iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VIII **Month of publication:** August 2021

DOI: https://doi.org/10.22214/ijraset.2021.37831

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: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

Calibration and Asset Management Software

Vaishnavi Badgire[1], Dr. Nitin Gavankar[2]
[1] *Student,* [2]*Assistant Professor, Walchand College of Engineering, Sangli*

Abstract: ***In an industry, to ensure smooth and reliable working of machines, calibration is an important phase to rectify the changes of devices. This solution is a new milestone in calibration and asset management industry. A web-based application provides portability to the application hence; share-holders/proprietors/industrialist can manage their assets any time, any-where. To make any application reliable and Secure, testing is an important phase. The intent of a security testing is to identify the vulnerabilities, so that the developers can pull out these vulnerabilities from the application and make the web application and data safe from any unauthorized action. Tools such as Zenmap, OWSAP, and OpenSSL used to ensure unbreakable working of application.***

Keywords: Calibration, Asset Management, Security Testing, HTTP's Conversion

I. INTRODUCTION

Calibration is a measurement of the difference between device to be tested and standard. When application is working in real scenario, small precision mistake in values of measurement can turn into big loss. Hence, getting the correct measurements is an important aspect in asset management, in order to validate measurement values provided for instruments/devices and calibration used. Calibration and Asset Management software application provides a large number of features to calibration management. Web based design of software permits you to get information whenever, anywhere eliminating the requirement for keeping up/maintaining and overseeing paper-based records. Security testing is a way of protection of application data to be modified, truncate, copied by unauthorized or malicious user. The breaking of system by using various security testing tools can be helpful to prevent security scenarios when application works in real environment, hence rigorous security testing is essential in order to remove any potential loopholes before application goes in action.

II. LITERATURE REVIEW

1) *The Traditional Calibration Process:* The 8-step process shown in Fig 1, highlights the traditional paper-based calibration process. This is highly inefficient, labor intensive and involves manual data storage, which is time consuming, and error prone.

a) *Less Efficient:* The 8-step process takes more than 2 hours to complete, due to the intensive preparation and verification of results required.

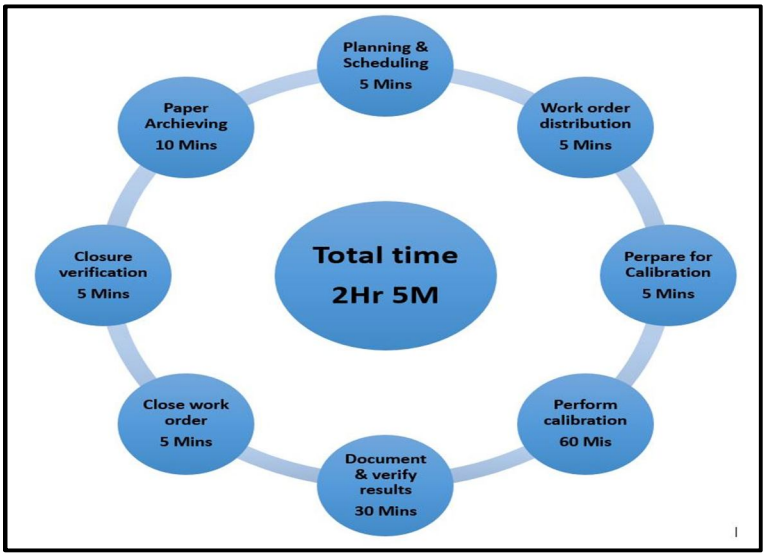


Figure 1. Traditional Calibration Process (7.2.1)

2) *The new Improved Calibration Process:* By utilizing the Calibration and Asset management software, in order to automate the calibration process which also removes manual data entry and storage. Further the process may also improve efficiency in terms time and money.

a) *Up to 40 Percent Faster:* Calibration and Asset Management software may complete the calibration process 40 percent faster than paper-based calibration.

