World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 7.029

CYBER SECURITY TEST PLATFORM ESTABLISHMENTS AND CYBERATTACKS PRACTICE

***Dr. Chetanpal Singh, Ass Professor Rahul Thakkar, Jatinder Warraich, Numan Ahmed and Vimal B. Patel**

India.

Article Received on 01/03/2024 **Article Revised on 21/03/2024** **Article Accepted on 11/04/2024**

***Corresponding Author**
Dr. Chetanpal Singh
India.

ABSTRACT

In this study, cyber security test platform aims to evaluate the vulnerabilities, of cyber-attack exercises to review cyber security challenges. In the introduction section, brief overview of the research context has been provided by developing research questions, and determining the problem statements. In the Literature review section, different articles will be analyzed for gathering better information about the research questions. Secondary research methodology will be utilized in this research paper, and brief explanation of chosen research methodology has been mentioned in the third section. The main purpose of this research paper is to conduct a proper platform, which can detect cyber-attack, and decrease the attack numbers. This paper will provide several improvement of the proposed platform for developing the scalability.

Index Terms: *Cyber exercise, test platform, cyber-physical system, security applications.*

INTRODUCTION

1.1 RESEARCH BACKGROUND

A cyber security platform is basically a key solution that has been used to secure and control an organisation's data and network systems. The cyber security testing platform is a privileged access and security audit system that is performed to identify vulnerabilities, weakness, as well as misconfigurations of the targeted hosts.[1] In this modern digitised era, for every organisation, cybersecurity is an important area that helps to provide safeguards from all types of possible cybersecurity risks. Effective cyber security measurements help the

organisation to reduce the possibilities of successful attacks as well as minimise the damages that a cyberattack can cause. In every organisation, the importance of several cybersecurity practices is more relevant, and the possibility of a data breach is reduced through the implementation of the measurements of security practices that utilise effective authentication mechanisms.[1] The chances of cybersecurity risks increase because of too much involvement in the latest technologies.

This research study will help the researchers to know the importance of the establishment of cyber security test platforms against any kinds of important information leakages, software & hardware damages, data thefts, as well as interruption of various services. The capability to understand and evaluate the threat data assists in reducing any damage as well as realising the flaws.[2] The internet system is completed in the company of priceless information as well as technical facilities which have eased the individuals with so much malicious information. The quality of the data can degenerate unintentionally with the assistance of data integrity tasks. Moreover, cyber security proposes a process to protect the entire information system of a company that is connected through modern internet systems. There are so many solutions for cyber security tests, and those are network security, mobile security, data security, application security, operational security, identity management, database and infrastructure security.[2] The two important tools that are used to do the security testing tools are "*static application security testing*" (SAST) along with "*dynamic application security testing*" (DAST). This research work will help the researcher to continue the research to highlight all the essential areas of the research work.

As the number of cybercrimes is increasing day by day, cyber security test platforms ensure the community continuously depends on their activities and services. The main goal behind cyber security testing is to point out the threats within the system and calculate the effective vulnerabilities in which way all the dangers can be easily encountered and where the system pauses its functions.[3] In this research, both the readers and the future researchers, after reviewing this research paper, can easily come to know the reason for which cyber security test platforms are arranged in most organisations or firms. In this process, various machine learning algorithms are used to maintain the validity, reliability, and generalizability of the organisation's information security system. Security testing proposes a software testing form that has been performed to analyse the entire system against any security-based expectations.[3] The purpose behind continuing this research is to make applications

impenetrable to the possible security threats in the vicinity of identifying both vulnerabilities and weaknesses of the security systems. The security system is basically used for the identification of potential vulnerable threats and the measurements of the overall security systems. After continuing the research work, the researcher needs to be controlled to continue the research in the insight of the general risks of facing the software. The actionable insight from these proposed topics is used to complete the security risks and gaps.

1.2 Problem statement

This research work is conducted based on highlighting the importance of the threats as well as measurements of the effective vulnerabilities that encountered the threats and issues faced in the information system. This research work will help to identify the vulnerabilities which are actively used within the organisation that used to lead an entirely insured security-based incident. As nowadays cyber crimes are rapidly increasing, the in-depth reason behind the importance of the establishment of cyber security test platforms and cyber security practices is needed, which will help the future researcher to carry on future research on numerous important areas.

