iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** II **Month of publication:** February 2024

DOI: https://doi.org/10.22214/ijraset.2024.58701

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue II Feb 2024- Available at www.ijraset.com

Analyze and Forecast the Cyber Attack Detection

Prof. Prakash Kshirsagar [1], Prof. Vrushali Wankhede[2], Abhijeet Hingane[3], Pankaj Kadam[4], Rutuja Patil[5], Harshali Tolkar[6]
[1, 2, 3, 4, 5, 6]*Keystone School of Engineering, Savitribai Phule Pune University, Pune*

Abstract: ***The relentless evolution of digital technologies has ushered in an era of unprecedented connectivity and convenience, but it has also exposed our digital infrastructure to a growing spectrum of cyber threats. In this context, the importance of robust cyber attack detection mechanisms cannot be overstated.The increasing complexity and sophistication of cyber threats necessitate equally advanced detection techniques.***
Cyber attack detection plays a pivotal role in safeguarding digital assets and maintaining the integrity of critical systems. This abstract delves into the foundational principles and contemporary strategies employed in this domain. Detecting cyber attacks presents a multifaceted challenge due to the ever-evolving tactics employed by malicious actors.
Keywords: Anomaly Detection , Signature-Based Detection, Behavioral Analysis, Network Traffic Analysis

I. INTRODUCTION

In today's digital age, cyberattacks have become a significant threat to individuals, organizations, and governments worldwide. These attacks can range from simple phishing attempts to highly sophisticated, state-sponsored cyber espionage. To safeguard sensitive data, critical infrastructure, and overall cybersecurity, it is crucial to have robust cyber attack detection mechanisms in place. Cyber attack detection is the process of identifying, analyzing, and responding to unauthorized access, malicious activities, or anomalies within computer systems, networks, and digital environments.

The primary goal of cyber attack detection is to detect and mitigate threats as quickly as possible to minimize damage and protect data integrity, confidentiality, and availability.

The applicability of cyber attack detection is universal, cutting across industries and sectors, underscoring its fundamental role in preserving data integrity, privacy, operational continuity, and safeguarding against the myriad of cyber threats prevalent in today's interconnected world.

Detection systems have evolved to swiftly identify complex and sophisticated cyber threats, including malware, ransomware, phishing attempts, and zero-day exploits, enabling proactive responses to mitigate potential damages.

Achievements in detection technologies allow for continuous real-time monitoring of network activities, enabling the rapid identification of anomalies and suspicious behavior that could signal a potential cyber attack.

II. SYSTEM ARCHITETURE

1) Designing architecture for a Cyber Attack Detection System involves integrating various components to monitor, analyse, and respond to potential threats effectively.
2) System logs from servers, endpoints, firewalls, and other network devices.
3) Data collected from different sources are pre-processed to ensure uniformity and readiness for analysis.
4) Dashboards and visualizations to present real-time threat intelligence, detection trends, and incident response metrics.
5) Continuous monitoring and feedback mechanisms are essential to evaluate the effectiveness of the Cyber Attack Detection System and adapt to evolving threats.
6) Implementing a comprehensive architecture that encompasses these layers, organizations can enhance their capabilities for detecting, analysing, and responding to cyber threats effectively, thereby strengthening their overall cybersecurity posture.