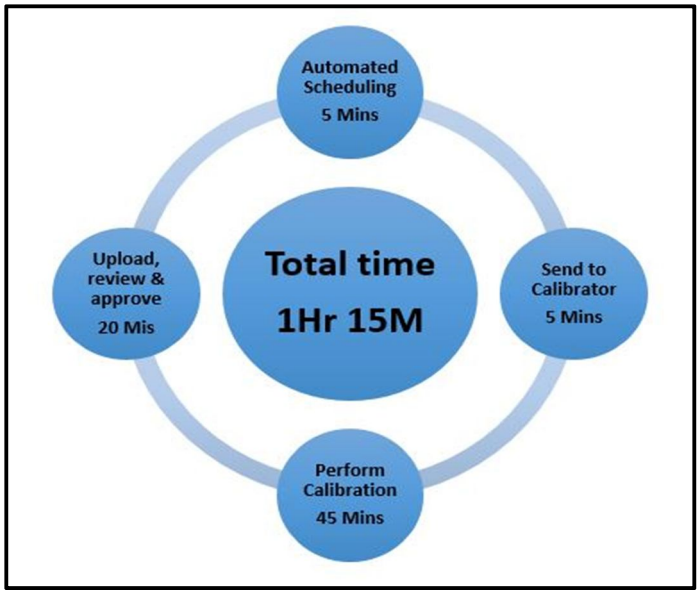


Figure 2. The New Improved Calibration Process (7.2.1)

Considering all above issues, the main Objective of this study is to improve security of software which manages or monitors the threats. Further, the main objectives is divided into 3 steps:

- To understand the basic concepts of Calibration and Asset.
- To implement enhancements and fix existing defects.
- To analyze and evaluate accuracy and performance of proposed system.

III. METHODOLOGY

In software development release, security testing is one of the most important part. Security testing of any system focuses on finding all possible loopholes and weaknesses of the system that might result into the loss of information or reputation of an organization.

Fig 3 shows security testing of Calibration and Asset Management Software Application –

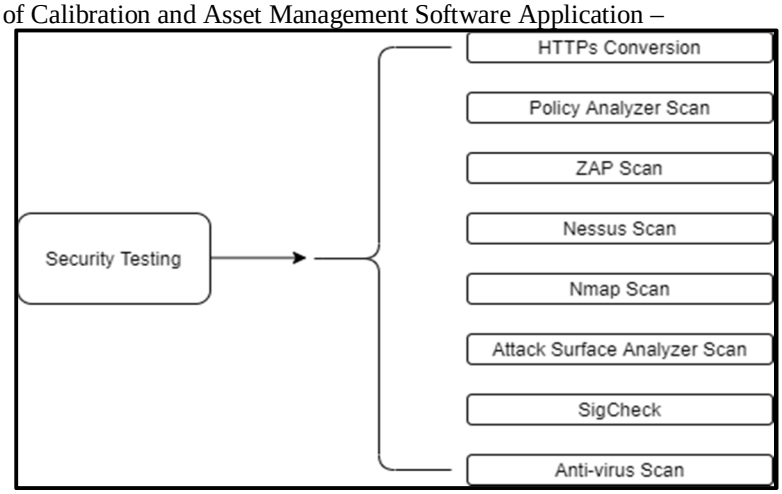


Figure 3. Security Testing Types

1) *HTTP's Conversion:* HTTPs conversion makes your web application alongside all the information you get from clients safer and more secure. It assists with limiting danger of information burglary and abuse of individual data. It improves positive positioning on Google. For clients, endorsements are simple approach to construct trust.

