Emerging Technologies and Cyber Ethics: Exploring Future Challenges and Opportunities

Dr. C.K. Gomathy, Dr.V.Geetha-Assistant Professor, Department of CSE, SCSVMV, India
Ms. Perumalla L Sai Purna Srinidhi, Mr. Rajasrivatsan Srinivasan CSE, SCSVMV, India.

ABSTRACT

In an era marked by the rapid evolution of technology, the fusion of state-of-the-art innovations with cybersecurity has become both a beacon of promise and a source of profound ethical contemplation. This article embarks on a comprehensive exploration of the intricate relationship between emerging technologies and the ethical considerations they evoke, delineating a roadmap for navigating the future challenges and opportunities they present.

From the realm of artificial intelligence, where machine learning algorithms hold the promise of revolutionizing cybersecurity defense mechanisms, to the frontier of quantum computing, with its potential to render current encryption standards obsolete, each advancement brings forth a multitude of ethical quandaries. Similarly, blockchain technology, hailed for its potential to enhance data integrity and transparency, also raises concerns regarding privacy and decentralization. The convergence of biotechnology and cybersecurity introduces unprecedented possibilities for biometric authentication and medical data security, yet it also invites scrutiny regarding the ethical use of personal biological data and the potential for biometric surveillance. Moreover, as autonomous systems become increasingly prevalent in cybersecurity operations, questions regarding accountability, transparency, and the potential for autonomous decision-making to align with ethical principles come to the fore.Within this complex landscape, issues such as data privacy, algorithmic biases, digital rights, and the ethical implications of technological proliferation require careful examination. By delving into these ethical dimensions, this article aims to equip stakeholders with the knowledge and insights necessary to navigate the evolving intersection of technology and morality.

Ultimately, this exploration serves not only to illuminate the ethical challenges inherent in emerging technologies but also to catalyze a collective effort towards developing ethically conscious approaches to cybersecurity. By fostering a deeper understanding of the ethical implications of technological advancements, we can strive towards a future where innovation and morality coexist harmoniously in the digital age.

Keywords: Cybersecurity, Artificial Intelligence, Machine Learning, Quantum Computing, blockchain technology, Biometric authentication

1. INTRODUCTION

In today's interconnected world, the ease with which we can send and receive various forms of data, whether it's an email, an audio file, or a video, with just a click of a button is truly remarkable. However, amidst this convenience, it's crucial to ponder over the security of our data during transmission. This is where the realm of cybersecurity comes into play. The internet, now an indispensable part of everyday life, is expanding at an unprecedented rate. Alongside this expansion, numerous cutting-edge technologies are reshaping the landscape of

human society. Yet, paradoxically, these very advancements often leave our private information vulnerable, leading to a surge in cybercrimes.

Today, more than 60 percent of all commercial transactions occur online, underscoring the urgent need for robust cybersecurity measures to ensure secure and transparent transactions. Cybersecurity is not merely confined to the IT industry; it extends its reach into various other domains, including cyberspace. Even modern technologies like cloud computing, mobile computing, e-commerce, and online banking demand heightened levels of security, as they store sensitive personal information. The significance of enhancing cybersecurity and safeguarding critical information infrastructures cannot be overstated. It is crucial not only for the security of nations but also for their economic prosperity. Safeguarding the internet and its users has become integral to the development of new services and governmental policies alike. Combatting cybercrime requires a multifaceted approach. While technical measures play a vital role, they alone are insufficient. Effective investigation and prosecution by law enforcement agencies are equally indispensable. Many nations and governments are thus enacting stringent laws to bolster cybersecurity and prevent the loss of critical information.

Furthermore, individual awareness and education on cybersecurity are paramount. Every person must be equipped with the knowledge and skills to protect themselves from the growing threat of cybercrimes. By collectively addressing cybersecurity challenges, we can create a safer digital environment for all.

2. CYBER CRIME

Cybercrime refers to criminal activities conducted through digital channels, leveraging technology and the internet to perpetrate illicit acts. It encompasses a wide range of offenses, from financial fraud and data theft to harassment, espionage, and sabotage. The evolution of technology has expanded the scope and sophistication of cybercrimes, posing significant challenges to individuals, organizations, and governments worldwide.

