Vol. 3 No. 1 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach

Tayyba Jabeen[1]
Department of Computer science, Faculty of Computer Science and Information Technology Superior University Lahore, 54000, Pakistan. tayyabajabeen60@gmail.com

Yasir Mehmood[2]
Department of Computer Science, Faculty of Computer Science and Information Technology Superior University Lahore, 54000, Pakistan. ym03094575755@gmail.com

Hamayun Khan[3]
Department of Computer Science, Faculty of Computer Science and Information Technology Superior University Lahore, 54000, Pakistan. hamayun.khan@superior.edu.pk

Muhammad Fawad Nasim[4]
Department of Computer Science, Faculty of Computer Science and Information Technology Superior University Lahore, 54000, Pakistan. fawad.nasim@superior.edu.pk

Syed Asad Ali Naqvi[5]
Department of Computer Science, Faculty of Computer Science and Information Technology Superior University Lahore, 54000, Pakistan. syedasad.alinaqvi@superior.edu.pk

Abstract

The dark web, part of the deep web, can be accessed only through specialized computer software and used for illegal activities such as cybercrime, drug trafficking, and exploitation. Technological advancements like Tor, bitcoin, and cryptocurrencies allow criminals to carry out these activities anonymously. Identity theft

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

and data breaches are becoming considerable issues with the rapid growth in the technological world such as the dark web marketplace. This study explores some high-profile data breaches like Equifax and Anthem. Also included the financial impact of stolen data or data breaches on individuals as well as organizations. Furthermore, this article demonstrated the role of the dark web in selling stolen data. The stolen data could be a person's personal information such as name, email address, credit card details and social security number. Different data circulation approaches are discussed in this article like dark web marketplaces and forums. Cryptocurrency is being used for the transactions for such selling, because of its anonymity feature which a typical currency can not provide. This research also demonstrated the role of cyber security and laws such as GDRP and CCPA.

Keywords: Dark Web, Identity Theft, Stolen Data, Data Circulation on Dark Web, Data Breaches, Cyber Security

Introduction

In this modern world of the internet identity theft has become a big concern for individuals as well as organizations at both small and large scales. Identity theft is the illegal and intentional access and utilization of someone else's personal information it could be anything including bank account passwords, credit card numbers, or social media passwords. In 2017, a report from the U.S. Department of Justice declared that 7% or 17.6 million of the American population from 16 years old to onward were victims of identity theft [1, 2]. Identity theft can occur in many different forms such as financial fraud and illegal transactions, and medical theft which involves using stolen data to get access to medical facilities. OIT Online Identity Theft lies in the list of fastest-growing crimes

Vol. 3 No. 1 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

these days. A survey stated that in 2012 identity theft caused $2183 financial loss, later another study showed that it increased to $16 billion loss [3, 4]. One of the leading causes of identity theft is the mismanagement of confidential personal data. To avoid identity theft prevent personally identifiable information (PII) for example make sure not to share OTP SMS with anybody you do not trust. In the business sector as well, identity theft holds some severe consequences. Breaches of information about clients or employees may lead to legal complications such as losing client trust, and considerable financial penalties. Only a single breach can damage the reputation of an organization, as the impacted entities demand responsibility and assurances regarding data protection in the future [4, 5].

In [6] introduces how data breaches act as a primary facilitator of identity theft, operating as the gateway by which confidential data is accessible to hackers. When an unauthorized person or a group of people gain access to the personal information saved in a digital system via phishing attacks, malware attacks, or exploiting software vulnerabilities, is known as a data breach. For instance, Anthem, one of the high-profile health insurers in the United States faced a data breach in 2015 in which approximately 80 million individuals' personal information leaked. Prominent breaches at some other organizations such as the Sony Playstation Network data breach and Equifax have brought attention to the depth and the severity of these disasters, compromising millions of data in a single event. Even a single breach may possess far-reaching consequences due to the interconnection nature of digital ecosystems. Stolen data often contains personally identifiable information (PII) like name, address,

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

and date of birth, which is frequently connected with financial information to enable illegal measures [7, 8].