Steps for generating Digital Signature Certificate –

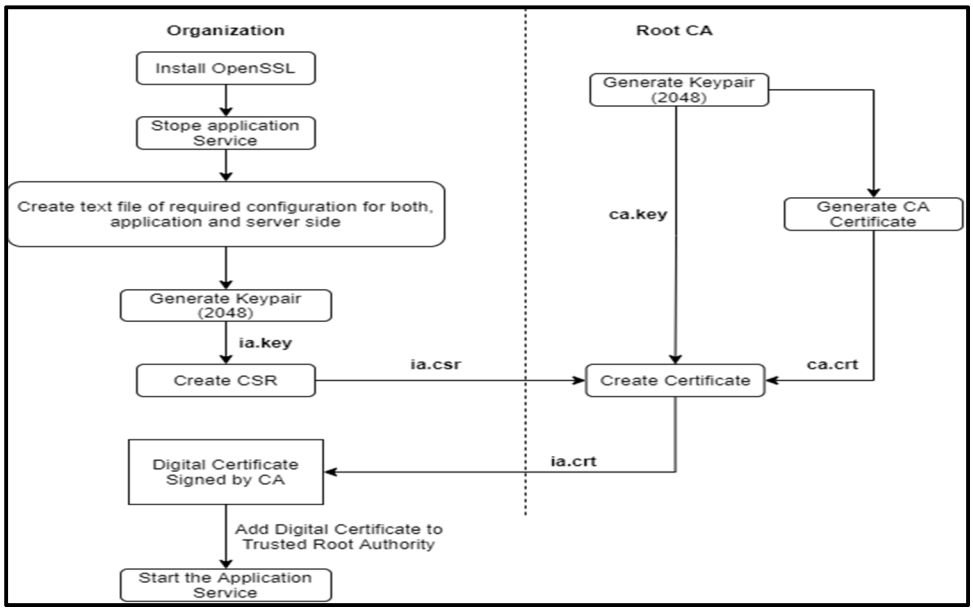


Figure 4. HTTP's Conversion Steps

2) *Policy Analyzer Scan:* Policy Analyzer is a flimsy independent application. This application doesn't need installation, and doesn't need authoritative rights (aside from the "local policy" feature). Strategy Analyzer is an efficacy for investigating and contrasting arrangements of Group Policy Objects (GPOs). This would feature when a bunch of Group Policies have repetitive settings or interior irregularities, and also can feature the contrasts among variants or sets of Group Policies.

This would likewise think about GPOs at odds with current local policy settings and in opposition of local registry settings.

Steps for performing Policy Analyzer Scan –

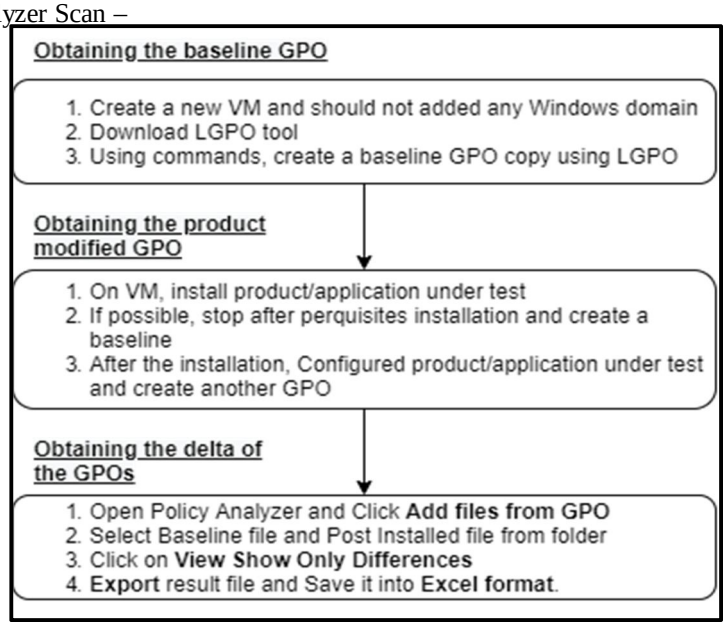


Figure 5. Policy Analyzer Scan Steps

3) ZAP Scan: OWSAP Dependency-Check is a utility that distinguishes project dependencies and checks if there are any known, openly revealed, vulnerabilities. Dependency check will scan the product binaries to figure out the dependencies and then compare it with its database to flag any components that may have publicly disclosed vulnerability.

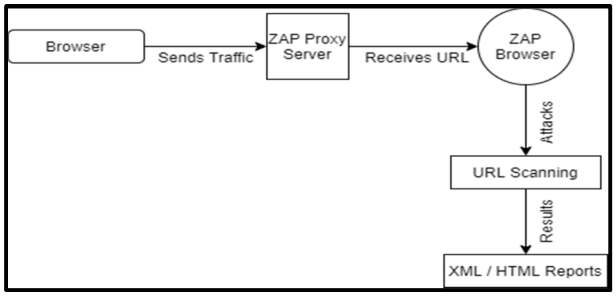


Figure 6. ZAP Scan (7.2.2)

4) Nessus Scan: The Nessus security scanner is a software, which will review a given arrange and decide the hosts that are on the organization and the conventions, administrations and programming running at the hosts.

