International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i03.003 ISSN: 2581-4621

Cyber Sleuths: Strengthening Digital Defenses through Malware Detection and Prevention

Sweathashree V[1], Vaishnavi M[2], Vasika B[3], Vidhya B[4], Brinda B M[5]
[1] UG – Computer Science Engineering, Paavai College of Engineering, Namakkal, Tamilnadu
[2] UG – Computer Science Engineering, Paavai College of Engineering, Namakkal, Tamilnadu
[3] UG – Computer Science Engineering, Paavai College of Engineering, Namakkal, Tamilnadu
[4] UG – Computer Science Engineering, Paavai College of Engineering, Namakkal, Tamilnadu
[5] Assistant Professor, Computer Science Engineering, Paavai College of Engineering, Namakkal, Tamilnadu
Corresponding Author Orcid ID: https://orcid.org/0009-0004-7905-1181

ABSTRACT
Malware propagation is a significant threat to the security and privacy of individuals and organizations worldwide. To combat this ever-evolving threat, a collective effort is required to identify and report instances of malicious activities. In this project, we propose a novel approach to reporting and tracking the propagation of malware in real-time. Leveraging the power of artificial intelligence and machine learning, our system will analyze data from various sources to identify potential threats and alert users before the malware has a chance to spread. Our approach also includes a user-friendly reporting mechanism that encourages individuals to report suspicious activity, contributing to a shared database of threat intelligence. By pooling resources and expertise, we aim to create a collaborative network that can effectively identify and neutralize malware attacks, safeguarding the digital landscape for all.
Keywords-Cyber security sensor networks, indicator distribution, malware information sharing platform

1. Introduction

In today's digital age, the threat of malware spreading is ever-present. Malware, or malicious software, can infect computer systems and networks, causing data breaches, financial losses, and reputational damage. To combat this threat, cyber security professionals use a variety of tools and techniques, including Indicator of Compromise (IOC) and malware information-sharing platforms. IOCs are pieces of information that can indicate the presence of a malware infection or other security threat. These indicators can include IP addresses, domain names, file hashes, and other characteristics of a malicious file or network traffic. By monitoring these indicators, security professionals can detect and respond to threats more quickly. Malware information-sharing platforms are online communities where security researchers and professionals can share information about new and emerging threats. These platforms allow users to share IOCs, malware samples, and other information that can help identify and prevent future attacks. Through these platforms, security professionals can collaborate and work together to stay ahead of emerging threats and protects their organizations from potential harm. The combination of IOCs and malware information-sharing platforms is a powerful tool in the fight against malware. By sharing information about new threats and identifying IOCs, security professionals can quickly detect and respond to attacks, preventing them from spreading further. It is essential to participate in these platforms and share information with other professionals to stay ahead of emerging threats and keep computer systems secure. Sharing information about malware and IOCs on these platforms is crucial to staying ahead of the latest threats. By sharing information, security professionals can quickly detect and respond to attacks, preventing them from spreading further. This information sharing can also help identify the sources of malware, such as the actors behind the attack or the tools and techniques used to spread the malware. Furthermore, the value of these platforms is not just limited to cyber security professionals. They can be useful for anyone who uses digital devices, including individuals and businesses. Sharing information on these platforms can help raise awareness of emerging threats and provide valuable insights into how to protect digital assets. In conclusion, using IOCs and malware information-sharing platforms is an essential strategy for combating the threat of malware spreading. By sharing information and collaborating, cyber security professionals can stay ahead of emerging threats, protect their organizations, and maintain the integrity of their digital assets.