©IJRASET: All Rights are Reserved

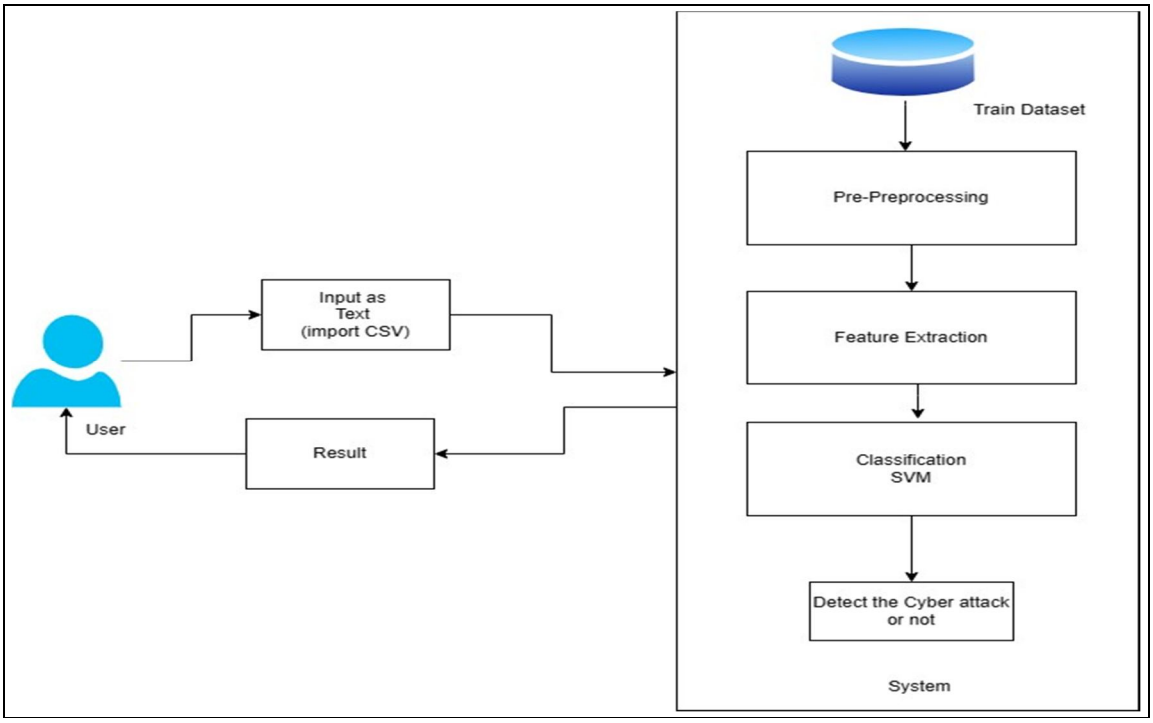


Figure a - System Architecture

III. LITERATURE SURVEY

1) Paper Name: Multivariate Gaussian-Based False Data Detection Against Cyber-Attacks
Author: YU AN , AND DONG LIU ,
Abstract :Modern distribution power system has become a typical cyber-physical system (CPS), where reliable automation control process is heavily depending on the accurate measurement data. However, the cyber-attacks on CPS may manipulate the measurement data and mislead the control system to make incorrect operational decisions. Two types of cyber-attacks (e.g., transient cyber-attacks and steady cyberattacks) as well as their attack templates are modeled in this paper. To effectively and accurately detect these false data injections, a multivariate Gaussian based anomaly detection method is proposed. The correlation features of comprehensive measurement data captured by micro-phasor measurement units (μPMU) are developed to train multivariate Gaussian models for the anomaly detection of transient and steady cyberattacks, respectively. A k-means clustering method is introduced to reduce the number of μPMUs and select the placement of μPMUs. Numerical simulations on the IEEE 34 bus system show that the proposed method can effectively detect the false data injections on measurement sensors of distribution systems.

2) Paper Name: KeySplitWatermark: Zero Watermarking Algorithm for SoftwareProtection Against Cyber-Attacks
Author: CELESTINE IWENDI ABDUL REHMAN JAVED
Abstract :Cyber-attacks are evolving at a disturbing rate. Data breaches, ransomware attacks, cryptojacking, malware and phishing attacks are now rampant. In this era of cyber warfare, the software industry is also growing with an increasing number of software being used in all domains of life. This evolution has added to the problems of software vendors and users where they have to prevent a wide range of attacks. Existing watermark detection solutions have a low detection rate in the software. In order to address this issue, this paper proposes a novel blind Zero code based Watermark detection approach named KeySplitWatermark, for the protection of software against cyber-attacks. The algorithm adds watermark.