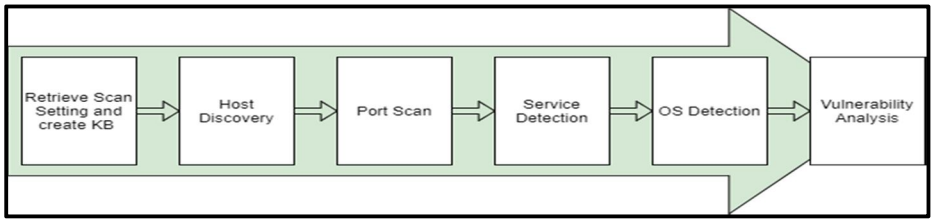


Figure 7. Nessus Scan Sequence (7.2.3)

Understand the Nessus Scan sequence is important because Nessus can only function vulnerability tests that are correct for the OS and the services running on the target.

5) Nmap Scan: Nmap ("Network Mapper") is a free and open source (license) efficacy for network disclosure and security reviewing. Many devices and organization directors likewise think that it's convenient for task, for example, network directory, handles service upgrade schedules, and supervises host or services up time.

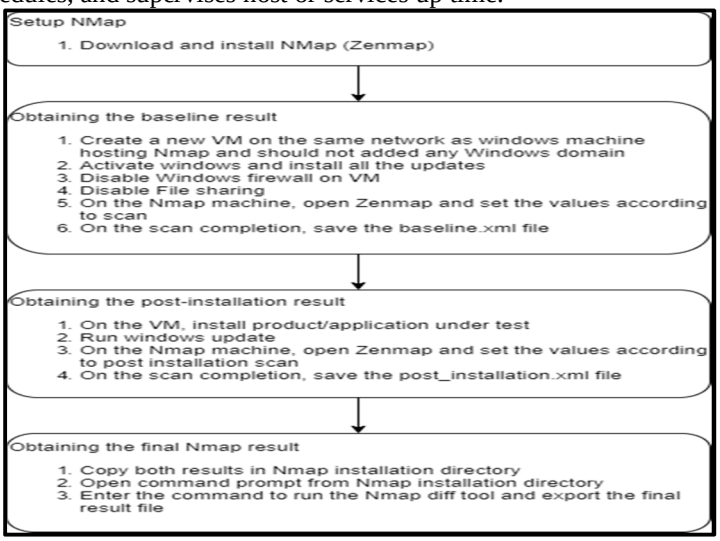


Figure 7. NMap Scan Sequence

Always host run Nmap scans on a private network since Nmap scans can create a lot of network traffic and will be pick up by IDS devices on Network.

6) *Attack Surface Analyzer:* Attack Surface Analyzer takes a depiction of the framework state before and after installation of product(s) and presents the progress of various key components of the Windows attack surface.