2. Experimental Methods or Methodology

The objective of detecting and reporting malware spreading is to prevent and mitigate the potential damage that it can cause to computer systems and networks. By identifying and reporting malware-spreading indicators, security professionals can quickly respond to threats, contain them, and prevent further damage. Detection of malware spreading can be achieved through various techniques, including monitoring network traffic for suspicious activity, scanning files for malware signatures, and analysing system logs for unusual behaviour. The goal is to identify potential indicators of malware spreading, such as IP addresses, domain names, file hashes, and other characteristics that suggest the presence of malicious software. Reporting the detection of malware spreading is equally important. Reporting can involve notifying relevant stakeholders, such as IT teams, management, and law enforcement agencies, depending on the severity of the threat. Timely reporting can prevent further damage, help identify the source of the malware, and facilitate the development of effective mitigation strategies. Effective reporting of malware spreading should be clear, concise, and contain all relevant information. This includes details about the detected malware, the affected systems, and any IOCs that were identified. This information can help other security professionals and organizations prepare for and respond to similar threats. In summary, the objective of detecting and reporting malware spreading is to prevent and mitigate the damage that it can cause. Detection involves using various techniques to identify potential indicators of malware spreading, while reporting involves notifying relevant stakeholders and sharing information about the detected threat. By achieving these objectives, security professionals can protect computer systems and networks and maintain the integrity of digital assets. One notable area of research is the use of machine-learning techniques for detecting malware propagation in large-scale networks. V. A. Siris et al. proposed a novel approach that demonstrated the effectiveness of machine learning for detecting malware propagation in real-world datasets. Another area of research is the use of Indicators of Compromise (IOCs) for detecting and responding to cyber threats. M. Shoshitaishvili et al. proposed a framework for sharing and correlating IOCs, demonstrating its effectiveness through a series of experiments. This approach can help security professionals quickly detect and respond to emerging threats, preventing further damage to computer systems and networks. In addition to detecting and responding to threats, reporting incidents is also critical for effective incident response. E. Schultz et al. conducted a comprehensive analysis of the reporting of malware incidents, including the challenges and best practices associated with reporting. Their study highlights the importance of timely and accurate reporting, as well as the need for clear and concise reporting to facilitate effective incident response. Overall, these studies highlight the importance of detecting and reporting malware spreading and provide insights into the techniques, challenges, and best practices associated with this area of research. These findings can be used to develop more effective approaches to malware detection and incident response, helping to protect computer systems and networks from emerging threats.

3. Results and Discussion

3.1 Incident Response Teams

Incident response teams need to be able to quickly and effectively respond to security incidents using a combination of technical tools and processes, as well as effective communication and collaboration with other security teams and stakeholders.

1. Preparation: Incident response teams must be prepared to respond quickly and effectively to security incidents. This includes defining roles and responsibilities, establishing incident response procedures, and implementing tools and technologies to support incident response.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i03.003 **ISSN: 2581-4621**

2. Detection and Analysis: The first step in responding to a security incident is to detect and analyse the incident. This includes monitoring security events and alerts, analysing network and system logs, and using threat intelligence to identify potential security threats.

Figure 1 System architecture of the Security Operations Centre

3. Containment and Eradication: Once a security incident has been identified, the next step is to contain and eradicate the incident. This involves isolating affected systems and networks, removing malware and other malicious code, and restoring systems and data to their pre-incident state.
4. Recovery: After the incident has been contained and eradicated, the focus shifts to recovery. This involves restoring systems and data to full functionality, verifying that systems are secure, and conducting a post-incident review to identify areas for improvement.
5. Communication and Reporting: Effective communication is critical during a security incident. This includes communicating with stakeholders, such as management, legal, and regulatory bodies, as well as providing timely and accurate incident reports.
6. Continuous Improvement: Incident response teams must continually review and improve their incident response processes and procedures. This includes conducting regular training and awareness programs, updating incident response plans, and conducting regular exercises and simulations to test the effectiveness of the incident response program.

3.2 Information Sharing and Analysis Centres

1. Audience: Technical security practitioner
2. Resource technology specifics: Host virtualization, Network function virtualization (NFV), Software-defined networking (SDN), Generic, User equipment, Radio access network (RAN), core network, enterprise network, UICC/eUICC/iUICC, Internet of Things (IoT)
3. Resource type: Process or procedure
4. Resource enforcement: Voluntary
5. Resource certification type: Self-assessment

3.3 Management and Legal Teams:

Malware: suggests harmful programming. Quite possibly of the most broadly perceived computerized risk, malware is modifying that a cybercriminal or software engineer has made to disturb or hurt a veritable client's PC. Habitually spread through an unconstrained email association or genuine looking download, malware may be used by cybercriminals to get cash or in politically prodded computerized attacks.
Infection: A self-repeating program that connects itself to clean records and spreads all through a PC framework, contaminating documents with malignant code.

DOI:10.46647/ijetms.2023.v07i03.003 ISSN: 2581-4621

Trojans: A kind of malware that is veiled as real programming. Cybercriminals stunt clients into moving Trojans onto their laptops where they inflict damage or assemble data.
Spyware: A program that rapidly records what a client does, so that cybercriminals can utilize this data. For instance, spyware could get MasterCard subtleties.
Ransom ware: Malware that secures a client's records and information, with the danger of eradicating it except if a payoff is paid.
Adware: Promoting programming that can be utilized to spread malware.
Botnets: Organizations of malware-contaminated PCs that cybercriminals use to perform undertaking online without the client's authorization.
SQL infusion SQL (organized language question) infusion is a sort of digital assault used to assume command over and take information from a data set. Cybercriminals exploit weaknesses in information-driven applications to embed malignant code into a data set utilizing a vindictive SQL explanation. This gives them permission to the fragile information contained in the informational index.
Phishing is when cybercriminals target casualties with messages that have all the earmarks of being from a real organization requesting touchy data. Phishing attacks are ordinarily used to trick people into giving over MasterCard data and other individual information.

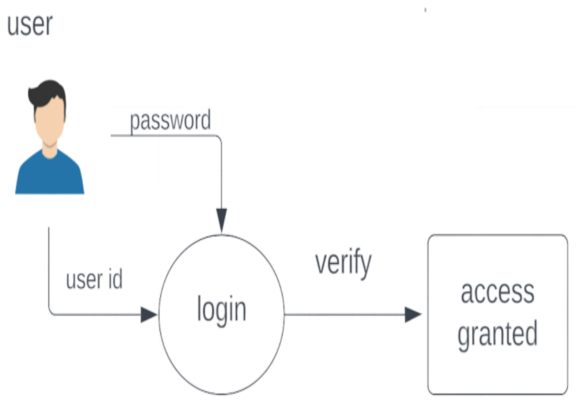

Figure 2 Information Sharing and analysis center

Man-in-the-center assault: a sort of digital danger where a cybercriminal catches correspondence between two people to take the information. For example, in a temperamental WIFI association, an aggressor could catch data being passed from the loss device and the association.
Refusal of administration assault: this is where cybercriminals keep a PC framework from satisfying genuine solicitations by overpowering the organizations and servers with traffic this delivers the framework unusable, keeping an association from completing fundamental capabilities.
Dridex malware: In December 2019, the U.S. Branch of Equity (DoJ) charged the head of a coordinated digital lawbreaker bunch as far as concerns them in a worldwide Dridex malware assault. This malevolent mission impacted general society, government, foundations, and organizations around the world.
Dridex is a financial Trojan with an extent of limits. Influencing casualties beginning around 2014, it contaminates PCs through phishing messages or existing malware. Equipped for taking passwords, banking subtleties, and individual information which can be utilized in false exchanges, it has caused huge monetary misfortunes adding up to many millions.
Because of the Dridex assaults, the UK's Public Network Protection Center encourages the general population to "guarantee gadgets are fixed, against infection is turned on and exceptional and records are supported".
Opinion stunts: In February 2020, the FBI forewarned U.S. occupants to be aware of assurance distortion that digital hoodlums complete using dating objections, conversation channels, and

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i03.003 ISSN: 2581-4621

applications. Guilty parties exploit people searching for new associates, fooling losses into offering individual data.

CONCLUSION

That's what this paper introduced; information mining advancements have fundamentally spread, starting from the start of the new hundred years. The improvements in data advancements and the detonated measures of created information have come about a rising need for information mining. Information Mining includes promising means to examine and uncover stowed-away information inside possibly a lot of information notwithstanding foreseeing future ways of behaving. In this way, it is being utilized in numerous applications for security including recognizing and characterizing malware as well concerning network safety.

On other hand, malware advancements have additionally detonated. There are a few information mining calculations that can be utilized to identify and order malware. Subsequently, there is presently a basic need to foster new DM philosophies and calculations that are versatile, quick, and adaptable for recognizing and ordering malware as well as changing crude information into valuable data to get frameworks. In any case, great information, first of all, is the necessity for better information investigation, because these calculations are all around as commendable as the information that has been gathered. The following stage is to choose the most productive strategies to mine the information. Moreover, some qualities should consider while picking reasonable information mining calculations and techniques to be utilized for a specific reason.

There are clear contrasts in the kinds of fields and issues that are conducive to every calculation. The best model is many times found by experimentation: attempting various calculations and methods that ought to apply with alert. At times, to get the most ideal outcomes, the specialists ought to be analyzed or even consolidate information mining strategies. This paper presented a survey for Malware Characterization, Malware Investigation Strategy, and Malware Discovery Method. As well as a few existing strategies for identifying and characterizing malware utilizing information mining, where we make sense of different realities of the discovery challenge, like component choice techniques, record portrayal, order calculations, and the unevenness issue.

References

1. Souri A, Norouzi M, Asghari P (2017) An analytical automated refinement approach for structural modeling large-scale codes using reverse engineering. Int J Inf Technol 9:329–333. https://doi.org/10.1007/s41870-017-0050-7
2. Cohen F (1987) Computer viruses: theory and experiments. Comput Secur 6(1):2235
3. Ször P, Ferrie P (2001) Hunting for metamorphic. In: Proceedings of 2001 Virus Bulletin Conference, Virus Bulletin, pp 123–144
4. Christodorescu M, Jha S, Maughan D, Song, Wang C (eds) Advances in information security. Malware detection, vol 27. Springer, New York, p 311
5. Ször P (2005) The art of computer virus research and defense. Addison Wesley, Saddle River, p 713
6. Christodorescu M, Jha S, Kinder J, Katzenbeisser S, Veith H (2007) Software transformations to improve malware detection. J Comput Virol 3(4):253–265
7. Souri A, Navimipour NJ, Rahmani AM (2017) Formal verification approaches and standards in cloud computing: a comprehensive and systematic review. Comput Stand Interfaces. https://doi.org/10.1016/j.csi.2017.11.007
8. Gobble, M.M. Digitalization, digitization, and innovation. *Res. Technol. Manag.* **2022**, *61*, 56–59. [**Google Scholar**] [**CrossRef**]
9. Thangavel, K.; Plotnek, J.J.; Gardi, A.; Sabatini, R. Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity. In Proceedings of the IEEE/AIAA 41st Digital Avionics Systems Conference, Portsmouth, NH, USA, 18–22 September 2022. [**Google Scholar**]

DOI:10.46647/ijetms.2023.v07i03.003 ISSN: 2581-4621

10. Harley Malware: New Attack on Android Devices. Available online: https://infosecwriteups.com/harley-malware-new-attack-on-android-devices-ae2c599c2217 (accessed on 5 June 2022).
11. Debnath, P.; Mohiuddine, S.A. *Soft Computing Techniques in Engineering, Health, Mathematical, and Social Sciences*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2021; pp. 1–232. [Google Scholar]
12. Mohurle, S.; Patil, M. A brief study of WannaCry threat: Ransomware attack 2017. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 1938–1940. [Google Scholar]
13. Aidan, J.S.; Garg, U. Advanced Petya ransomware and mitigation strategies. In Proceedings of the IEEE First International Conference on Secure Cyber Computing and Communication, London, UK, 15–17 December 2018. [Google Scholar]
14. Bernardi, L.; Mavridis, T.; Estevez, P. 150 Successful machine learning models: 6 lessons learned at booking.com. proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, New York, NY, USA, 4–8 August 2019. [Google Scholar]
15. Sasidharan, S.K.; Thomas, C. ProDroid—An Android malware detection framework based on profile hidden Markov model. *Pervasive Mob. Comput.* **2021**, *72*, 101336. [Google Scholar] [CrossRef]
16. Bin Lin, Alexey Zagalsky, Margaret-Anne D. Storey, and Alexander Serebrenik. 2016. Why Developers Are Slacking Off: Understanding How Software Teams Use Slack. In Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work and Social Computing. 333–336.
17. Andrea Di Sorbo, Sebastiano Panichella, Corrado Aaron Visaggio, Massimiliano Di Penta, Gerardo Canfora, and Harald C. Gall. 2015. Development Emails Content Analyzer: Intention Mining in Developer Discussions (T). In 30th IEEE/ACM International Conference on Automated Software Engineering, ASE 2015, Lincoln, NE, USA, November 9-13, 2015. 12–23.
18. Emad Shihab, Zhen Ming Jiang, and Ahmed E. Hassan. 2009. Studying the Use of Developer IRC Meetings in Open Source Projects. In 25th IEEE International Conference on Software Maintenance (ICSM 2009), September 20-26, 2009, Edmonton, Alberta, Canada. 147–156.
19. Antônio Mauricio Pitangueira, Paolo Tonella, Angelo Susi, Rita Suzana Pitangueira Maciel, and Márcio de Oliveira Barros. 2017. Minimizing the Stakeholder Dissatisfaction Risk in Requirement Selection for Next Release Planning. Information & Software Technology 87 (2017), 104–118.
20. Tsung-Yi Lin, Priya Goyal, Ross Girshick, Kaiming He, and Piotr Dollár. 2017. Focal Loss for Dense Object Detection. In Proceedings of the IEEE international conference on computer vision. 2980–2988.
21. Vo Ngoc Mai Anh; Hoang Kim Ngoc Anh; Vo Nhat Huy; Huynh Gia Huy; Minh Ly. "Improve Productivity and Quality Using Lean Six Sigma: A Case Study". International Research Journal on Advanced Science Hub, 5, 03, 2023, 71-83. doi: 10.47392/irjash.2023.016
22. Somu C, Karthi A, Sanjay S, Karthikeyan R, Dinesh S and Ganesh N 2017 Synthesis of various forms of carbon nanotubes by arc-discharge methods—comprehensive review Int. J. Res. Eng. Technol. 4 IRJET-V4I164
23. R. Devi Priya, R. Sivaraj, Ajith Abraham, T. Pravin, P. Sivasankar and N. Anitha. "MultiObjective Particle Swarm Optimization Based Preprocessing of Multi-Class Extremely Imbalanced Datasets". International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems Vol. 30, No. 05, pp. 735-755 (2022). Doi: 10.1142/S0218488522500209
24. Swathi Buragadda; Siva Kalyani Pendum V P; Dulla Krishna Kavya; Shaik Shaheda Khanam. "Multi Disease Classification System Based on Symptoms using The Blended Approach". International Research Journal on Advanced Science Hub, 5, 03, 2023, 84-90. doi: 10.47392/irjash.2023.017
25. Susanta Saha; Sohini Mondal. "An in-depth analysis of the Entertainment Preferences before and after Covid-19 among Engineering Students of West Bengal". International Research Journal on Advanced Science Hub, 5, 03, 2023, 91-102. doi: 10.47392/irjash.2023.018

26. Ayush Kumar Bar; Avijit Kumar Chaudhuri. "Emotica.AI - A Customer feedback system using AI". International Research Journal on Advanced Science Hub, 5, 03, 2023, 103-110. doi: 10.47392/irjash.2023.019
27. Rajarshi Samaddar; Aikyam Ghosh; Sounak Dey Sarkar; Mainak Das; Avijit Chakrabarty. "IoT & Cloud-based Smart Attendance Management System using RFID". International Research Journal on Advanced Science Hub, 5, 03, 2023, 111-118. doi: 10.47392/irjash.2023.020
28. Minh Ly Duc; Que Nguyen Kieu Viet. "Analysis Affect Factors of Smart Meter A PLS-SEM Neural Network". International Research Journal on Advanced Science Hub, 4, 12, 2022, 288-301. doi: 10.47392/irjash.2022.071
29. Lely Novia; Muhammad Basri Wello. "Analysis of Interpersonal Skill Learning Outcomes in Business English Students Class". International Research Journal on Advanced Science Hub, 4, 12, 2022, 302-305. doi: 10.47392/irjash.2022.072
30. Ms. Nikita; Sandeep Kumar; Prabhakar Agarwal; Manisha Bharti. "Comparison of multi-class motor imagery classification methods for EEG signals". International Research Journal on Advanced Science Hub, 4, 12, 2022, 306-311. doi: 10.47392/irjash.2022.073
31. Aniket Manash; Ratan Kumar; Rakesh Kumar; Pandey S C; Saurabh Kumar. "Elastic properties of ferrite nanomaterials: A compilation and a review". International Research Journal on Advanced Science Hub, 4, 12, 2022, 312-317. doi: 10.47392/irjash.2022.074
32. Prabin Kumar; Rahul Kumar; Ragul Kumar; Vivek Rai; Aniket Manash. "A Review on coating of steel with nanocomposite for industrial applications". International Research Journal on Advanced Science Hub, 4, 12, 2022, 318-323. doi: 10.47392/irjash.2022.075
33. Twinkle Beniwal; Vidhu K. Mathur. "Cloud Kitchens and its impact on the restaurant industry". International Research Journal on Advanced Science Hub, 4, 12, 2022, 324-335. doi: 10.47392/irjash.2022.076
34. V.S. Rajashekhar; T. Pravin; K. Thiruppathi , "Control of a snake robot with 3R joint mechanism", International Journal of Mechanisms and Robotic Systems (IJMRS), Vol. 4, No. 3, 2018. Doi: 10.1504/IJMRS.2018.10017186
35. T. Pravin, C. Somu, R. Rajavel, M. Subramanian, P. Prince Reynold, Integrated Taguchi cum grey relational experimental analysis technique (GREAT) for optimization and material characterization of FSP surface composites on AA6061 aluminium alloys, Materials Today: Proceedings, Volume 33, Part 8, 2020, Pages 5156-5161, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2020.02.863.
36. Pravin T, M. Subramanian, R. Ranjith,Clarifying the phenomenon of Ultrasonic Assisted Electric discharge machining, "Journal of the Indian Chemical Society", Volume 99, Issue 10, 2022, 100705, ISSN 0019-4522, Doi: 10.1016/j.jics.2022.100705
37. M. S. N. K. Nijamudeen, G. Muthuarasu, G. Gokulkumar, A. Nagarjunan, and T. Pravin, "Investigation on mechanical properties of aluminium with copper and silicon carbide using powder metallurgy technique," Advances in Natural and Applied Sciences, vol. 11, no. 4, pp. 277–280, 2017.
38. T. Pravin, M. Sadhasivam, and S. Raghuraman, "Optimization of process parameters of Al10% Cu compacts through powder metallurgy," Applied Mechanics and Materials, vol. 813-814, pp. 603–607, 2010.
39. Rajashekhar, V., Pravin, T., Thiruppathi, K.: A review on droplet deposition manufacturing a rapid prototyping technique. Int. J. Manuf. Technol. Manage. 33(5), 362–383 (2019) https://doi.org/10.1504/IJMTM.2019.103277
40. Rajashekhar V S, Pravin T, Thirupathi K, Raghuraman S.Modeling and Simulation of Gravity based Zig-zag Material Handling System for Transferring Materials in Multi Floor Industries. Indian Journal of Science and Technology.2015 Sep, 8(22), pp.1-6.
41. Shoeb Ahmed Syed; Steve Ales; Rajesh Kumar Behera; Kamalakanta Muduli. "Challenges, Opportunities and Analysis of the Machining Characteristics in hybrid Aluminium Composites (Al6061-SiC-Al2O3) Produced by Stir Casting Method". International Research Journal on Advanced Science Hub, 4, 08, 2022, 205-216. doi: 10.47392/irjash.2022.051

42. Nirsandh Ganesan; Nithya Sri Chandrasekar; Ms. Gokila; Ms. Varsha. "Decision Model Based Reliability Prediction Framework". International Research Journal on Advanced Science Hub, 4, 10, 2022, 236-242. doi: 10.47392/irjash.2022.061
43. Vishnupriya S; Nithya Sri Chandrasekar; Nirsandh Ganesan; Ms. Mithilaa; Ms. Jeyashree. "Comprehensive Analysis of Power and Handloom Market Failures and Potential Regrowth Options". International Research Journal on Advanced Science Hub, 4, 10, 2022, 243-250. doi: 10.47392/irjash.2022.062
44. Ashima Saxena; Preeti Chawla. "A Study on the Role of Demographic Variables on Online Payment in Delhi NCR". International Research Journal on Advanced Science Hub, 4, 08, 2022, 217-221. doi: 10.47392/irjash.2022.052
45. Vishnupriya S; Nirsandh Ganesan; Ms. Piriyanga; Kiruthiga Devi. "Introducing Fuzzy Logic for Software Reliability Admeasurement". International Research Journal on Advanced Science Hub, 4, 09, 2022, 222-226. doi: 10.47392/irjash.2022.056
46. GANESAN M; Mahesh G; Baskar N. "An user friendly Scheme of Numerical Representation for Music Chords". International Research Journal on Advanced Science Hub, 4, 09, 2022, 227-236. doi: 10.47392/irjash.2022.057
47. Kakali Sarkar; Abhishek Kumar; Sharad Chandra Pandey; Saurabh Kumar; Vivek Kumar. "Tailoring the structural, optical, and dielectric properties of nanocrystalline niobate ceramics for possible electronic application". International Research Journal on Advanced Science Hub, 5, 01, 2023, 1-7. doi: 10.47392/irjash.2023.001
48. Pavan A C; Somashekara M T. "An Overview on Research Trends, Challenges, Applications and Future Direction in Digital Image Watermarking". International Research Journal on Advanced Science Hub, 5, 01, 2023, 8-14. doi: 10.47392/irjash.2023.002
49. Pavan A C; Lakshmi S; M.T. Somashekara. "An Improved Method for Reconstruction and Enhancing Dark Images based on CLAHE". International Research Journal on Advanced Science Hub, 5, 02, 2023, 40-46. doi: 10.47392/irjash.2023.011
50. Subha S; Sathiaseelan J G R. "The Enhanced Anomaly Deduction Techniques for Detecting Redundant Data in IoT". International Research Journal on Advanced Science Hub, 5, 02, 2023, 47-54. doi: 10.47392/irjash.2023.012
51. Nguyen Kieu Viet Que; Nguyen Thi Mai Huong; Huynh Tam Hai; Vo Dang Nhat Huy; Le Dang Quynh Nhu; Minh Duc Ly. "Implement Industrial 4.0 into process improvement: A Case Study in Zero Defect Manufacturing". International Research Journal on Advanced Science Hub, 5, 02, 2023, 55-70. doi: 10.47392/irjash.2023.013
52. Gyanendra Kumar Pal; Sanjeev Gangwar. "Discovery of Approaches by Various Machine learning Ensemble Model and Features Selection Method in Critical Heart Disease Diagnosis". International Research Journal on Advanced Science Hub, 5, 01, 2022, 15-21. doi: 10.47392/irjash.2023.003
53. Nirsandh Ganesan; Nithya Sri Chandrasekar; Ms. Piriyanga; Keerthana P; Mithilaa S; Ms. Jeyashree. "Effect of Nano Reinforcements Tio2 And Y2O3 on Aluminium Metal Matrix Nanocomposite". International Research Journal on Advanced Science Hub, 5, 01, 2023, 22-32. doi: 10.47392/irjash.2023.004
54. Nur Aeni; Lely Novia; Mr. Muhalim; Nur Fitri. "Incorporating Secret Door in Teaching Vocabulary for EFL Vocational Secondary School Students in Indonesia". International Research Journal on Advanced Science Hub, 5, 01, 2023, 33-39. doi: 10.47392/irjash.2023.005