3) Paper Name: Cyber-attack Detection Strategy Based on Distribution System State Estimation
Author: Huan Long, Zhi Wu, Member, Chen Fang
Abstract :Cyber-attacks that tamper with measurement information threaten the security of state estimation for the current distribution system. This paper proposes a cyberattack detec- tion strategy based on distribution system state estimation (DSSE). The uncertainty of the distribution network is repre- sented by the interval of each state variable.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

A three-phase in- terval DSSE model is proposed to construct the interval of each state variable. An improved iterative algorithm (IIA) is devel- oped to solve the interval DSSE model and to obtain the lower and upper bounds of the interval. A cyber-attack is detected when the value of the state variable estimated by the traditional DSSE is out of the corresponding interval determined by the in- terval DSSE.

4) Paper Name: Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning
Author: AHMED SAMY 1,2, HAINING YU , AND HONGLI ZHANG
Abstract :The number of cyber-attacks and data breaches has immensely increased across different enterprises, companies, and industries as a result of the exploitation of the weaknesses in securing Internet of Things (IoT) devices. The increasing number of various devices connected to IoT and their different protocols has led to growing volume of zero-day attacks. Deep learning (DL) has demonstrated its superiority in big data fields and cyber-security. Recently, DL has been used in cyber-attacks detection because of its capability of extracting and learning deep features of known attacks and detecting unknown attacks without the need for manual feature engineering. However, DL cannot be implemented on IoT devices with limited resources because it requires extensive computation, strong power and storage capabilities. This paper presents a comprehensive attack detection framework of a distributed, robust, and high detection rate to detect several IoT cyber-attacks using DL

5) Paper Name: Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks
Author: ATHANASIOS DIMITRIADIS, EFSTRATIOS LONTZETIDIS
Abstract:Traditional attack detection approaches utilize predefined databases of known signatures about already-seen tools and malicious activities observed in past cyber-attacks to detect future attacks. More sophisticated approaches apply machine learning to detect abnormal behavior. Nevertheless, a growing number of successful attacks and the increasing ingenuity of attackers prove that these approaches are insufficient. This paper introduces an approach for digital forensics-based early detection of ongoing cyber-attacks called Fronesis. The approach combines ontological reasoning with the MITRE ATTCK framework, the Cyber Kill Chain model, and the digital artifacts acquired continuously from the monitored computer system.

IV. METHODOLOGY

1) Cyber attack detection methodologies encompass a range of techniques and strategies aimed at identifying, mitigating, and responding to malicious activities within a computer network or system.
2) This approach involves comparing incoming network traffic, files, or activities against a database of known attack signatures. If a match is found, it indicates a potential cyber attack.
3) Machine learning and statistical analysis are commonly used in anomaly detection systems.
4) Analysis involves using predefined rules or algorithms to identify suspicious patterns or activities that may indicate a cyber attack.
5) Implementing a comprehensive incident response plan, coupled with continuous monitoring of systems and networks, is essential for timely detection and response to cyber attacks.
6) The regular updates, testing, and refinement of detection methodologies are crucial to staying ahead of evolving cyber threats.

A. Analysis Model-SDLC model to be applied

The software development cycle is a combination of different phases such as designing, implementing and deploying the project. These different phases of the software development model are described in this section. The SDLC model for the project development can be understood using the following figure The chosen SDLC model is the waterfall model which is easy to follow and fits bests for the implementation of this project.

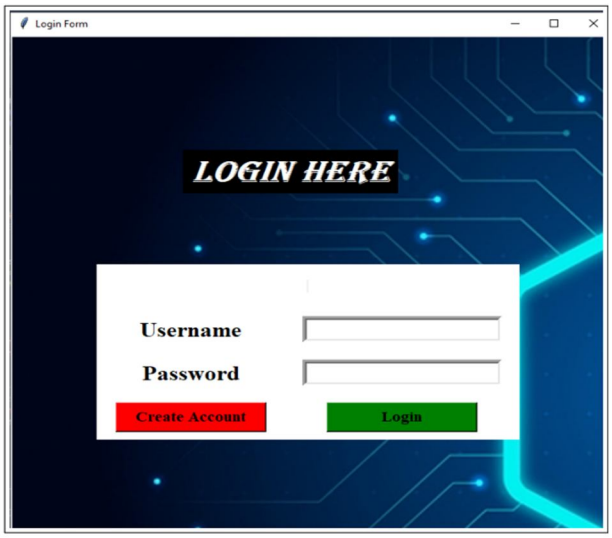
1) *Requirements Analysis:* At this stage, the business requirements, definitions of use cases are studied and respective documentations are generated.
2) *Design:* In this stage, the designs of the data models will be defined and different data preparation and analysis will be carried out.
3) *Implementation:* The actual development of the model will be carried out in this stage. Based on the data model designs and requirements from previous stages, appropriate algorithms, mathematical models and design patterns will be used to develop the agent's back-end and front-end components.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

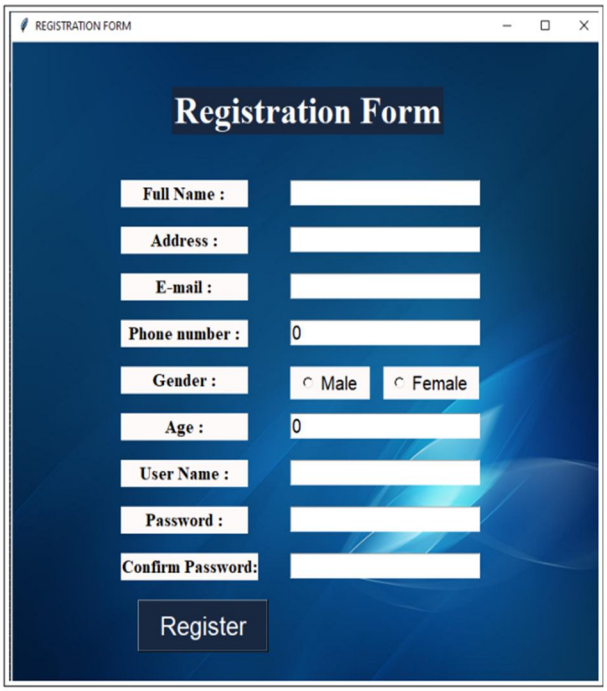
4) *Testing:* The developed model based on the previous stages will be tested in this stage. Various validation tests will be carried out over the trained model.
5) *Deployment:* After the model is validated for its accuracy scores its ready to be deployed or used in simulated scenarios.
6) *Maintenance:* During the use of the developed solution various inputs/scenarios will been countered by the model which might affect the models overall accuracy. Or with passing time the model might not fit the new business requirements. Thus, the model must be maintained often to keep its desired state of operation. SVMs can model non-linear decision boundaries effectively using techniques like the kernel trick, which transforms data into a higher-dimensional space where nonlinear relationships become linear.

V. RESULT

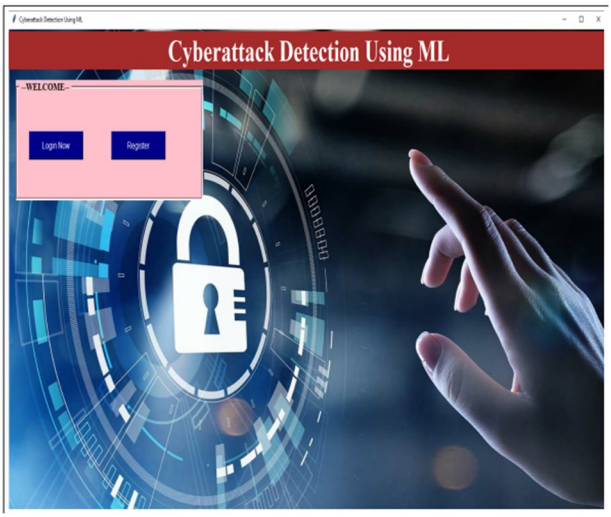
1) *Login Page:*



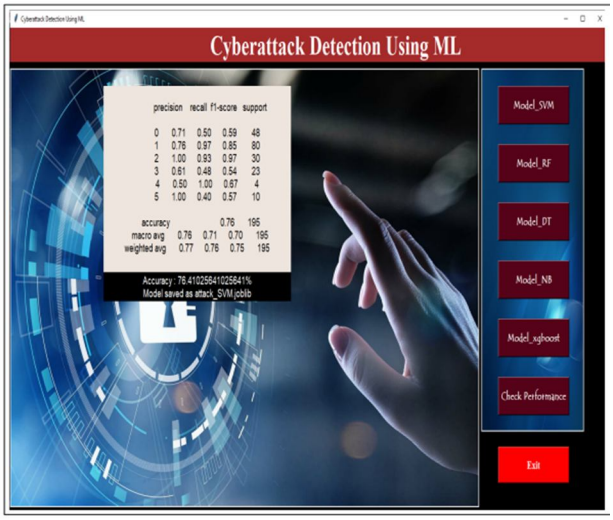
2) *Registration Page:*



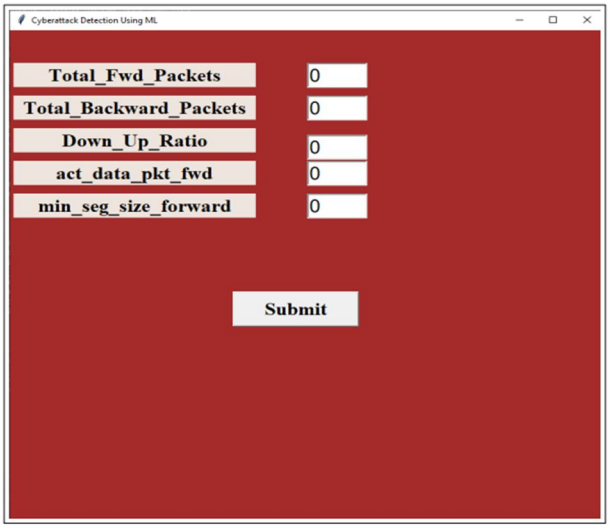
3) *GUI Main Page:*



4) *Output1 page:*



5) *Output2 page:*



VI. CONCLUSION

In conclusion, cyber attack detection plays a vital role in modern cyber security by providing early threat detection, but it comes with limitations and requires careful planning and management to be effective. Its applications span across various domains to protect against a wide range of cyber threats.

VII. AKNOWLEDGEMENT

We would like to express our deep and sincere gratitude to our Director Prof. Y.R.Soman, Principal Dr.Sandeep Kadam HOD Prof. Sagar Rajebhosale, Project guide Prof. Prakash Kshirsagar and project Co-guide Prof. Vrushali Wankhede for giving us the opportunity to do this project and provide valuable guidance throughout this project. From the inception of the project to its completion, provided unwavering encouragement, expert insights, and constructive feedback that significantly contributed to the success of this project. Their dedication to fostering learning and innovation has been a constant source of inspiration. We are truly fortunate to have had the opportunity to work under Prof. Prakash Kshirsagar's Guidance. Their wealth of knowledge, patience, and commitment to excellence have not only enriched the project but also enhanced my understanding of the subject matter.

REFERENCES

[1] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," IEEE Trans. Smart Grid, vol. 6, no. 5, pp. 2375–2385, Sep. 2021

[2] A. R. Javed, M. O. Beg, M. Asim, T. Baker, and A. H. Al-Bayatti, "AlphaLogger: Detecting motion-based side-channel attack using smartphone keystrokes," J. Ambient Intell. Humanized Comput., pp. 1–14, Feb. 2020

[3] K. Zetter. (2020, Mar.). Inside the cunning, unprecedented hack of Ukraine's power grid. [Online]. Available: https://wired.com

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," IEEE Internet Things J., vol. 4, no. 5, pp. 1250–1258, Oct. 2021.3.