1.3 RESEARCH AIMS AND OBJECTIVES

Aim

This research study is continued with the aim of continuing the research work to highlight the importance of cyber security test platforms establishments along with cyberattack performances.

Objectives

This research work will be conducted focusing on the following objectives and those objectives are,

- To point out the roles and responsibilities of cyber security test platforms as well as various cyberattack practices
- To identify the required tools that are used as effective cybersecurity software tools for maintaining information security
- To discover the current trends of the latest cybersecurity best activities, measurements, and techniques to strengthen the information security system of a company
- To identify the issues that can be solved through cyber security test platforms and cyberattack practices

1.4 Research questions

RQ1. What are the roles and importance of the establishment of cyber security platforms and cyberattack practices to ensure an effective information system?

RQ2. What are the current trends of the latest cybersecurity best activities, measurements, and techniques to strengthen the information security system?

RQ3. What are the issues that can be solved through cyber security test platforms and cyberattack practices?

RQ4. What are the required tools which are used as effective cybersecurity software tools for maintaining information security?

1.5 Research Significance

The security advisories issued every year by the ICS-CERT ('*Industrial Control System-Computer Emergency Response Team*') are rapidly increasing. So the significance of this research work is to highlight the important areas and tools that are used for the establishment of cyber security test platforms and various cyber attack practices to ensure organisational activities.[4] As nowadays almost all organisations become aware of their data securities, it should be necessary to continue the entire research work by detecting and understanding both security vulnerabilities as well as weaknesses in various source codes.

LITERATURE REVIEW

Significance of Cyber security and testing platforms

Businesses across all sectors have been experiencing an increase in threats in the platforms of cybersecurity for the last few years. In 2022, most numbers of cybersecurity companies have seen the highest development in cyber attacks. According to,[8] more than half of business companies in the country have reported breaches in cybersecurity in one year. Today, business companies can only conduct business with the involvement of hackers. The nature of attacks on cyber platforms has changed drastically in a few years, the percentage of malware practices has decreased, and phishing numbers increased to more than 85%. Business organisations across the globe have tried to implement cyber security to protect computers, mobile phones, servers and networks from malicious intent attacks. It is essential to implement protective measures to protect the systems and important information of the business. After the application of GDPR, it is important to cover the personal data of the companies and their employees. Some components of cyber security have been designed to strike the cyber attackers early, although cybersecurity professionals today are keen on

defending the assets of the companies at first. It has been utilised as the process to protect everyone from cybercrime, and it can provide help from finding theft to identifying threats at the international level.

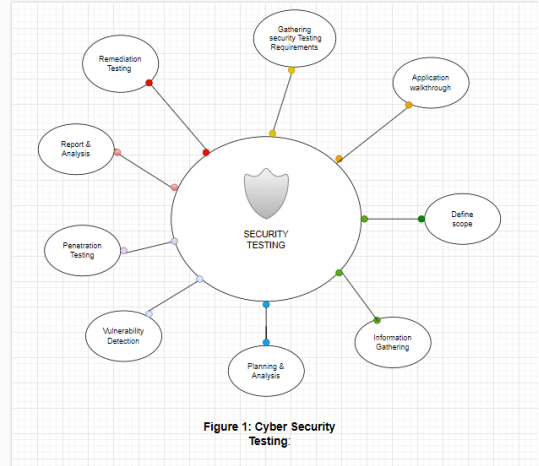

Figure 1: Cyber Security Testing

Source[9]

As per the opinion of,[9] a breach in the security of the servers can expose the personal and essential information of companies across the wo; It is considered a serious issue and has a strong impact on the financial conditions of the companies. Cybersecurity is very much essential to protect the business operations of companies in the time of globalisation and digital technology. It encompasses several technologies and approaches to protect servers, official and personal data, and computer systems from various cyber-attackers. There are some subdomains of cybersecurity, such as application security, cloud security, Data security, mobile security and Network security. As per,[10] application security helps the server to implement defences that are different and put them into the software of the organisation to protect the server from a range of threats. To implement this application successfully, it needs a cybersecurity expert to assess secure code, design the application securely and apply full information to reduce the rate of unauthorised access to the server. Cloud security helps companies to secure their servers by creating an architecture of the cloud; several service providers of cloud systems utilise this application, such as AWS, Google and Azure. The subdomain of data security helps companies to maintain authentication protocols that can be two or multi-factor. Mobile security is considered essential to the new generation, and this security application protects personal and official information gathered on the mobile device and guides them from unauthorised access, loss of device and virus attacks.