In certain cases, attackers target some specific industries where data is considered more valuable such as healthcare and finance due to its potential for exploitation. Data breaches not only limited to financial loss it also involve psychological trauma for individuals, according to more than 7% of individuals are being facing identity theft. Healthcare centers are at the top of the list for attackers to target because data is highly valuable at such locations. In the healthcare sector, from 2005 to 2019, 249.09 million individuals experienced data breaches. Furthermore, in 2018 from 65 countries, 536 data breaches were reported. Organizations confront customer trust issues and increased oversight by regulators, while victims often experience years of complications in restoring their stolen data. These outcomes demonstrate the frequent requirement of a robust cyber-security framework to avoid data breaches and preserve confidential data [9, 10]. The dark web is a hub of all illegal activities including cybercrime and drug trafficking. The dark web also emerged as a primary marketplace where stolen data circulates. It increases the impact of identity theft and data breaches. It operates as a secret part of the Internet and is accessible only via particular software like Tor, which promises the anonymity of the users. In 2021, approximately 300,000 individuals used dark web resources per day. This anonymity makes the site an attractive spot for criminal or malicious acts, such as illegal assets, and stolen personal information. The dark web is an online marketplace for anything including weapons, hire services for murder, narcotics, drugs, credit

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

card data, and indecent pornography but it is not limited to such factors [11, 12].

In 2020, more than 22 million records were sold on the dark web transactions for buying and selling purposes are facilitated through Cryptocurrencies such as Bitcoin on the dark web, because they offer an extra layer of anonymity that ordinary means of payment cannot offer [13, 14]. The use of encrypted communication channels on the dark web means that nobody on the network knows the identity of any end-to-end communication channel, further complicating locating and stop illegal acts. Consequently, in the prevention of data circulation on the dark web, cyber-security experts and law enforcement keep facing substantial difficulties [15, 16].

This paper aims to examine how stolen data circulates on the dark web while emphasizing the connection between data breaches, identity theft, and the marketplace dynamics of the dark web. Moreover, it examines the progression of stolen data from initial breach to exploitation and distribution, focusing on involved economic structures, technologies, and the participants. This paper further addresses the implications for cyber-security, ethics, and legal frameworks, demonstrates gaps in current research, and recommends strategies to tackle these difficulties. It hopes to offer concrete steps for ordinary individuals, organizations, and researchers to protect their data and combat identity theft more effectively [17, 18].

Literature Review

Over the last decade, data breaches has become one of the ongoing threats in this modern world, which is the primary facilitator of identity theft. Data breaches assist cybercriminals to

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

commit fraud and exploit victims. Usually data breach is divided into two main categories internal data breach and external data breach: internal data breach include system vulnerabilities, poor infrastructure, and unauthorized access to the database, on the other hand, external data breach include theft, hacking, and malware or ransomware [19, 20].

Data Breaches as Catalysts for Identity Theft

From 2005 to 2009, the main cause of data breaches was stolen or discarded devices including laptops, smartphones, CDs, and hard drives. Some of the most common data breaches which caused identity theft, their statistics and types are discussed below [21, 22].

Data Breach and its Financial Lost

The healthcare industry is highly affected by data breaches and cyber crimes. Data breaches in the health sector include unauthorized access or revealing sensitive health information which is typically stored in electronic health records (EHRs) or other digital systems [23]. For instance, the Anthem's data breach timeline is, from December 2014 to January 2015, which caused the revealing of 78.8 million current and previous customers' data including their names, date of birth, and social security numbers [24, 25].

Highest percentages and the risks by which the healthcare industry is affected are 72% via Malicious network traffic, 56 % through phishing, 48% by vulnerable OS, man-in-middle attacks 16% and 8% by malware (Reddy et al., 2023). In 2019, 2013 data breaches were reported from 86 countries [26]. According to IBM report, in 2019, $3.92 million was the average cost of a data breach, whereas $6.45 million was the cost of a data breach in the healthcare industry. In the first half quarter of 2008, approximately

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

86 million data breach cases were noticed, later in 2019, Kroll report stated that in last 12 month, 33% of Indian organizations had fraud data breaches where as the global figure is 29% [27, 28]. Equifax announced the largest financial identity breach of US consumers in which over 145 million records were stolen, which was caused by Equifax's Automated Consumer Interview System (ACIS) [29]. 2019 was the year of Marriott hotel data breach in which over 327 million individual records of passport and credit card information were stolen confronted a data breach that exposed emails, names, slated and hashed passwords of almost 137 million users [30, 31].