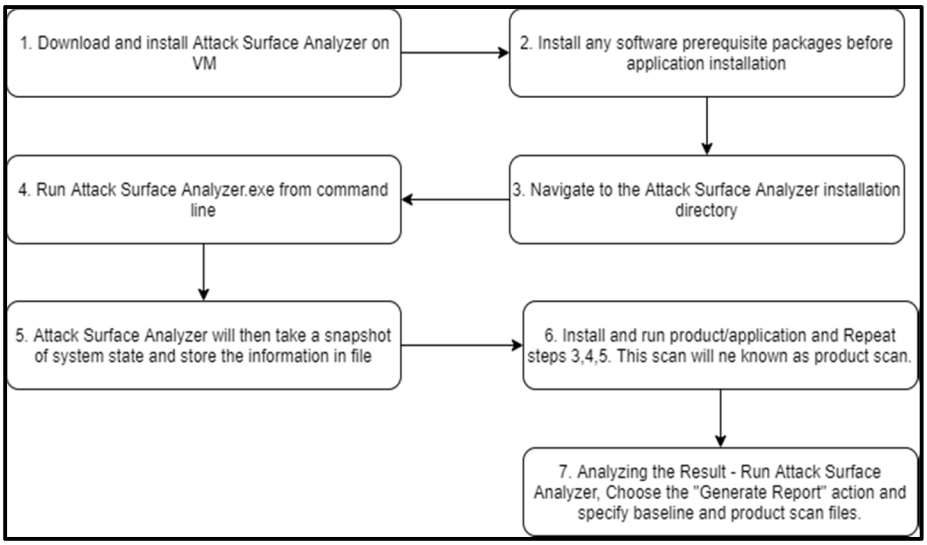


Figure 8. Attack Surface Analyzer Scan Steps

7) *Sig Check:* To verify which binaries actually signed in our product, we use Microsoft Sysinternal's SigCheck tool. Authenticode applies digital signature innovation to ensure the origin and uprightness of binary data such as installable software. A customer internet browser, or other framework parts, can utilize the authentic ode marks to check the accuracy of the information when the software downloaded or introduced. When we sign a binary, we can optionally timestamp the binary. Timestamping helps to validate when the binary actually signed. In addition, it extends the validity of the digital signature on the binary. I.e., by default, the digital signature is valid only until the signing certificate is valid. However, the validity of a timestamped binary's digital signature is until the validity of the root certificate that countersigned the signing certificate.

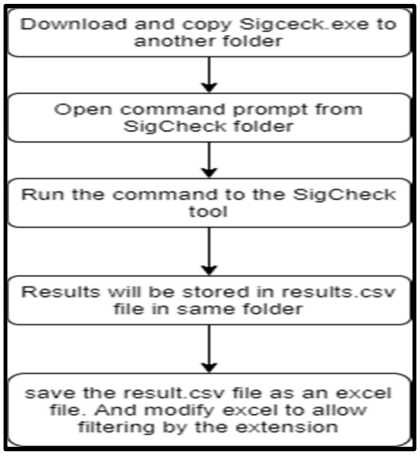


Figure 9. SigCheck Testing Steps

8) *Antivirus Scan:* Virus scans search through your framework to find and eliminate any malicious threats on your system. It discovers most antivirus software prepares for malware. This can incorporate threats like viruses and worms, just as, spyware, trojans, ransomware, and adware.

Steps to run Antivirus Scan –

a) Select the application folder
b) Right click on that folder and hit on "Scan for threat" tab
c) Save the file after scanning and check the logs if any virus is present

IV. RESULTS AND DISCUSSION

In this study, we are expecting the proposed system to complete the calibration process in minimal time when compared with traditional calibration process.

In addition, the proposed system is expected to give more efficiency with low cost. Furthermore, this software expected to reduce the labor work and paper-based calibration procedure. In addition, the result obtained are expected to give more accurate and specific for the devices/instruments.

Sr. No.	Name	Result
1	HTTPs conversion	- Improved application security - Improved search engine ranking
2	Policy Analyzer Scan	- Get overall security policies by comparing with baseline
3	ZAP Scan	- Get overall application vulnerabilities - Scan dependency of application
4	Nessus Scan	- Discovers vulnerabilities in system (software/hardware) - Shows what port and listening services are open
5	NMAP Scan	- Highlight pre and post installation changes as a various category
6	Attack Surface Analyzer Scan	- Identify test coverage of application - Identify the vulnerable code pieces - Threat identification and assessment
7	SigCheck	- Specify the binaries which are signed in application before production
8	Antivirus Scan	- Monitor the system - Create log reports - Attempt to repair any damage (if possible)

Table 1. Security Testing Results

V. CONCLUSION AND FUTURE WORK

Calibration management has always been great challenge to industrialist /proprietors /stakeholders. In this study, closely analyzed and evaluated a traditional asset management system, which provided valuable insights by which customer can add new features, functionalities to current calibration system. Also, proposing a portable, flexible, easy to use web-based application for management of assets, automatic calibration scheduling and workload management. Various tools and techniques have used to ensure security of data and system. Which are Zenmap, OWSAP, SigCheck, Nessus, and OpenSSL. By using these tools, we are now surer that users' data is safe and there is minimal chance of data theft. The next phase of this work consists of newly generated requirements by customers, which need to be fix. Also, have to analyze and evaluate accuracy and performance of proposed system.

