity are a few additional issues that these systems present [5, 6]. The automated fall detection method has been divided into two groups, namely wearable

devices and ambient device techniques [6]. In this study [7], a method for using floor vibration sensors was suggested. These sensors are able to determine the location of the person by utilising the vibration system. Its processor aids in the analysis of the data location and the fall detection. Walls may have an array of IR sensors installed to assist detect fall activity. While these arrays can recognise a heated moving item, they cannot distinguish a static backdrop [8].

3. System Design & Applications

Wireless communication is a crucial component of node coordination. BSNs struggle to constrict the radius to communicate inside the body's perimeter since they are exclusive in their methods. By restricting the broadcast range, this preserves privacy, lowers node power usage, and lessens interference from nearby BSNs. Radiofrequency (RF) channels are used by WSNs for communication. The wireless BSNs are being tested by the attenuation of emotional by transmitting the signals or signs, whichever is coming from the body, because the shadow of the body has a visible pathway to ingest the RF energy that gets combined with the causes, developments, criticality, and the other factors affecting path loss. The self-organizing capabilities offered by the sensor networks must be maintained by utilitarian efforts [7].

The IPv6-based 6LowPAN technology, which provides wireless low power focused on the IEEE 802.15.4 standard, may be used to construct the wireless system to interact between electronic devices and the IoT smart gateway. In contrast to other current technologies like Bluetooth or Wi-Fi, this technology has been developed to facilitate

the interoperability, compatibility, and connection of heterogeneous WSNs at extremely low cost and minimal need. The current 6LowPAN network, which is in charge of transferring data between the cloud and wearable devices, relies on 6LoBR to offer communication both within and outside of the network as well as routing and forwarding capabilities.

4. WBAN Applications influences on Healthcare:

Actually, WBAN applications cover numerous areas to enhance people's quality of life. They can be classified in a variety of ways, based on their use in medical fields or not. [6] In addition to fitness tracking applications like cognitive and emotional recognition to support driving and social interaction, these non-medical applications include motion gesture identification in interactive games and support for medical emergencies like earthquakes, bushfires, and terrorist attacks. Medical applications are those that are intended for older adults or those with chronic illnesses. Typical examples include biofeedback applications that regulate emotional states, assisted living programs that enhance the quality of life for those with impairments, early disease detection, prevention, monitoring, senior care at home, and rehabilitation following surgery.[7] In general, two types of body sensors are used in health monitoring: (a) physiological sensors, which are used to measure vital signs of the human body either internally or externally, such as blood pressure, body temperature, or electrocardiography (ECG); or (b) biokinetic sensors, which are able to collect signals based on the movement of the human body, such as speed or angular rate of rotation. When paired with body sensors,

ambient sensors can provide further data on environmental pressure, light, humidity, and temperature. Since the sensors are also in charge of keeping an eye on their surroundings, they may be able to supply information for diagnosis and treatment, as is customary in the house[8]. But, when designing WBAN applications needs to consider a number of technical demands, like the movements and temperatures of nodes, location of the nodes and low capabilities of nodes in terms power and processing. Additionally, other constraints closely associated with wireless technology, which is used to facilitate communication between the on-body inside-body nodes, should be considered, like the small distance, data rates the data rate. For instances, apps that utilize implanted sensors must rely on systems that reduce energy consumption so that they can extend the life of batteries while also ensuring maximum performance the shortest delay possible is an essential requirement for those applications which require a high degree of criticality, for example the operation of heart patients who are elderly. These requirements and statements are the reason we study diverse WBAN applications, and also to identify the requirements to meet for an efficient operation. [4] Also, we study the diverse technology used, and attempt to connect WBAN applications.

5. Applications versus Technologies

Wireless technology provides an extremely convenient method of data transmission wireless technology is involved in the communication between sensors and between base stations sensors.

1) Reliability: The data transmitted by WBAN sensors is related to health information, and precision is required.

2) Latency: Some applications for medical use dealing with emergency information cannot handle lengthy response times. Therefore, real-time data transmission that has the ability to guarantee performance is essential.

3) Security: These systems handle sensitive and valuable data. These days, data security and confidentiality are top priorities.

4) Power consumption: Replacement of batteries with WBAN is simple which means there's less emphasis on energy consumption in certain circumstances.

In 2005 [9] analyzed the features that the body's human anatomy can be as a communication medium and the impact it has on wearable devices that operate within or close to the human body. The researchers called it the wireless Personal Area Network (PAN). The name was later changed to PAN was changed to the title Body Area Network (BAN) to incorporate applications and communication that involve devices that wearable (on/around) implanted devices. The form of WSN made up of wearable sensors is referred to by the name of Wireless Body Area Network (WBAN). It consists of wearable devices that are capable of monitoring different bodily parameters of a human body remotely. They are able to be placed over a body's surface or embedded within the body [11].

6. Challenges & Proposed Work

The body sensor network research to date has already focused on healthcare applications, particularly highlighting the drawbacks of conventional techniques to

gather patient data, which provide imprecision owing to necessity and market demand. Yet, body sensor systems can consistently and for a longer period of time collect quantitative data from several types of sensors. Due to its versatility, body sensor networks will be able to allow telehealth applications for medicine outside of hospital walls and will provide highly individualized treatment. BSNs collaborate with the many foundations that might potentially assist with medical services in order to provide individualised care for each person in need. When delaying impermeable uses, such as longitudinal assessment, BSNs that can be bidden during detection and handling may extend and safeguard body functionality [11].

To improve deep brain stimulation, heartbeat, prosthetic actuation, and medicine delivery, body sensor network researchers must continue their efforts. Applications for physiological and bio-kinetic sensing are expanding as athletes and fitness enthusiasts try to improve human performance. The BSNs are well situated to transmit feedback and interactive elements crucial for the fitness applications of the future. BSNs have a large number of sensor nodes, and each one is capable of communicating, sampling, and processing vital signs including blood pressure, heart rate, oxygen saturation, and physical activity, as well as other environmental factors like location, temperature, and humidity. In most cases, these network sensors are placed on the body purposefully as little fixes or hidden in the clothing of users, allowing thorough health checks in their surrounding environment for a long period.

For resource allocation, Quality of Service (QoS), coexistence, and privacy, the

networking of devices in, on, and around the body provides extraordinary challenges. Modest networking methods increase system performance and lessen intrusiveness on the one hand, while compromises in privacy or QoS are unacceptable for delicate or life-critical medical applications. It is unclear if a unified network solution is preferable to application-specific protocols and typologies notwithstanding the wide range of application contexts that BSNs provide. In comparison to WSNs, BSNs are less likely to become redundant [15].

Hence, creating a cooperative and intelligent QoS for the sensor nodes must be the main focus. As a consequence of the in-body implantation approach and the use of on-body sensors, they exhibit considerable variability, which highlights the issue of sensor requirements and placement restrictions. Others ask for several wirelessly networked devices safely connected at different body places, while yet others call for tiny, biocompatible implanted devices with less frequent connection with the outside world. Other designs call for multiple wired networks in a single garment. They continually and naturally collect vast amounts of data, which microprocessors must interpret to derive useful information. To take advantage of the imbalance of resources, maintain system efficiency, and guarantee that data is accessible when required, data processing must be hierarchical [16].

A number of tests have been run utilising various system settings in order to assess the system. After examining the experimental values for various statistical factors like gain, recall, precision, or accuracy, the findings were obtained. The terms false-negative

(FN), false-positive (FP), true positives (TP), and true negatives (TN) are defined by these criteria (TN).

7. CONCLUSION

BSNs are used to link sensors to the human body in order to track and gather physiological data. The fields of health care, social welfare, sports, and entertainment may all make extensive use of this data. The human body is seen as a component of a communication network using the omnipresent network theory. BSN thus offers a wide range of possible applications and market. BSN, WSN, and other wireless approaches can be used without any signal loss and without causing any harm to the human body, which is a difficulty given how the spectrum that may be used for wireless communication might impact people. Robustness, security, and interference-free communication are important considerations when it comes to protocols. Even though extensive study on BSNs has produced several studies, there are still a great deal of unresolved problems. For instance, while constructing sensor nodes, greater consideration should be given to minimising node size and reducing energy usage. Designers may have the option to overlook human tissues that may have been injured as a result of the sensor's heat when it comes into contact with the body by concentrating on a specific area. Briefly stated, BSNs are the fusion of multi-disciplinary fields with the goal of resolving many important problems in a number of these fields, which necessitates further investigation by academics.

8. References

1. Oleiwi, S.S.; Mohammed, G.N.; Albarazanchi, I. Mitigation of packet loss with end-to-end delay in wireless body area network applications. *Int. J. Electr. Comput. Eng.* 2022, 12, 460. [CrossRef]
2. Liu, Q.; Mkongwa, K.G.; Zhang, C. Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. *SN Appl. Sci.* 2021, 3, 1–19. [CrossRef]
3. Karchowdhury, S.; Sen, M. Survey on attacks on wireless body area network. In *International Journal of Computational Intelligence & IoT*, Forthcoming; SSRN: Rochester, NY, USA, 2019.
4. Roy, M.; Chowdhury, C.; Aslam, N. Security and privacy issues in wireless sensor and body area networks. In *Handbook of Computer Networks and Cyber Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 173–200.
5. Asam, M.; Ajaz, A.; Jamal, T.; Adeel, M.; Hassan, A.; Butt, S.A.; Gulzar, M. Challenges in wireless body area network. *Int. J. Adv. Comput. Sci. Appl.* 2019, 10. [CrossRef]
6. Narwal, B.; Mohapatra, A.K. A survey on security and authentication in wireless body area networks. *J. Syst. Archit.* 2021, 113, 101883. [CrossRef]
7. Maheswar, R.; Kanagachidambaresan, G.; Jayaparvathy, R.; Thampi, S.M. *Body Area Network Challenges and Solutions*; Springer: Berlin/Heidelberg, Germany, 2019.
8. Prasadu Peddi (2018), "A STUDY FOR BIG DATA USING DISSEMINATED FUZZY DECISION TREES", ISSN: 2366-1313, Vol 3, issue 2, pp:46-57.
9. Garousi, V.; Rainer, A.; Felderer, M.; Mäntylä, M.V. Introduction to the Special Issue on: Grey Literature and Multivocal

Literature Reviews (MLRs) in Software Engineering. Inf. Softw. Technol. 2022, 141, 106697.

10. Pahuja, R.; Verma, H.; Uddin, M. A wireless sensor network for greenhouse climate control. IEEE Pervasive Comput. 2013, 12, 49–58. [CrossRef]
11. Mansour, A.; Leblond, I. Ecosystem monitoring and port surveillance systems. AIAAS Adv. Appl. Acoust. 2013, 2, 91–111.
12. P. Madhuri Paul, Prasadu Peddi (2021), “Security And Energy In A Wireless Body Area Network: A Protocol Evaluation”, ISSN: 1735-188X, Vol 18, No 6, pp: 7968-7976

AN INTERNET OF THINGS (IOT) SECURITY STUDY INFORMED SUGGESTED MODEL OF IOT SECURITY MANAGEMENT SYSTEM

Pushpa Latha Thumma¹, Dr Prasadu Peddi²

¹Research Scholar, Dept of Computer Science, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan.

²Assistant Professor, dept of computer science and Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University.

pushpareddy28@gmail.com

Abstract— The Internet of Things (IoT) is a modern kind of intelligent communications that has several uses in business, manufacturing, communications, agriculture, and other fields. The development of IoT is the focus of all studies and several businesses in order to provide numerous services and improve our lives. The design, standards, and security of the new technology present several difficulties. We provide a full summary of the IoT's debut in this article, including its history, components, connections, and applications. The architecture of IoT layers has been briefly discussed. In order to address the majority of IoT security issues, establish regulations and terms of service, and meet security standards, we also cover the IoT security and privacy concerns. The first consideration in developing security solutions and IoT network management systems is security needs. Also, in order to identify internal and external assaults and prevent them, this article provides a thorough foundation on the many kinds and targets of attacks. The introduction of several security measures in this research relies on an explanation of the types of attacks and issues in each IoT security layer. The goal of this research is to identify the most practical security measures with minimum power and time requirements. An IoT security management paradigm is presented in this study. The relevant security protocols and methods for IoT security layers are selected using the suggested paradigm. By choosing the best security techniques for IoT layers to reduce power and time consumption, this suggested model helps to improve the performance of the IoT network.

Keywords-- Internet of Things, Cyber-attack, Security threats.

I. INTRODUCTION

The Internet of Things (IoT), which is now the fastest-growing technology and has a significant influence on both social life and commercial contexts, has recently undergone rapid growth. Devices connected to the Internet of Things (IoT) are quickly spreading across society, as are IoT services. Their success has not gone unnoticed, as seen

by the rise in threats and assaults against IoT products and services.

A concept called the Internet of Things (IoT) has the potential to fundamentally change how we interact with technology. A future where every electronic gadget in our environment is a part of a single, linked network was considered the stuff of science fiction. Yet IoT has not only infiltrated the nonfiction genre; it is also sweeping the globe. IoT hardware is no longer a

specialised market. IoT gadgets are starting to enter our (smart) homes from our workplaces, where they are anticipated to have the most influence on our everyday lives. The majority of smart home equipment will be common, safe items like toasters and kettles. Even if these gadgets are breached and exploited, there isn't much a hacker can do to upset you other than spoiling your breakfast. Since that IoT is still in its early stages of growth, the market is now concentrating on these areas. Nevertheless, the Internet of Things (IoT) cannot be seen as a singular object, platform, or even technology. More attention must be given to interfaces, platforms, mobile apps, and common/dominant standards in order to realise the anticipated fast development from IoT potential [1][2].

II. INTERNET OF THINGS (IOT)

The internet of things, or IoT, is a network of connected computers, mechanical and digital machinery, items, animals, or people that may exchange data across a network without needing human-to-human or human-to-computer contact. A person with a heart monitor implant, a farm animal with a biochip transponder, a car with built-in sensors to warn the driver when tyre pressure is low, or any other living thing or artificial construct that can be given an IP address and transfer data over a network can all be considered "things" in the internet of things.[6][7].

IoT standards don't provide enough possibility for things to utilise and access network resources evenly in terms of the standard challenge. Sadly, new smart objects and applications can't be supported by

conventional network protocols. In order to accommodate new objects and applications, the IoT network needs have a defined standard [11]. IoT includes a lot of power-limited sensors, as was already mentioned. Hence, IoT machine to machine communications will not be supported by the use of standard security techniques. To achieve cheap computational power and easy security solutions, IoT requires security procedures. Attackers may employ a variety of strategies at various stages to destroy the IoT network. Data security is becoming the most important factor to take into account when designing an IoT network. From this point on, the IoT system is significantly impacted by the security and privacy issues. The following examples show the security and privacy problems associated with IoT:

1. User confidentiality and data security The Internet of Things (IoT) system is built on numerous smart items sharing information and data through various channels. Personal information about individuals that reveals their personalities and behaviours may be included in the shared data. As was already said, the IoT system offers automated device and user identification. All user data may be gathered from linked items that are kept in the system or shared across other smart objects through various channels [11]. Without any authentication procedures, all user private data is vulnerable to the most hazardous assaults and dangers. Hence, in the Internet of Things network, privacy and data security are crucial.

2. Integration of trust management and policy The administration of IoT trust is very difficult due to the restricted protocols, resources, and capabilities of various smart gadgets. IoT security, information security, services, apps, and user privacy all depend

on trust management. The communication and administration of data between smart objects depend on trust management. Different and heterogeneous devices are present in IoT levels. For instance, every device creates a significant volume of data that is susceptible to various dangers, faults, and assaults. These mistakes and assaults might spread to all IoT levels. Users won't accept it, and as a result, data accuracy and service quality will decline. The following objectives should be met by trust management in IoT. Initially, it has to establish trust connections between IoT items and trust-based agreements for their interaction. In accordance with IoT policy integration, it should also protect user privacy, data transfer, and trust communication. Finally, it should improve system security and robustness as well as IoT service quality. [8]

3. **Complete Security** Each smart thing in the Internet of Things delivers enormous amounts of data to other objects. An authenticated smart object should include security features to protect people, devices, and services. Security measures are also used to guard against threats and attempts to access data or services. This process is known as end-to-end security. IoT devices, IoT gateways, access and network connections, IoT applications, platforms, and users are all included in the End-to-End security domain. Processes for access control, encryption, and authentication are the three core components of End-to-End security. A concise overview of the End-to-End security situation may be given in the following phases. Each smart object that wishes to link to another one must be an authorised object as well. A smart object may transmit and receive data or instructions after it has been authorised. After that, a smart item may connect to the cloud directly. The cloud provider handles authentication

and manages communication between smart items. A smart item connects to the Internet via the gateway once authentication and control procedures have been put in place. Then, communications sent between smart objects are encrypted using the encryption method.

4. **Management of Identity and Authentication** IoT authentication mechanisms may be implemented using a variety of techniques, including public key infrastructure, ID, and passwords (PKI). Nevertheless, due to the diversity and complexity of the items, traditional authentication procedures are not relevant for the Internet of Things [40]. In terms of identity management, it is used to manage smart object identities, services, and functions. It offers services for access control, identification, and authentication. The linkages of smart objects are defined by identity management. The IoT platform's connection, network domains, and applications are all included. Hence, the effectiveness of the authentication procedures determines identity management.

III. SECURITY CHALLENGES FACING IOT

IoT security is the defence against intrusion of Internet of Things devices. Although many company owners are aware that their PCs and phones need to be protected with antivirus software, the security dangers associated with IoT devices are less widely understood, and protection for these devices is far too often disregarded. There are a lot of Internet of Things devices.

Everything all around us are becoming more and more internet-connected, from vehicles and refrigerators to monitoring equipment on production lines. The IoT industry is expanding at an astounding rate; according to Juniper Research, by 2022, there will be more than 50 billion IoT sensors and devices

in use worldwide. Businesses are swiftly embracing IoT devices owing to the great potential for savings, even while consumer IoT devices provide lifestyle advantages.

For instance, Harley-Davidson boosted net margin by 19% and cut expenses by 7% after converting their York, Pennsylvania facility into a "smart factory" that uses IoT devices at every stage of the manufacturing process.

Data Integrity (a)

(a) An ecosystem that is connected with IoT and includes billions of devices is interconnected. The whole data that is sent and transferred back and forth from the sensor to the main server will be manipulated if even one data point is altered. Integrity should be ensured by using digital signatures and a decentralised distributed ledger [14].

(b) Capability for encryption

The process of encrypting and decrypting data is ongoing. The IoT network's sensors are still unable to process data. Firewalls and separating the devices onto different networks may stop brute force attacks.

(c) Privacy Concerns

IoT is primarily focused on the interchange of data across different platforms, gadgets, and users. Smart devices collect data for a variety of purposes, including enhancing productivity and user experience, aiding in

decision-making, delivering better service, etc.; as a result, the final destination of the data must be properly secured and protected.

(d) Common Framework

As there is no unified framework, each manufacturer is forced to handle security and privacy management on their own. Reusability of code may be accomplished after a common, standardised framework has been developed since the individual efforts will then be used together in an expanding way [13].

IV. CONCLUSION

Every layer of the IoT architecture is open to assaults. As a result, there are several security dangers and demands that must be met. The current status of IoT research is mostly focused on access control and authentication protocols, however due to the fast advancement of technology, it is crucial to combine new networking protocols like IPv6 and 5G to accomplish the progressive fusion of IoT topologies. This chapter's primary goal was to highlight important security challenges related to IoT, with a specific focus on security threats and their defences. Many IoT devices become easy targets due to a lack of security mechanisms, and even these are infected without the victim's awareness. These security needs, such as confidentiality, integrity, and authentication, are covered in this chapter. Several IOT applications are addressed in this study. By highlighting the key problems with IoT security and fostering a better knowledge of the risks and their characteristics emanating from different invaders, such as businesses and intelligence

agencies, we believe that this article will be helpful to researchers in the security sector

V REFERENCES

[1] R.Vignesh and 2A.Samydurai ans1 Student, 2Associate Professor Security on Internet of Things (IOT) with Challenges and Countermeasures in 2017 IJEDR | Volume 5, Issue 1 | ISSN: 2321-9939.

[2] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, 203-209, 1987.

[3] J.-Y. Lee, W.-C.Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in *Int'l Symposium on Next-Generation Electronics (ISNE)*, 1-2, 2014.

Y. Xie and D. Wang, "AnItem-Level Access Control Framework for Inter-System Security in the Internet of Things," in *Applied Mechanics and Materials*, 1430-1432, 2014.

[4] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in *Int'l Symposium on Wireless Personal Multimedia Communications (WPMC)*, 604-608, 2012.

[5] M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," *Int'l Journal of Critical Infrastructure Protection*, vol. 5, 86-97, 2012.

[6] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in *Int'l Conference on Wireless and Mobile Computing, Networking and Communications*

(WiMob), 165-172, 2014.

Mirza Abdur Razzaq and Muhammad Ali Qureshi "Security Issues in the Internet of Things (IoT): A Comprehensive Study" by (IJACSA) *International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 6, 2017

[7] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, 2014.

[8] M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS)*, *International Conference on. IEEE*, 2014, pp. 1–8.

[9] Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, pp. 2787-2805, October 2010.

[10] Pushpa Latha Thumma, Prasadu Peddi (2021), "Survey Of Iot Threats And Countermeasures: Identifying Solutions And Addressing Future Challenges", ISSN: 1735-188X, Volume18, issue 6, pp: 7977- 7982

[11] Fahandezh, M., "A Framework for IPSec Functional Architecture," *MASc Thesis, ECE, Faculty of Grad. Studies and Research, U. Windsor*, 2005.

Prasadu Peddi (2018), "A STUDY FOR BIG DATA USING DISSEMINATED FUZZY DECISION TREES", ISSN: 2366- 1313, Vol 3, issue 2, pp:46-57.