Types of Data Breaches

Data breaches are of different types but the impacts of its is almost same in every case Some types of data breaches shown in Figure 1 are discussed bellow:

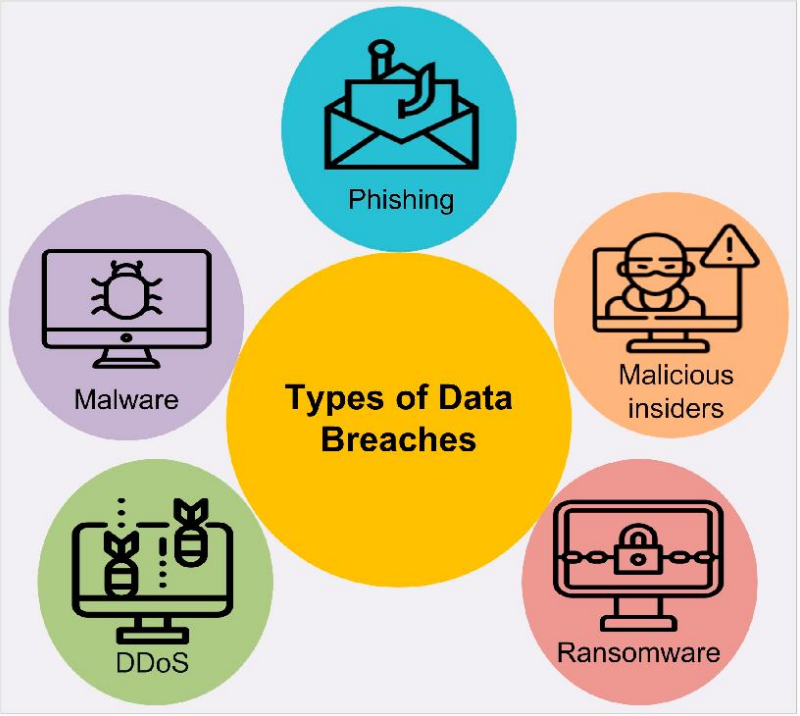

Figure 1: Data Breach's Types [32]

Vol. 3 No. 1 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Phishing Attack

Phishing is a technique by which an attacker can have important information of an internet user. Attacker gain the data by spoofing which is a fraudulent email asking user to login to a fake website. Some of the most common examples of phishing attack includes Twitter Bitcoin Scam. According to APWG report a considerable increase happened in average phishing attacks per month which was 5753%, due to which stolen data rate goes over half a billion, and data includes personal records. further mentioned that within the time duration of October 2013 to February 2016, cases of business email scam due to which financial loss was $2,3 billion were reported to FBI. And this huge loss was only because of business email scam, not any other phishing technique was involved [33, 34].

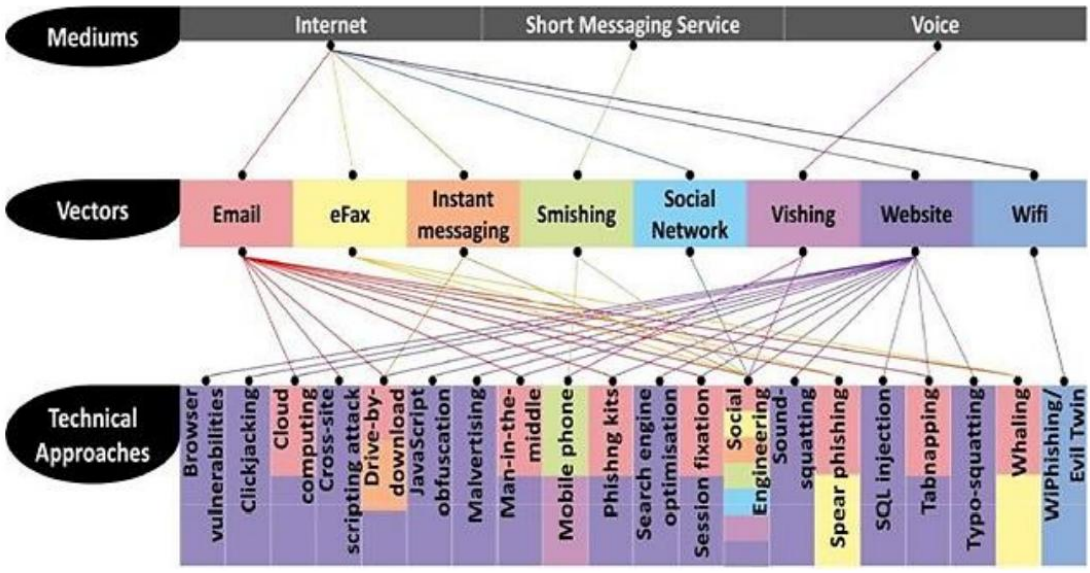

Figure 2: Phishing Attack Techniques [35]