One hallmark of cybercrime is its borderless nature, allowing perpetrators to operate across jurisdictions with relative anonymity. This global reach amplifies the impact of cybercrimes, enabling criminals to target victims indiscriminately, regardless of geographical location. Moreover, the interconnected nature of the digital landscape means that cybercrimes can have far-reaching consequences, affecting not only direct victims but also interconnected networks and systems. Cybercriminals employ various tactics and techniques to exploit vulnerabilities in computer systems, networks, and online platforms. These may include phishing attacks, malware infections, ransomware schemes, social engineering, and identity theft, among others. The motivations behind cybercrimes are diverse, ranging from financial gain and espionage to activism, revenge, and disruption.

The proliferation of cybercrime poses significant economic, social, and security threats on a global scale. Financial losses resulting from cybercrimes amount to billions of dollars annually, impacting businesses, governments, and individuals alike. Moreover, cybercrimes can undermine trust in digital technologies, erode privacy rights, and compromise national security by targeting critical infrastructure and sensitive information. Addressing the challenges posed by cybercrime requires a multi-faceted approach, encompassing technological solutions, legal frameworks, international cooperation, and public awareness. Effective cybersecurity measures, including robust encryption, intrusion detection systems, and security protocols, are essential for thwarting cyber threats. Additionally, legislative initiatives and law enforcement efforts play a crucial role in deterring cybercriminals and holding them accountable for their actions

2.1 TYPES OF CYBER CRIME

- **Phishing:** Phishing involves fraudulent attempts to obtain sensitive information, such as usernames, passwords, and financial details, by masquerading as a trustworthy entity in electronic communication. Phishing attacks often occur via email, social media, or text messages, with the goal of deceiving recipients into disclosing confidential information. Common phishing tactics include spoofed websites, fake login prompts, and urgent requests for personal information.

- **Ransomware:** Ransomware is a form of malware that encrypts a victim's files or locks them out of their system, demanding payment (usually in cryptocurrency) for decryption or restoration. Ransomware attacks can have devastating consequences for individuals and organizations, leading to data loss, financial extortion, and operational disruptions. These attacks often exploit vulnerabilities in software or rely on social engineering tactics to infiltrate systems.

- **Data Breaches**: Data breaches involve unauthorized access to sensitive information, such as personal data, financial records, or intellectual property. Breached data may be used for identity theft, fraud, or sold on the dark web for profit. Data breaches can occur due to security vulnerabilities in systems, insider threats, or malicious hacking activities. The consequences of data breaches can be severe, resulting in financial losses, reputational damage, and legal liabilities for affected entities.

- **Identity Theft:** Identity theft occurs when a perpetrator steals personal information, such as Social Security numbers, credit card details, or login credentials, to impersonate someone else for financial gain or other malicious purposes. Identity thieves may use stolen information to open fraudulent accounts, make unauthorized purchases, or commit other crimes in the victim's name. Identity theft can have long-lasting repercussions for victims, including financial hardship and damage to their credit history.

- **Cyberbullying:** Cyberbullying involves the use of digital communication platforms, such as social media, messaging apps, or online forums, to harass, intimidate, or threaten individuals. Cyberbullies may engage in targeted harassment, spreading malicious rumors, or sharing private information without consent. Cyberbullying can have profound psychological and emotional effects on victims, leading to anxiety, depression, and even self-harm. It is a prevalent issue, particularly among adolescents and young adults, but can affect individuals of all ages.

- **Online Fraud:** Online fraud encompasses various fraudulent schemes conducted over the internet, including investment scams, romance scams, and fake online purchases. Fraudsters may use deceptive tactics to lure victims into parting with their money or sensitive information, promising unrealistic returns or goods and services that they never intend to deliver. Online fraud schemes often exploit trust, urgency, or ignorance to manipulate victims into taking action, resulting in financial losses and emotional distress.
- **Cyber Espionage:** Cyber espionage involves unauthorized access to sensitive information or intellectual property for espionage purposes, typically perpetrated by nation-states or state-sponsored actors. Cyber spies may infiltrate government agencies, businesses, or critical infrastructure to steal classified information, trade secrets, or military intelligence. Cyber espionage poses

significant national security risks, undermining sovereignty, economic competitiveness, and diplomatic relations between nations.

- **Distributed Denial of Service (DDoS) Attacks:** DDoS attacks involve flooding a target system or network with an overwhelming volume of traffic, rendering it inaccessible to legitimate users. These attacks disrupt normal operations, causing service outages, downtime, and financial losses for affected organizations. DDoS attacks may be launched for various motives, including extortion, competitive sabotage, or ideological reasons, and can be facilitated by botnets or other malicious tools.

- **Cyber Stalking:** Cyber stalking entails the persistent harassment, surveillance, or intimidation of an individual using digital communication technologies. Cyber stalkers may use social media, email, or other online platforms to monitor their victims' activities, track their movements, or send threatening messages. Cyber stalking can escalate into offline harassment or physical violence and is often characterized by a pattern of obsessive behavior directed at the victim.

- **Child Exploitation:** Child exploitation involves the sexual abuse, grooming, or exploitation of minors through online platforms, including social media, chat rooms, or file-sharing networks. Perpetrators may coerce children into sharing explicit images or engaging in sexual acts, using manipulation, deception, or threats to exploit their vulnerability. Child exploitation is a serious and pervasive issue, with devastating consequences for victims and their families, and requires concerted efforts from law enforcement, educators, and internet service providers to combat effectively.

3. CYBER SECURITY

Ensuring the privacy and security of data remains paramount for any organization. In today's digital era, where information is predominantly stored in cyber formats, safeguarding sensitive data is imperative. Social networking platforms offer users a perceived sense of safety as they engage with friends and family. However, cybercriminals persistently target these platforms to exploit personal information. Likewise, when conducting online banking transactions, individuals must adhere to stringent security protocols. These measures are essential to mitigate the risk of data breaches and unauthorized access, thereby safeguarding personal and financial information.

INCIDENTS	JAN – JUNE 2022	JAN – JUNE 2023	PERCENTAGE (INCREASE/DECREASE)
Fraud	2439	2490	2
Intrusion	2203	1726	-22
Spam	291	614	111
Malicious Code	353	442	25
Cyber Harassment	173	233	35
Content Related	10	42	320
Intrusion Attempts	55	24	-56
Denial Services	12	10	-17
Vulnerability Reports	45	11	-76
Total	5581	5592	

Table 3.1 : Comparison of Cybersecurity Incidents between 2022 – 2023

The above Comparison of Cyber Security Incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly exhibits the cyber security threats. As crime isincreasing even the security measures are also increasing. According to the survey of U.S Technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber attacks are a serious threat to both their data and their business continuity.

- 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year.

- The majority of companies are preparing for when, not if, cyber attacks occur only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

3.1 TRENDS CHANGING IN CYBER SECURITY:

Here mentioned below are some of the trends that are having a huge impact on cybersecurity.

- **Web servers:** The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers many of which get the attention of media, are also a big threat.Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

- **Cloud computing and its services :** These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

- **APT's and targeted attacks :** APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

- **Mobile Networks:** Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.

- **IPv6 New internet protocol :** IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.

- **Encryption of the code :**Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information.

3.2 CYBER SECURITY TECHNIQUES:

Cybersecurity techniques encompass a wide array of strategies, technologies, and practices designed to protect computer systems, networks, and digital assets from cyber threats. These techniques are continually evolving to address the evolving threat landscape and encompass various layers of defense to safeguard against potential vulnerabilities and attacks. Here's a detailed exploration of some common cybersecurity techniques:

- **Firewalls :** Firewalls act as gatekeepers between an organization's internal network and the external internet. They examine incoming and outgoing network traffic, determining whether to allow or block it based on predetermined security rules. Firewalls can be hardware-based or software-based and are often deployed at network entry points, such as routers or dedicated firewall appliances. They help prevent unauthorized access, filter out malicious traffic, and protect against common network-based attacks, such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

- **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** IDS and IPS systems monitor network traffic in real-time, searching for signs of suspicious or malicious activity. IDS systems passively analyze network packets, looking for patterns indicative of known attack signatures or abnormal behavior. When a potential threat is detected, IDS systems generate alerts for further investigation. IPS systems, on the other hand, can take active measures to block or mitigate detected

threats automatically. They can drop malicious packets, block communication with malicious IP addresses, or reconfigure network access controls to prevent further exploitation.

- **Antivirus Software :** Antivirus software, also known as anti-malware software, scans files, programs, and email attachments for known malware signatures or behavioral patterns. It compares scanned items against a database of known threats and removes or quarantines any identified malware. Antivirus software helps protect against a wide range of malware types, including viruses, worms, Trojans, spyware, and ransomware. Some modern antivirus solutions also employ advanced techniques, such as heuristic analysis and machine learning, to detect and block previously unknown threats.

- **Encryption :** Encryption is the process of converting plaintext data into ciphertext using cryptographic algorithms and keys. Encrypted data is unreadable without the corresponding decryption key, ensuring confidentiality and privacy. Encryption can be applied to data both in transit (e.g., during communication over the internet) and at rest (e.g., stored on servers or devices). It protects sensitive information from unauthorized access, interception, or tampering, even if the underlying communication channels or storage media are compromised. Common encryption algorithms include AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography).

- **Access Control :** Access control mechanisms enforce policies that dictate who can access specific resources (e.g., files, folders, applications) and what actions they are allowed to perform. Access control relies on authentication to verify user identities and authorization to grant or deny access based on predefined permissions. Access control measures can include password-based authentication, biometric authentication (e.g., fingerprint or facial recognition), role-based access control (RBAC), and attribute-based access control (ABAC). By limiting access to authorized users and enforcing the principle of least privilege, access control helps prevent unauthorized access and minimize the risk of data breaches or malicious activity.

- **Security Patch Management :** Security patch management involves regularly updating software, operating systems, and firmware to address known vulnerabilities and security weaknesses. Software vendors release patches or updates to fix security flaws identified through vulnerability research or reported by users. Timely patching helps protect systems from exploitation by cyber attackers who target unpatched software to gain unauthorized access, execute arbitrary code, or steal sensitive information. Security patch management processes typically include vulnerability assessment, patch deployment, testing, and validation to ensure updates are applied effectively without causing disruption to critical systems or services.

- **Multi-factor Authentication (MFA) :** Multi-factor authentication (MFA) requires users to provide multiple forms of verification to access systems, applications, or online accounts. Typically, MFA involves combining something the user knows (e.g., a password or PIN) with something they have (e.g., a security token or mobile device) and/or something they are (e.g., biometric data such as fingerprints or facial recognition). By requiring multiple authentication factors, MFA adds an extra layer of security beyond traditional password-based authentication, reducing the risk of unauthorized access due to stolen or compromised credentials. MFA can help prevent account takeover, phishing attacks, and credential stuffing attacks by making it more difficult for attackers to impersonate legitimate users.

- **Security Awareness Training :** Security awareness training educates employees, contractors, and users about cybersecurity best practices, policies, and procedures. Training programs raise awareness of common cyber threats, teach safe computing habits, and empower individuals to recognize and respond to potential security risks effectively. Security awareness training covers topics such as password security, phishing awareness, social engineering tactics, data protection practices, and incident reporting procedures. By fostering a culture of security awareness and accountability, organizations can reduce the likelihood of human error, improve compliance with security policies, and strengthen overall cybersecurity posture.

- **Data Loss Prevention (DLP) :** Data Loss Prevention (DLP) solutions help organizations prevent the unauthorized disclosure of sensitive data by monitoring, detecting, and blocking the transmission of confidential information. DLP technologies analyze data in motion (e.g., email, web traffic), data at rest (e.g., stored files, databases), and data in use (e.g., copy-paste actions) to identify and classify sensitive information. They enforce policies to prevent data leaks or exfiltration, such as blocking email attachments containing sensitive data, encrypting sensitive files, or blocking unauthorized USB devices. DLP solutions can also provide monitoring and auditing capabilities to track data access and usage, generate compliance reports, and facilitate incident response and forensics investigations.

- **Security Information and Event Management (SIEM) :** Security Information and Event Management (SIEM) systems collect, aggregate, and analyze security event data from various sources (e.g., network devices, servers, security logs) to identify and respond to security incidents effectively. SIEM platforms provide real-time monitoring, threat detection, and incident response capabilities by correlating and analyzing security events, alerts, and logs. They use advanced analytics, machine learning, and behavioral analysis techniques to detect anomalous behavior, suspicious activities, and potential security threats.

- **Penetration Testing :** Penetration testing, also known as ethical hacking, involves simulating cyberattacks to identify and exploit vulnerabilities in systems, networks, and applications. Penetration testers use a combination of automated tools and manual techniques to assess the security posture of an organization's infrastructure and applications. They identify weaknesses, misconfigurations, and vulnerabilities that could be exploited by malicious actors to compromise systems or steal sensitive data.By conducting regular penetration tests, organizations can proactively identify and address security vulnerabilities before they are exploited by real attackers.

4. CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

- DO use the Internet to communicate and interact with other people. Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world

- Don’t be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them. Internet is considered as world’s largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.

- Do not operate others accounts using their passwords. Never try to send any kind of malware to other's systems and make them corrupt. Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.

- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble. Always adhere to copyrighted information and download games or videos only if they are permissible. The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

5. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light eachday, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

6. REFERENCES

1. Dr.V.Geetha and Dr.C K Gomathy, Anomaly Detection System in Credit Card Transaction Dataset, AIP Conference Proceedings, https://doi.org/10.1063/5.0212564 Vol 3028, Issue 01 2024
2. Dr.V.Geetha and Dr.C K Gomathy, Crime data analysis and prediction using machine learning, AIP Conference Proceedings, https://doi.org/10.1063/5.0212566 Vol 3028, Issue 01 2024
3. Dr.C K Gomathy and Dr.V.Geetha House price prediction using machine learning, AIP Conference Proceedings, https://doi.org/10.1063/5.0212559 Vol 3028, Issue 01 2024
4. Dr.V.Geetha and Dr.C K Gomathy,Identification of birds species using deep learning, AIP Conference Proceedings, https://doi.org/10.1063/5.0212968 Vol 3028, Issue 01 2024
5. Dr.V.Geetha and Dr.C K Gomathy,Missing child recognition system using deep learning, AIP Conference Proceedings, https://doi.org/10.1063/5.0212567 Vol 3028, Issue 01 2024
6.Dr.V.Geetha and Dr.C K Gomathy, Price forecasting of agricultural commodities, AIP Conference Proceedings,) https://doi.org/10.1063/5.0212568 Vol 3028, Issue 01 2024
7. Dr.V.Geetha and Dr.C K Gomathy, The customer churn prediction using machine learning , AIP Conference Proceedings, https://doi.org/10.1063/5.0212569Vol 3028, Issue 01 2024
8. Dr.C K Gomathy and Dr.V.Geetha, Fall detection for elderly people using machine learning, AIP Conference Proceedings, https://doi.org/10.1063/5.0212561 Vol 3028, Issue 01 2024
9. Dr.C K Gomathy and Dr.V.Geetha, Fall Navigation and obstacle detection for blind, AIP Conference Proceedings, https://doi.org/10.1063/5.0212560 Vol 3028, Issue 01 2024
10. Dr.V.Geetha and Dr.C K Gomathy, Securing medical image based on improved ElGamal encryption technique, AIP Conference Proceedings,) https://doi.org/10.1063/5.0212570 Vol 3028, Issue 01 2024
11. Dr.C K Gomathy and Dr.V.Geetha, Software error estimation using machine learning algorithms, AIP Conference Proceedings, https://doi.org/10.1063/5.0212562 Vol 3028, Issue 01 2024
12. Dr.V.Geetha and Dr.C K Gomathy, Web scraping using robotic process automation, AIP Conference Proceedings,) https://doi.org/10.1063/5.0212571 Vol 3028, Issue 01 2024

13. Dr.C K Gomathy and Dr.V.Geetha, Crypto sharing DAAP, AIP Conference Proceedings, https://doi.org/10.1063/5.0212563 Vol 3028, Issue 01 2024
14. Dr.V.Geetha and Dr.C K Gomathy, Company employee profile using QR code, AIP Conference Proceedings,) https://doi.org/10.1063/5.0212572 Vol 3028, Issue 01 2024
15. Dr.V.Geetha and Dr.C K Gomathy, Unified platform for advertising with predictive analysis, AIP Conference Proceedings,) https://doi.org/10.1063/5.0212573 Vol 3028, Issue 01 2024
16. Gomathy, C.K., Geetha, V., Lakshman, G., Bharadwaj, K. (2024). A Blockchain Model to Uplift Solvency by Creating Credit Proof. In: Mandal, J.K., Jana, B., Lu, TC., De, D. (eds) Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2023. Lecture Notes in Networks and Systems, vol 738. Springer, Singapore. https://doi.org/10.1007/978-981-99-4433-0_39
17. CK.Gomathy, Manganti Dhanush, Sikharam Sai Pushkar, V.Geetha ,Helmet Detection and Number Plate Recognition using YOLOv3 in Real-Time 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2023) DVD Part Number: CFP23K58-DVD; ISBN: 979-8-3503-4362-5,DOI:10.1109/ICIMIA60377.2023.10425838, 979-8-3503-4363-2/23/$31.00 ©2023 IEEE
18. Dr.V.Geetha and Dr.C K Gomathy, Cloud Network Management System, International Journal of Early Childhood Special Education (INT-JECSE) DOI:10.9756/INTJECSE/V14I5.69 ISSN: 1308-5581 Vol 14, Issue 05 2022
19. Dr.C K Gomathy and Dr.V.Geetha,Fake Job Forecast Using Data Mining Techniques, International Journal of Early Childhood Special Education (INT-JECSE) DOI:10.9756/INTJECSE/V14I5.70 ISSN: 1308-5581 Vol 14, Issue 05 2022
20. Dr.V.Geetha and Dr.C K Gomathy,Cyber Attack Detection System, International Journal of Early Childhood Special Education (INT-JECSE) DOI:10.9756/INTJECSE/V14I5.71 ISSN: 1308-5581 Vol 14, Issue 05 2022
21.Dr.V.Geetha and Dr.C K Gomathy, Attendance Monitoring System Using Opencv, International Journal of Early Childhood Special Education (INT-JECSE) DOI: DOI:10.9756/INTJECSE/V14I5.68 ISSN: 1308-5581 Vol 14, Issue 05 2022
22. Dr.C K Gomathy and Dr.V.Geetha, The Vehicle Service Management System, International Journal of Early Childhood Special Education (INT-JECSE) DOI:10.9756/INTJECSE/V14I5.66 ISSN: 1308-5581 Vol 14, Issue 05 2022
23.Dr.C K Gomathy and Dr.V.Geetha, Multi-Source Medical Data Integration And Mining For Healthcare Services, International Journal of Early Childhood Special Education (INT-JECSE) DOI: DOI:10.9756/INTJECSE/V14I5.67 ISSN: 1308-5581 Vol 14, Issue 05 2022
24.Dr.V.Geetha and Dr.C K Gomathy, An Efficient Way To Predict The Disease Using Machine Learning, International Journal of Early Childhood Special Education (INT-JECSE) DOI:10.9756/INTJECSE/V14I5.98 ISSN: 1308-5581 Vol 14, Issue 05 2022
25.Dr.C K Gomathy and Dr.V.Geetha, Music Classification Management System, International Journal of Early Childhood Special Education (INT-JECSE) DOI: DOI:10.9756/INTJECSE/V14I5.72 ISSN: 1308-5581 Vol 14, Issue 05 2022
26. Dr. C.K. Gomathy , Dr. V.Geetha ,G.S.V.P.Praneetha, M.Sahithi sucharitha. (2022). Medicine Identification Using OpenCv. Journal of Pharmaceutical Negative Results, 3718–3723. https://doi.org/10.47750/pnr.2022.13.S09.457
27. Dr. V.Geetha ,Dr. C.K. Gomathy , Kommuru Keerthi , Nallamsetty Pavithra. (2022). Diagnostic Approach To Anemia In Adults Using Machine Learning. Journal of Pharmaceutical Negative Results, 3713–3717. https://doi.org/10.47750/pnr.2022.13.S09.456
28. Dr. C. K. Gomathy, " A Cloud Monitoring Framework Perform in Web Services, International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 3, Issue 5, pp.71-76, May-June-2018.
29. Dr. C. K. Gomathy, " Supply Chain - Impact of Importance and Technology in Software Release

Management, International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 3, Issue 6, pp.01-04, July-August-2018.
30. Dr.C.K.Gomathy, Dr.V.Geetha, Peddireddy Abhiram, "The Innovative Application for News Management System," International Journal of Computer Trends and Technology, vol. 68, no. 7, pp. 56-62, 2020. Crossref, https://doi.org/10.14445/22312803/IJCTT-V68I7P109
31. Dr. C. K.Gomathy, " A Semantic Quality of Web Service Information Retrieval Techniques Using Bin Rank, IInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 3, Issue 1, pp.1568-1573, January-February-2018.
32. Gomathy, C. K., et al. "A Location Based Value Prediction for Quality of Web Service." International Journal of Advanced Engineering Research and Science, vol. 3, no. 4, Apr. 2016.