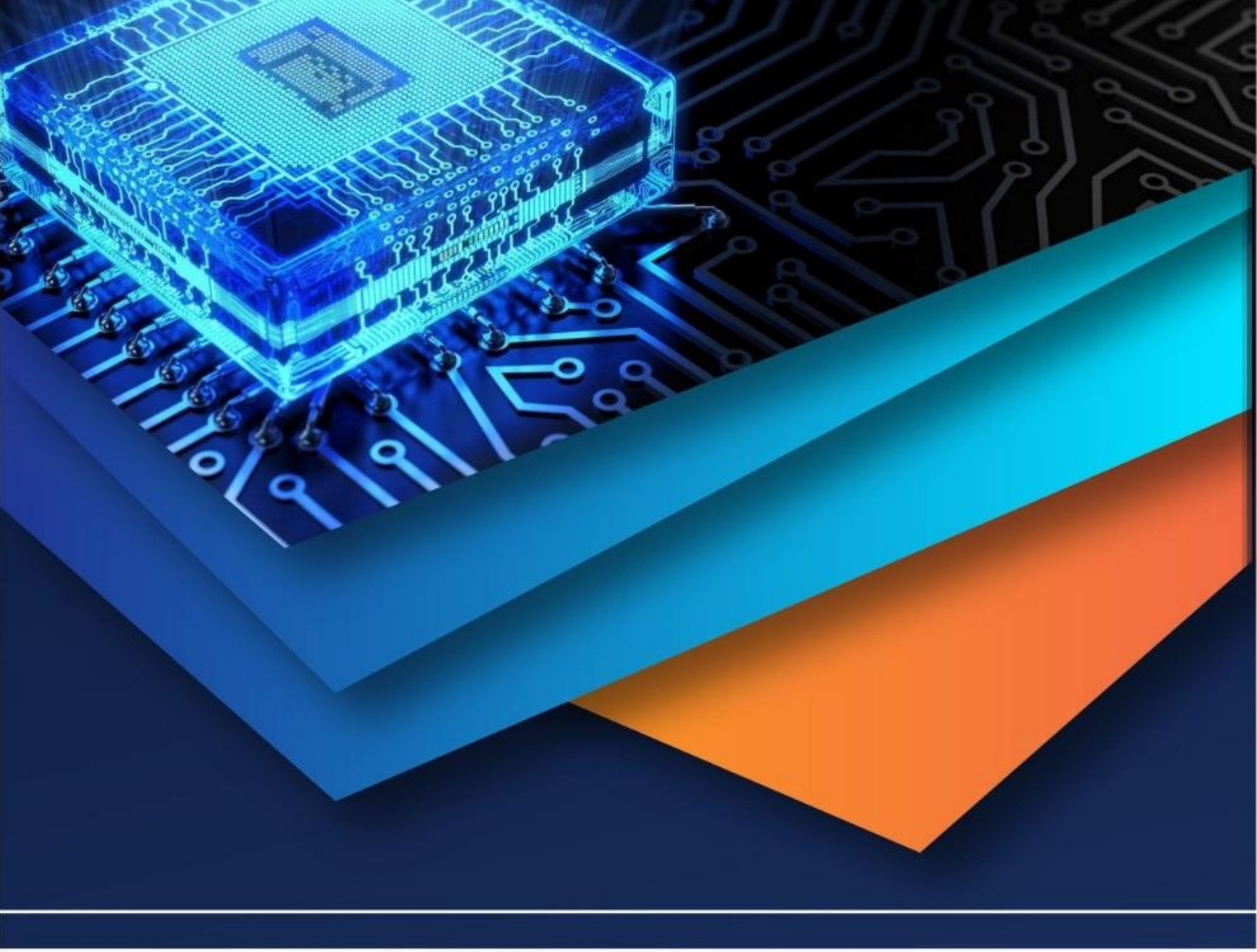
[5] H. Karimipour and V. Dinavahi, "Extended Kalman filter-based parallel dynamic state estimation," IEEE Trans. Smart Grid, vol. 6, no. 3, pp. 1539–1549, May 2019.

[6] M. P. Barrett, "Framework for improving critical infrastructure cybersecurity, version 1.1," NIST Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. CSWP 04162018, Apr. 2020.

[7] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, and S. Padmanaban, "False data injection attack detection based on Hilbert-huang transform in AC smart islands," IEEE Access, vol. 8, pp. 179002–179017, 2020.

[8] K. Chatterjee, V. Padmini, and S. Khaparde, "Review of cyber attacks on power system operations," in Proc. IEEE Region Symp. (TENSYMP), Jul.2020, pp. 1–6

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)