Malware Attack

Malware are often referred to malicious software, which is a significant threat to critical infrastructure. Main focus of such attack

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

is to damage to the target's systems or the network which provide services. Viruses, ransomware, and spyware are the most common types of malware attack [36, 37]. Ransomware has been identified to create extensive attack paths that have multiple variations. It has damaged a huge number of businesses such as telecommunications, transportation, banking systems, healthcare, and public law enforcement etc. Malware attack's detection is difficult in some case, for example, zero-day malware and malware hidden in an encrypted file [38].

Legal Frameworks their Limitations and Ethical Concerns

Legal responses such as GDPR and CCPA have been instrumental in setting global standards for data protection and privacy. However, inconsistencies in enforcement have limited their effectiveness. For instance, GDPR compliance varies significantly across industries and geographic regions, with larger corporations better equipped to meet its stringent requirements compared to SMEs [39].

Furthermore, legal frameworks often lag behind technological advancements, creating regulatory gaps. According [40] the slow pace of legislative updates allows attackers to exploit new vulnerabilities before appropriate regulations are enacted. This problem is exacerbated by the lack of international cooperation in enforcing cybersecurity laws [41].

The use of surveillance and data monitoring technologies raises significant ethical questions argue that while these technologies are critical for threat detection, they often infringe upon individual privacy rights. Who examine the potential misuse of surveillance tools for purposes beyond cybersecurity, such as social control and political suppression [42, 43].

Vol. 3 No. 1 (2025)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Emerging technologies like facial recognition and biometric authentication also present ethical challenges. According to [44-46] these technologies can be prone to biases that disproportionately affect certain demographic groups, leading to discrimination and further complicating their deployment in cybersecurity systems. [47-50].

Emerging Trends and Future Directions

Recent advancements in blockchain technology and decentralized systems offer promising solutions to some of the challenges in cybersecurity [51]. highlight the potential of blockchain to enhance data integrity and reduce the risk of breaches. However, attackers are already finding ways to exploit vulnerabilities in blockchain systems [52].

Another emerging trend is the focus on cybersecurity education and awareness. human error remains a leading cause of breaches, underscoring the need for more effective training programs. This is echoed by Kumar and Sharma (2022), who emphasize the importance of cultivating a cybersecurity culture within organizations [53].

Conclusion

Identity theft, a result of data breach by which data is accessed illegally and sold on the dark web. Data breach can cause severe financial and reputational damage to the individuals as well as organizations. Some high profile data breaches are the good examples of millions dollars financial loss due to data breach including Anthem and Sony. In a data breach a person's sensitive information could be stolen and later on can be used in illegal activities. It can also be sold on the dark web. The anonymity of Tor browser and Cryptocurrency facilitate the buyers and sellers to

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

exchange data securely on the dark web. Value and the pricing of the stolen data is based on the correctness and freshness of data. Data exchange techniques involve darkweb marketplaces and forums, and encrypted communication channels making it difficult for authorities to trace illegal activities.

Whereas the laws such as GDPR and CCPA intend to secure sensitive information of users, but the enforcement of such regulations varies according to area. Additionally, criminals change their techniques much faster than an improve in security system which leads to an ongoing game of catch-up. More difficulties occur due to the ethical considerations of more powerful surveillance and data monitoring.

An extensive approach is required to tackle identity theft efficiently. Such approach could involve the installation of advanced cyber security technologies, improving the implementation of existing data protection laws, and promoting international collaboration to trace and destroy cyber-crime networks. Educational initiatives and public awareness programs can assist individuals as well as organizations to combat identity theft by adopting enhanced data security methods.

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] Hassan, Salman, Danish Irfan, Fawad Nasim, Polycarp Shizawaliyi Yakoi, Muhammad Mansab, and Saleem Zubair. "Room Occupancy Detection Using IoT Sensor Data and Machine Learning." International Journal of Social Science Archives (IJSSA) 7,

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

no. 3 (2024).