REFERENCES

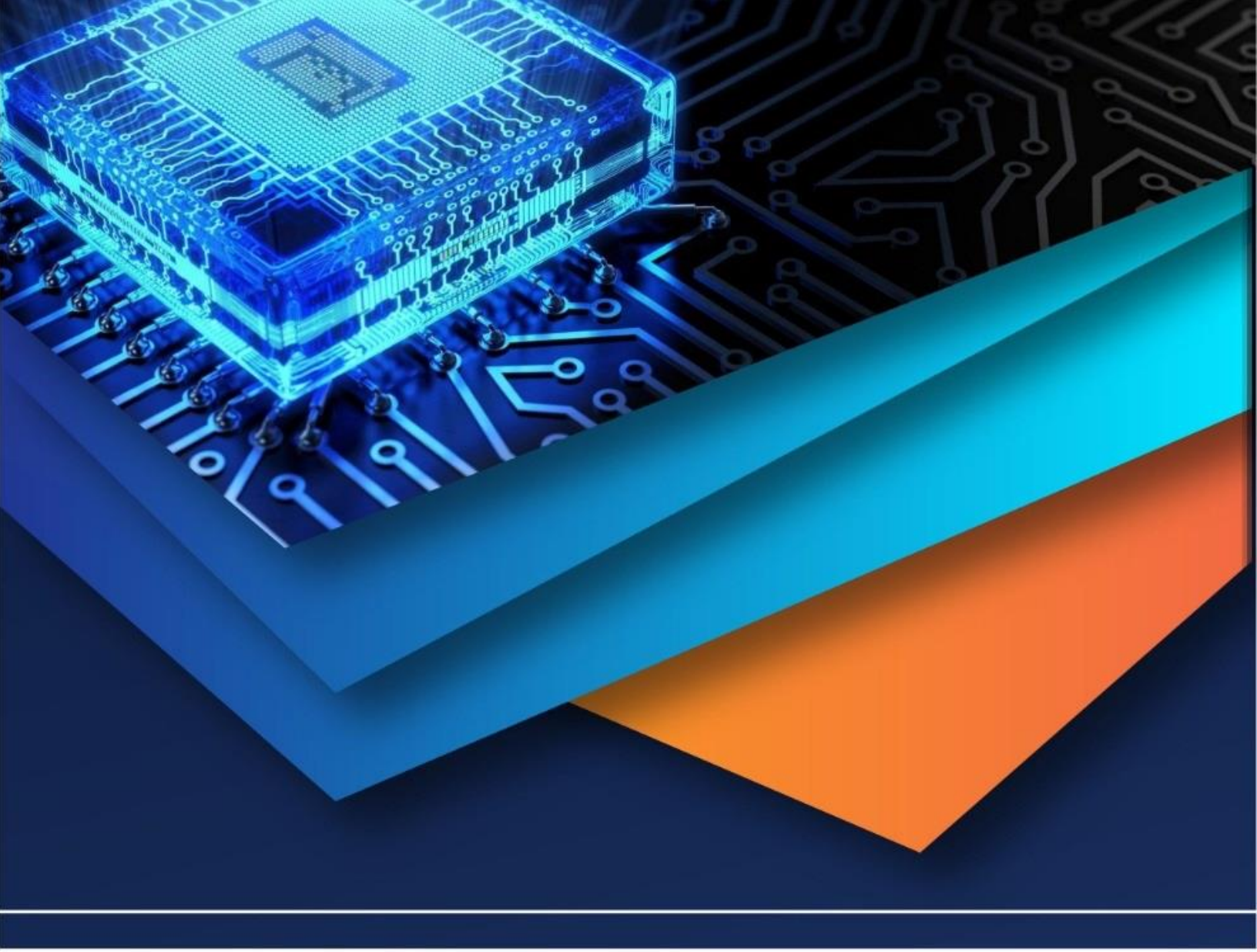
Journal Article

[1] M. Orzylowski, M. Hering, T. Kaluzniacki, W. Lobodzinski, P. Ostrowski and J. Wiechowski, "Automated calibration of temperature sensors," Proceedings of the 17th IEEE Instrumentation and Measurement Technology Conference [Cat. No. 00CH37066], Baltimore, MD, USA, 2000, pp. 285-289 vol.1, doi: 10.1109/IMTC.2000.846869.

[2] Bkjdv M. Orzylowski, T. Kaluzniacki, Z. Rudolf and G. Nowicki, "Precise temperature control for measurement purposes," IMTC/99. Proceedings of the 16th IEEE Instrumentation and Measurement Technology Conference (Cat. No.99CH36309), Venice, 1999, pp. 16-21 vol.1, doi: 10.1109/IMTC.1999.776712.

Websites

[1] baker-hughes-calibration-unified
[2] owasp-zed-attack-proxy
[3] a-brief-introduction-to-the-nessus-vulnerability-scanner
[4] Calibration
[5] Asset_management



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY