Vol. 2 No. 3 (2024)

Spectrum of Engineering Sciences

Online ISSN
3007-3138
Print ISSN
3007-312X

SPECTRUM OF ENGINEERING SCIENCES

A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks

Jawad Ahmad[1]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
Jawadahmad3389@gmail.com

Hamayun Khan[2]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Wajiha Salman[3]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan

Muzamal Amin[4]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
muzamalamin986@gmail.com

Zain Ali[5]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
Zaynlyrics123@gmail.com

Shumail Shokat[6]
Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan
Shumailshoukat888@gmail.com

Vol. 2 No. 3 (2024)
Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

Abstract

With the help of artificial intelligence methods like as generative adversarial networks (GANs), deepfake technology has developed to produce incredibly lifelike but fraudulent audio, video, and image content. This technology presents significant cybersecurity risks, including as identity theft, social engineering, and public opinion manipulation, even while it has uses in creative media and entertainment. This study explores public awareness and views of deepfake concerns, focusing on people's attitudes toward potential remedies and their level of knowledge regarding potential misuse. An online poll was included in the mixed-methods approach to collect quantitative information on public awareness, perceived risks, and views on technical or regulatory actions. The findings indicate that respondents are generally aware of deepfakes and are particularly concerned about the threats to their privacy, their confidence in digital information, and the possibility of malevolent usage in corporate or political contexts. Most participants support proactive measures to lessen these risks, such as public awareness campaigns, improved regulatory frameworks, and the creation of detecting technology. Findings show that in order to defend against deepfake dangers, lawmakers, software developers, and cybersecurity experts must act quickly to coordinate their reaction. This study adds to the expanding corpus of research on the effects of deepfakes by highlighting the significance of multi-stakeholder cooperation and educated public engagement in addressing this changing cybersecurity threat.

Keywords: Cybersecurity, Deepfake Technology, Generative Adversarial Networks (GANs), Artificial Intelligence (AI), Digital Media, Identity Theft, Social Engineering, National Security, Misinformation, Detection Algorithms, Public Awareness, Mitigation Strategies, Fraud Political.

Introduction

The cybersecurity landscape has taken on a new dimension with the introduction of deepfake technology, which brings with it both enormous [1, 2]. Deepfakes, which are produced using advanced artificial intelligence (AI) methods like generative adversarial networks (GANs), allow for the production of incredibly lifelike but completely fake material, such as pictures, videos, and audio recordings. Both cybersecurity experts and digital media users face a

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

difficult task because these modified media are frequently indistinguishable from authentic information [3, 4]. Deepfakes train AI models on large datasets of real photos and audio, then use sophisticated algorithms to create lifelike representations of people. This method enables the models to learn and replicate the traits of the target subject, producing media that realistically modifies appearances, duplicates voices, and simulates actions [5, 6]. The technology is a potent tool for both malevolent and creative reasons because it may produce content that looks real but is actually fake. Deepfakes have significant and varied cybersecurity ramifications. Deepfakes can be used for identity theft on a personal level, when dishonest actors fabricate convincing fake content to pose as people and perpetrate fraud. Deepfake movies, for example, might be used in social engineering assaults to trick people into revealing private information or taking illegal actions, which would be extremely dangerous for their privacy and personal security [7, 8]. Deepfakes pose a threat to corporate and institutional reputations by spreading false information. Deepfake campaigns may target organizations in an effort to disseminate misleading information or damage their reputation [9].

False remarks or videos may result in financial losses, business interruptions, and a decline in public confidence [10, 11]. Furthermore, deepfakes pose a threat to democratic processes and national security because to their capacity to sway public opinion and political discourse [12, 13]. It's difficult to identify and reduce the risks connected to deepfakes.

Conventional techniques for digital verification content, including metadata analysis and manual inspection, are frequently insufficient to thwart the complex changes made possible by deepfake technology [14]. The necessity for sophisticated detection methods and strong mitigation mechanisms grows as deepfakes become more convincing [15]. In order to detect deepfakes more accurately, current research and development activities are concentrated on enhancing detection algorithms and developing verification tools. Furthermore, mitigating the vulnerabilities posed by deepfakes requires regulatory agencies, cybersecurity specialists, and technology developers to collaborate and raise awareness [16]. A major cybersecurity risk is the emergence of deepfake technology. Effective management of this new threat requires an understanding of deepfakes'

Vol. 2 No. 3 (2024)
Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

characteristics, their effects on different industries, and the necessity of sophisticated detection and mitigation techniques. In order to protect against the possibly negative effects of deepfake technology, continuous attempts to improve security protocols and create creative solutions will be essential.

Figure 1. Deepfake Applications in IT Sector [3]

Literature Review

The dawn of deepfake technology, fueled by developments in artificial intelligence (AI) and machine learning, has posed a new cybersecurity frontier. Deepfakes are the fake media that result from the process of teaching AI algorithms, usually by using Generative Adversarial Networks (GANs), to generate authentic images, videos, or sounds that look like the real people [7]. Deepfakes initially came as a little bit funny, but nowadays they have become a great worry because of their potential misuse. Cybersecurity professionals, policymakers, and researchers are now tasked with dealing with the many problems this technology brings, such as misinformation, social engineering, and identity theft.

Vol. 2 No. 3 (2024)
Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

Evolution of Deepfake Technology

Deepfake technology developed from neural networks and AI-driven image processing through the next generations of the technique. GANs are the neural network-based models proposed by [17] paper and render two machines—one reproducing (generator) and the other criticizing (discriminator) to create original output through iterative learning schemes. Changes in computational power and access to large datasets have had a dramatic impact on the development of the deepfake technique in recent years, and the ability to detect real from fake content is being increasingly challenged [18, 21]. Though firstly just meant for fun and creativity, making deepfakes has grown to such an extent that a person with almost no IT knowledge can make authentic-looking, lying media [22, 25].

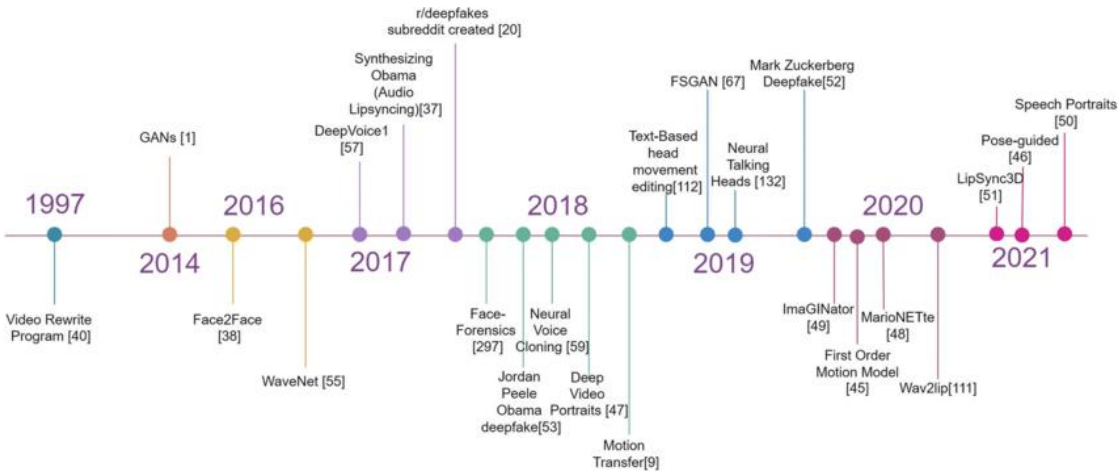

Figure 2. Evolution phases of DF Technology [26]

Development of Deepfake Technology

Neural networks and AI-based image processing have created deepfake technology as a result of the development of such technologies. [27, 30] papers came up with GANs, which are based on two neural networks—a generator and a discriminator—that through training make ever more real synthetic content. The implementation of the latest technology by means of the large computational powers and available datasets has further facilitated the making of deepfakes thus increasing the authenticity of the authentic media [32]. Although deepfake technology was at first meant for entertainment and content creation, it has developed very well, thus a user

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

with not much technical knowledge can create deceptive media, which is real in quality.

Cybersecurity Dangers Brought about by Deepfakes

Deepfake technology has been widely used both by hackers and ill-intentioned people, posing a myriad of cybersecurity threats:

Identity Theft and Fraud: Deepfake technology makes it possible for a fraudster to imitate another person's voice or face so that he can commit identity and fraud crimes. Internet thieves go for deepfake audio to do such things as vishing (voice phishing), where they pretend to be the company CEO to make fake transactions [33, 34]. Such types of attacks use the authenticity that the realistic audio deepfakes convey, thus creating major risks to companies and financial institutions.

Social Engineering and Psychological Manipulation: The high technology developments of deepfake have become a valuable tool during social engineering attacks on people. By creating layer-like videos or images humans can be the victims of criminal activities such as extortion, blackmail, or the distribution of malicious disinformation. The employment of deepfakes in political misinformation is on the rise, as the tampered images or sounds of politicians can be used to persuade the public who will vote them to power in the elections or shift public sentiment in general. The above-mentioned examples point to the most dangerous threats of deepfake to democracy and the media's credibility by fraudulent activity.

Corporate Espionage and Financial Crime: Deepfakes are frequently used in corporate espionage. Companies are being targeted with the disinformation and fraud attacks. For example, the criminals have imitated the operators by means of deep fake videos or voice calls and have been able to authorize unauthorized transactions, through which they have gotten significant financial losses. This development, on the one hand, evidences the power of deepfakes for fraud in the financial system and, on the other, highlights the necessity of powerful shield mechanisms inside the companies [35, 36].

Compromising National Security: Deepfakes present a significant threat to national security by enabling sophisticated disinformation campaigns. Such content can be used by malicious actors to spread misinformation, disrupt

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

social order, and even provoke conflict between countries. [23] paper emphasize that deepfake technology represents an "information apocalypse," wherein manipulated media could be used to create political disunity or spread false narratives, making it difficult for intelligence agencies to ascertain the credibility of digital information.

National Security Breach: Deepfakes greatly endanger national security by allowing the most elaborate information manipulation campaigns. Such content can be misused by individuals with malicious intent to spread misleading information, destroy the social fabric, or even instigate war between nations. Talk about a "digital apocalypse" in which the technology of deepfakes moves from record to manipulated media that can be utilized for political disinformation or fake news situations, making it extremely hard for intelligence agencies to.

Challenges and Mitigations of Detection

Deepfake detection still encompasses the core difficulty when the technology used to create them constantly exceeds the capacity of the detection systems. Detection algorithms include forensic techniques and deep learning models that examine, among others, the temporaries in the eyes or mouth, or the correct audio pitch, yet they are often powerless against the sophisticated deepfake methods. Blockchain-based processes are also proposed for verifying the genuineness of such media, however, rolling these out at scale is far more troublesome. Furthermore, propose a machine learning approach in which the system is exposed to the deepfake tricks that become progressively more subtle; however, this will incur a high level of maintenance.

Vol. 2 No. 3 (2024)
Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

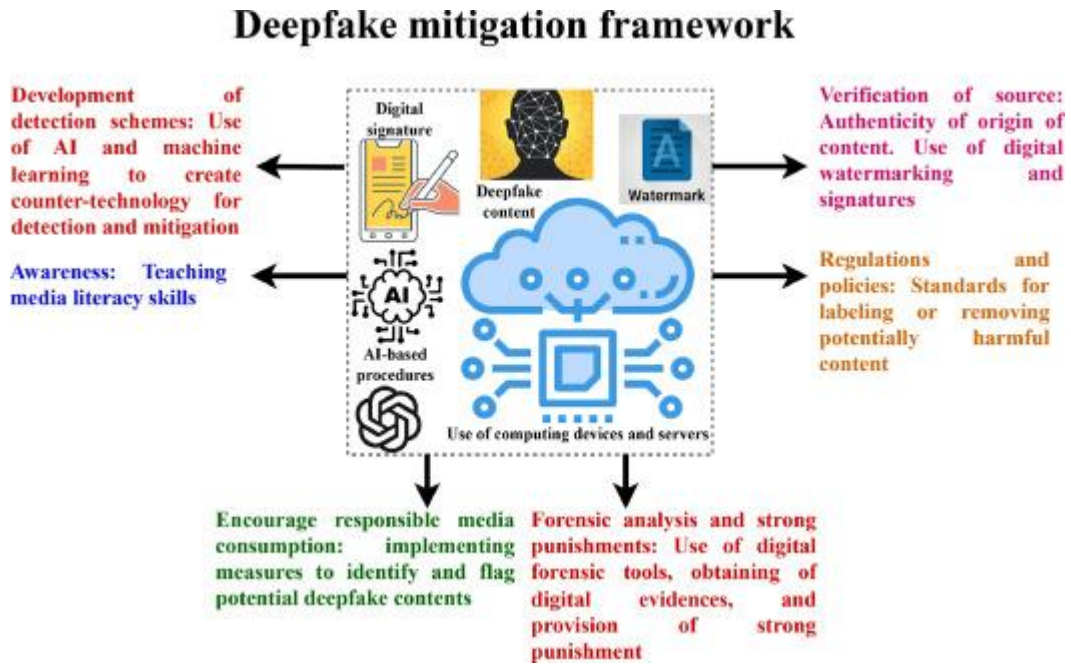

Figure 3. Challenges and Mitigations of Detection [37]

Ethical and Regulatory Challenges

The ethical and regulatory issues of deepfake technology are as a matter of fact the main complexities that need to be untangled. The situation is such that there are very few laws and regulations related to deepfake technology, and the existing ones are not fast enough to meet the pace of AI development. In the United States and the European Union, the government has passed some legislation to protect the citizens against deepfake threats, whereas the global regulatory efforts still remain fragmented and inconsistent. The ethical problems of deepfake usage are also a major issue, particularly in cases of privacy intrusion and the erosion of public trust in digital media [38].

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

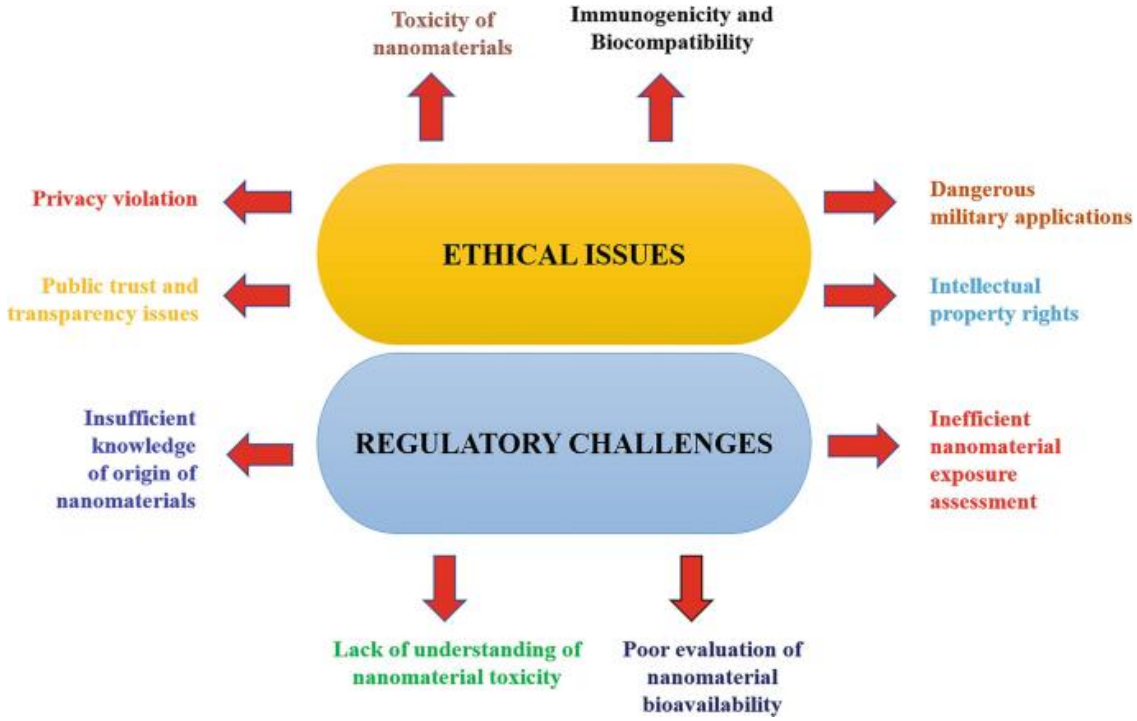

Figure 4. Ethical and Regulatory Challenges [39]

Methodology

Research Design

This study embarks a multi-faceted method to examine how the public views the main application of deepfake technology on the side of the ethics of cybersecurity. This combines the qualitative insights into technologies and other aspects of doings from the content of the documents with the quantitative data coming from a survey that passed within a small group of random respondents. Most importantly, this research will provide insights into the awareness of deep fake technology and how much these deep fake concepts concern people. In addition, it also measures the perceived level of risk arriving with it.

Survey Instrument

Primary data collection from the general public was through an online survey, designed specifically for this study to gather the views of the public on deepfakes and cybersecurity issues. Data acquisition was based on a developed questionnaire that gathered subjective impressions about deepfake, participants' familiarity with deepfake technology, the perceived threats

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

related to deepfake misuse, and the participants' related mitigation strategies were explored.

A mixture of closed-ended and Likert-scale questions was also included in the questionnaire. The survey concentrated on the major issues given below:

Awareness of Deepfake Technology: Questions estimate the knowledge and comprehension of the respondents in terms of the deepfake and how it is being generated.

Perceived Risks: Participants expressed their worries about identity theft, social engineering, corporate espionage, and national security threats caused by deepfakes.

Impact on Trust: Items of the survey examined if subjects feel deepfakes reduce trust in digital media and society.

Support for Mitigation Strategies: The respondents had to state their views on possible solution measures such as technological developments and regulations to the corresponding problems.

Demographics: Some demographic questions have also been added to categorize the responses by age groups to be used in the identification of common characteristics of people of different ages, genders, and educational backgrounds.

Sample and Data Collection

40 responses in all were gathered from participants who were enlisted online, aiming to include people from a variety of backgrounds in order to capture a variety of viewpoints. The study was able to evaluate awareness and perceptions across a range of knowledge levels because no particular requirements were placed on participants' acquaintance with deepfake technology.

Because the poll was anonymous, participants' privacy was protected and candid answers were encouraged. Two weeks were allotted for data gathering in order to give respondents enough time to respond, and the dataset that was produced reflects the general public's opinion regarding cybersecurity and deepfake technology.

Data Analysis

Descriptive and inferential statistics were used to statistically examine the survey data. Participants' awareness, perceptions of dangers, and support for

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

deepfake mitigation strategies were compiled using descriptive statistics. To give a clear picture of the overall trends in the data, frequencies, means, and percentages were computed.

To investigate the connection between participants' perceptions of deepfake hazards and demographic characteristics, inferential methods like chi-square tests were utilized. The study investigated, for instance, whether age or educational attainment affected respondents' anxiety about identity theft or support for regulatory actions.

Thematic analysis was used to find recurrent themes and insights in the qualitative answers to open-ended survey questions. This analysis helped to capture nuanced opinions and suggestions from participants regarding the ethical and regulatory challenges posed by deepfake technology.

Results

The survey results indicate significant concerns among participants regarding the use of deepfake technology, particularly its impact on privacy, corporate security, and public trust. Below are key findings derived from the responses:

Awareness of Deepfake Technology

The fact that most participants (85%) understood the idea of deepfake technology indicates that the general public is comparatively aware of deepfakes. There is a knowledge gap in the mechanics underlying deepfakes, though, as only 45% of respondents said they understood the technical parts of how they are made.

Perceived Risks

Concerns regarding the potential misuse of deepfake technology were raised by participants, who highlighted the following risks:

Fraud & Identity Theft:

- According to 70% of respondents, deepfakes seriously jeopardize both personal privacy and financial stability.
- The possibility that deepfakes could be used to mimic people and facilitate financial fraud and identity theft worries a lot of participants.

Social Engineering & Psychological Manipulation:

- According to about 65% of respondents, deepfakes are a tactic used in social engineering attacks.
- In order to trick people into disclosing private information or making bad

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

choices, participants fear that deepfakes could be used to produce phony media or messages.

Corporate Espionage

More than 60% of those surveyed believe that corporate espionage may use deepfakes.

Potential reputational damage, staff dishonesty, and the encouragement of illegal activity within businesses are among the issues.

National Security

- Approximately 55% of those surveyed are worried about how deepfakes can affect national security.
- Participants draw attention to the danger of disseminating false information during political gatherings or clashes, since this could undermine public confidence and security.

Impact on Trust

The survey results show that deepfakes significantly impact trust in digital media, with 75% of participants agreeing that deepfake technology undermines the credibility of online information. Respondents indicated that the rise of deepfakes makes it harder to trust videos, images, and audio shared on social media and other digital platforms.

Support for Mitigation Strategies

A majority of respondents supported various strategies to mitigate deepfake risks:

Technological Solutions: 68% of participants supported the development of advanced AI tools to detect deepfakes. Many respondents felt that investment in technology is essential to stay ahead of increasingly sophisticated deepfake algorithms.

Regulatory Measures: 72% supported government regulation of deepfake technology, particularly for content related to public figures and sensitive information. Respondents emphasized the need for stricter laws to hold creators of malicious deepfakes accountable.

Public Awareness Campaigns: Over 60% of respondents highlighted the importance of public education initiatives to help individuals recognize and report deepfake content.

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

Conclusion

This research outlines several challenges associated with the rise of deepfake technology in regard to cyber security. Study results reveal an increasing awareness of the national security, privacy and business risks deepfakes pose. Deepfakes blur the lines between genuine and synthetic content, eroding public trust in the veracity of digital media, and could facilitate identity theft, fraud and political disinformation.

Addressing the problem of deepfakes requires technological, legislative, and educational solutions. While new developments in AI detection techniques offer an exciting strategy for detecting deepfake content, this approach will only go so far without legislative action that establishes clear norms and avails bad actors of the necessary tools needed to be held accountable.

Public awareness campaigns can also be vital in educating citizens on the dangers of deepfake, their risks and responses.

To sum up, deepfake technology is a rising cybersecurity threat that necessitates continued study, legislative action, and public awareness campaigns. To protect people, businesses, and society at large from the possible negative effects of this innovative technology, cybersecurity experts, regulatory agencies, and technology developers must collaborate as deepfake techniques continue to advance.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[2] Aburomman, A. A., &Reaz, M. B. I. (2017). A survey of intrusion detection systems based on ensemble and hybrid classifiers.Computers & Security,65, 135-152.

[3] Chawla, N. V., & Zheng, A. X. (2021). Deepfakes: A security and privacy perspective. *IEEE Transactions on Neural Networks and Learning Systems*, 32(5), 1234–1247.

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

[4] Floridi, L. (2018). Artificial intelligence as a public policy issue. *Philosophy & Technology*, 31(4), 639–648.

[5] Kietzmann, J., McCarthy, I., & Silvestri, L. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146.

[6] Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 39–52.

[7] Agrawal, S., & Agrawal, J. (2015). Survey on anomaly detection using data mining techniques.Procedia Computer Science,60, 708-713.

[8] Ahmad, S., Lavin, A., Purdy, S., & Agha, Z. (2017). Unsupervised real-time anomaly detection for streaming data.Neurocomputing,262, 134-147.

[9] Akhi, A. B., Kanon, E. J., Kabir, A., &Banu, A. (2019).Network Intrusion Classification Employing Machine Learning: A Survey. (Doctoral dissertation)Department of Computer Science and Engineering, United International University, Bangladesh.

[10] Alizadeh, H., Khoshrou, A., &Zuquete, A. (2015). Traffic classification and verification using unsupervised learning of Gaussian Mixture Models. In2015 IEEE international workshop on measurements & networking (M&N). 1-6. IEEE. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[11] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[12] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[13] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[14] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[15] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[16] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[17] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[18] Khan, A. Yasmeen, S. Jan, U. Hashmi, "ENHANCED RESOURCE LEVELING INDYNAMIC POWER MANAGEMENT TECHNIQUEOF IMPROVEMENT IN PERFORMANCE FOR MULTI-CORE PROCESSORS" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[19] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[20] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[21] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[22] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications,

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[23] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[24] M. S. Abdul Razak, S. P. A. Gothandapani, N. Kamal, and K. Chellappan, “Presenting the Secure Collapsible Makerspace with Biometric Authentication”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 1, pp. 12880–12886, Feb. 2024.

[25] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[26] Amangele, P., Reed, M. J., Al-Naday, M., Thomos, N., & Nowak, M. (2019). Hierarchical Machine Learning for IoT Anomaly Detection in SDN. In2019 International Conference on Information Technologies (InfoTech). 1-4. IEEE.

[27] Anderson, J. P. (1980). Computer security threat monitoring and surveillance.Technical Report, Fort Washington, PA, James P. Anderson Co.

[28] Aung, Y. Y., & Min, M. M (2018). An analysis of K-means algorithm based network intrusion detection system. Advances in Science, Technology and Engineering Systems Journal,3(1), 496-501. Bauer, F. C., Muir, D. R., &Indiveri, G (2019). Real-Time Ultra-Low Power ECG Anomaly Detection

[29] Bhati, B. S., Rai, C. S., Balamurugan, B., & Al-Turjman, F. (2020). An intrusion detection scheme based on the ensemble of discriminant classifiers.Computers & Electrical Engineering,86, 106742.

[30] Bhattacharyya, D. K., &Kalita, J. K. (2013).Network anomaly detection: A machine learning perspective. CRCPress.

[31] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[32] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[33] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[34] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[35] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[36] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[37] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[38] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[39] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023