[2] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, ‘‘The security of big data in fog-enabled IoT applications including blockchain: A survey,’’ Sensors, vol. 19, no. 8, p. 1788, Apr. 2019.

[3] Imtiaz, A., Shehzad, D., Nasim, F., Afzaal, M., Rehman, M., & Imran, A. (2023, November). Analysis of Cybersecurity Measures for Detection, Prevention, and Misbehaviour of Social Systems. In 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS) (pp. 1-7). IEEE.

[4] Cellular IoT Connections Reached 3.4 Billion in 2023. Available online: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook

[5] H. 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

[6] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[7] Imtiaz, A., Shehzad, D., Nasim, F., Afzaal, M., Rehman, M., & Imran, A. (2023, November). Analysis of Cybersecurity Measures for Detection, Prevention, and Misbehaviour of Social Systems. In 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS) (pp. 1-7). IEEE.

[8] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7

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

countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[9] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[10] Nasim, F., Masood, S., Jaffar, A., Ahmad, U., & Rashid, M. (2023). Intelligent Sound-Based Early Fault Detection System for Vehicles. Computer Systems Science & Engineering, 46(3).

[11] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[12] 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

[13] 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

[14] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[15] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity

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

and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

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

[17] Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture: Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

[18] 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

[19] 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

[20] 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

[21] 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

[22] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing

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

System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[23] 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

[24] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[25] 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

[26] 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

[27] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering siences, 2(3), 528-586.

[28] 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",

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

IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 201

[29] 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

[30] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[31] 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

[32] 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

[33] 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

[34] 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

[35] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity

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

and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[36] 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

[37] 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

[38] 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

[39] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[40] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[41] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning

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

Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[42] 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

[43] O. Parker, "Building an Impenetrable Vault: Advanced Cybersecurity Strategies for Database Servers," Int. J. Cybersecurity, vol. 12, no. 4, pp. 25–34, 2024, doi: 10.1234/ijcs.2024.1254.

[44] H. Ibrahim, M. Khan, and A. Sharif, "A Study on Cybersecurity Challenges in E-learning and Database Management Systems," IEEE Access, vol. 8, pp. 112345–112356, 2020, doi: 10.1109/ACCESS.2020.9116415.

[45] M. Almaiah, K. Ali, and A. Hassan, "Classification of Cybersecurity Threats, Vulnerabilities, and Countermeasures in Database Systems," J. Tech. Sci., vol. 17, no. 8, pp. 78–89, 2024, doi: 10.4321/jts.2024.7889.

[46] S. M. Toapanta, O. A. Escalante, L. E. Mafla, and R. M. Arellano, "Analysis for the Evaluation and Security Management of a Database in a Public Organization to Mitigate Cyber Attacks," IEEE Access, vol. XX, pp. 1–14, 2020, doi: 10.1109/ACCESS.2020.3022746.

[47] M. Roberts and D. Blake, "AI-Enhanced Database Management: Strengthening Cybersecurity for Intelligent Data Protection," J. Data Sec., vol. 10, no. 1, pp. 34–45, 2023, doi: 10.6789/jds.2023.1001.

[48] E. Oye, R. Zion, and T. Adams, "Cybersecurity Threats," Cybersec Today, vol. 11, no. 5, pp. 12–22, 2024, doi: 10.9876/ct.2024.112.

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

[49] Janeja, V. P. (2022). Types of cyberattacks. In V. P. Janeja (Ed.), Data Analytics for Cybersecurity (pp. 78–90). Cambridge University Press. https://doi.org/10.1017/9781108231954.006

[50] Elkhodr, M., Shahrestani, S., & Cheung, H. (2021). Database security and privacy for IoT applications: Best practices. Journal of Information Security and Applications, 58, 102734. https://doi.org/10.1016/j.jisa.2021.102734

[51] Chen, M.; Mathews, R.; Ouyang, T.; Beaufays, F. Federated learning of out-of-vocabulary words. arXiv 2019, arXiv:1903.10635.

[52] Ammad-Ud-Din, M.; Ivannikova, E.; Khan, S.A.; Oyomno, W.; Fu, Q.; Tan, K.E.; Flanagan, A. Federated collaborative filtering for privacy-preserving personalized recommendation system. arXiv 2019, arXiv: 1901.09888.

[53] Dwork, C., McSherry,F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. Theory of computing, 4(1), 1-12.