Three recognised examples of cybercrime are crimes that are assisted by the puters, when hackers get into the system of a computer and where computers are used incidentally. There are several kinds of cyber threats; Malware attacks, trojan attacks, cyber-terrorism, SQL injection, Phishing and Service denial. Companies need to use some essential software testing to prevent these cyber attacks; penetration testing, security testing, usability testing, configuration testing, SAAS and fuzzing are considered significant testing software that can prevent cyberattacks.

According to.[11] the system of penetration testing is usually considered a pre-planned attack against the infrastructure of Information and technology, website and applications of several companies. It is essential to provide real-time experience to the business management employees and the hackers' working process tools. Security testing is also necessary for every stage of the software development process, and it helps to contain security vulnerabilities and high turnover rates. Usability testing is also essential at the time of developing products of the company, such as new websites and applications of mobile devices of IoT. It helps gain more customer base as they can understand the effects and efficiency. A business server must not be hacked at the time of conducting business, and the application of cloud computing, such as SAAS and IAAS, is important to the company as it is an advanced technology. Companies use advanced and late applications of this cloud computing software to ignore vulnerabilities. By utilising software testing in cyber security, business organisations can develop more secure systems, and it is essential to prevent online threats.

Essentiality of cyber security test platforms and cyber attack practice to prevent cyber attacks

Penetration testing forms are considered to be an essential part of assessing the risk of security for all businesses, rectifying the clear defects and eliminating the subtle susceptibility from the perspective of hackers. Besides this, the cyber attacks practice is considered to be practice to defend the servers, computers, electronic systems, data and networks from malicious attacks. Here from the opinion of the researchers[12], a lot of research effort has been conducted to develop the cyber-security of the smart grids by utilising various kinds of techniques. The current power systems consist of the generations and sensors that give permission to two-way communication with the infrastructure of the system with reliable energy production via the combination of "Distributed Energy Resources (DERs)" and "Advanced Metering Infrastructure (AMI)". This complicated communication

system bears major benefits; by developing reliability, manageability and energy efficiency, it creates the vulnerabilities of the system to cyber attacks for the huge numbers of access points and devices that do its operation outside the administrative domain considered to be traditional. Since the power grid can lead to disastrous events, it is optional to research the effects or consequences of cyber attacks on the power system.

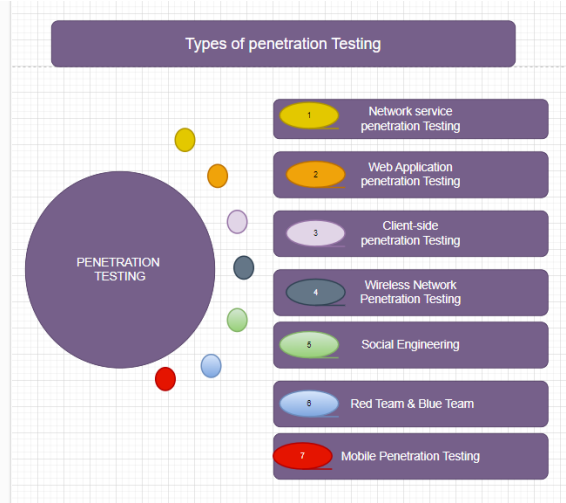

Figure 2: Penetration Testing

Source:[13]

From the opinion of some authors,[13] in North American blackouts, the lack of system awareness is considered to be the main reason behind the blackouts, which highlights the essentiality of the analysis of cyber-attacks in terms of maintaining a reliable and stable power supply operation. The cyber attack could damage or destroy the equipment or request false demands that might result in a huge rate of energy generated. Additionally, the spiteful attack also bears the dangerous capability of causing false negatives or a condition that is a wrong overload in the power system. Another disruption is also running the potential conduction in the various parts of the smart grid and electric vehicle infrastructure. Spiteful attacks can stop the services in the substation computers by obstructing communications with the device. The real-time detection of cyber attacks is supreme for the authentic performance of the vital infrastructure involving smart grids. Constant and online system observation is needed to detect the cyber attacks that have been targeted to see and gain attack pliability. The individual sensors in a wide-scale network are considered to be the primary target of security understanding. It is possible for the compromised insider to access the data stored easily in a compromised confluence. In theory, the key cancellation of the compromised node is possible by the application of a proper or authentic mechanism to the sensor network.

However, the approach of authentication on the basis of security gateway structure or cryptography could be more practical for the storage constraints and computation of the system.

According to the opinion of another researcher,[14] it is optimised that the techniques of advanced anomaly detection and security control theories on the basis of various methods of state estimation are very capable of immunising the power system where the major part of this is physically impractical, mathematically expensive and unscalable for the network which is complicated in a large-scale. In the present day, a large amount of information is produced on all of the grids that develop the entrance ability for the monitoring of the real-time system. The historical information describes the operation of the system that bears the capability to rectify the possible and anomalies attacks. Although the traditional techniques of "Bad Data Detection (BDD)" are not ready for the purpose of real-time computation, and the difficulties related to storing the great volume of the information generated in the smart grid. Such kind of difficulties enlarges the potentiality of the utilisation of techniques of data analysis, like ML, in terms of handling the data set that is structured in a complicated way with Artificial Intelligence in terms of preventing and detecting cyber attacks. Here from the opinion of other researchers,[15] ML algorithms are possible to use in evaluating different types of measurement combinations via states, AMI and control actions by understanding their structures of them, where they can detect the "False Data Injection (FDI)" attack by understanding the non-linear and complicated connection among the measurements. Several ML algorithms are compared and tested for the matter of detecting the FDI attacks, where machine learning has got success in classifying the attacks related to FDI. A method of hybrid intrusion detection has been suggested on the basis of a process of common path miming in terms of detecting the unusual power system events from the PMU relays, information and energy management system logs. Additionally, the techniques of cyber attack detection on the basis of a correlation between the two parameters of PMU utilising the Pearson correlation coefficient have also been suggested. Such methods evaluated the transformation of correlation between the two parameters using the Pearson correlation coefficient.

Present trends of the modern cyber security activities, measurements and techniques

Automation has developed its essentiality in the matter of cyber security. The Automated procedures of security bear the capability to decrease the time that it has taken to give a

response and detect threats and develop the exactness to detect threats. Automation has also reduced the dependency on manual procedures that can be prone to human error and time-consuming. Here according to,[16] in the present day, the Fourth Industrial Revolution is famous as 4.0, which visualises the rapid change in industries, procedures, social patterns and technology as an outcome of developed smart automation and interconnectivity. This type of revolution has influenced most industries all over the world and caused an enormous transformation in a manner that is non-linear at an unrivalled rate, with the inference for all the economies, industries and disciplines. Industry 4.0 has been described as a term that is utilised to define the current trend of the industrial exchange of data and technology automation, which involves the Internet of Things, cognitive computing and cyber-physical systems with the improvement of the smart factory. The start of the digital revolution to Industry 4.0 has taken place with data gathering, obeyed by the AI in terms of interpreting the information. So, the "intelligence revolution" is able to be considered in the matter of servicing and computing, as AI has reshaped the world that includes intelligence and human behaviour into systems or machines.

From the opinion of,[17] in the present days, machine learning modelling has been applied in a practical way, especially in the matter of cyber security.

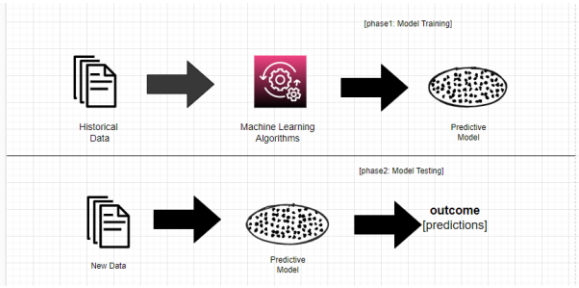

Figure 3: General structure of the ML-based predictive model considering both the training and testing phase.

Source[17]

For instance, the application of the ML strategy in order to get the covid 19 assistance to the people who actually need it. Several cyber-attacks and anomalies have the chance in terms of being detected by utilising the approaches of machine learning in the part of cyber security. Additionally, the strategy based on ML has the ability to improve an effective smart parking system for the environments of smart cities. Besides this, AI is considered the buzzword as it has prepared to influence businesses of all sizes and shapes in all industries. The AI of the

sector can develop the available services or products to make all these more safe, reliable and effective.

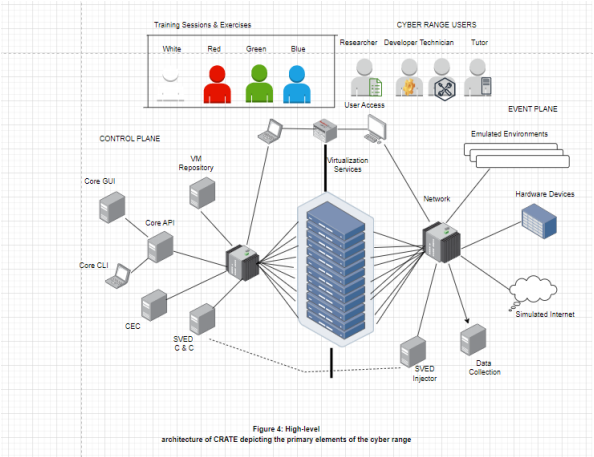

Figure 4: High-level architecture of CRATE depicting the primary elements of the cyber range.

Source[18]

The above figure shows a high level of CARTE's architecture, with the servers considered to be visualisation that abode the imitated environments in the centre part. On the left side, the control plane is used to manage the cyber range, and on the right side, the event plane is utilised for the system where the execution of the experiments or research and training is conducted. The plane planes are depicted as two zones of security, which are separated from one another, which is important in terms of ensuring that the execution of the events in the event plan has not affected the control plane.

The server for virtualisation gives abode to the virtual machine utilised in the imitated environment. Currently, there are approximately 500 virtualisation servers existing in CARTE, where the virtualisation servers generally operate a customised, tiny operating system on the basis of Linux that is renowned by the name CarteOS. In order to facilitate the maintenance of cyber range and ensure the honour of the servers, CarteOS operate in a read-only domain and cover the file systems that are utilised in storing the configuration and virtual machine. This has enabled the server's operating system to be replaced without impacting or affecting the organised virtual machine or its composition, permitting CarteOS to be upgraded as the latest software versions and updates regarding security become available.

Cyber security testing tools and their usage

Since the beginning of 2020, organisations across the world have been facing several cybersecurity problems. Ransomware attack rates have increased by more than 140% after the pandemic. Companies have hired many cybersecurity analysts in business management to assess security-related issues, and they are responsible for reporting any security breaches and evaluating the servers' weaknesses of the respective companies. Several types of cyber security tools have been used to find any vulnerabilities in the web applications and servers of the companies. According to,[19] cyber security tools can enhance the possibility of identifying threats to servers. Some important cyber security testing tools are;

Burp Suite is a well-known software, and it is considered one of the best toolboxes that can provide testing of web security. The application of this tool is designed to use by click with a point process. It is a graphical tool, and it works to conduct security testing on any online application. The application of this tool helps the entire process of testing from the mapping of the initials, and it can analyse the attack surface of an application by discovering any flaws of security in the application. It is a security solution for web applications, and it helps companies to test any vulnerability manually, and it also helps to Intercept messages of HTTP. Burp Suite is used to conduct several activities, such as trying a web application, web crawling and web application analysis. This tool can be built into the browser of Chrome.

Vega is a web security scanner and a web security testing platform, and it helps to test web application securities. The application of Vega helps to identify any SQL injection and also other vulnerabilities in the server of any company. It helps to find cross-site scripting which can be reflected or stored. As per,[20] The application of Vega provides TLS security settings and sees all the possible opportunities to enhance the security of the TLS servers. It has an automated scanner that helps to test the servers quickly and can intercept proxy servers at the time of tactical inspection. This application can be updated by utilising the application of artificial intelligence in the javascript language.

OpenVas software is a vulnerability scanner, and it can be helpful in conducting unauthenticated testing and authenticated testing of several industrial protocols. According to[21] It also can help to improve the tuning of performance at the time of scanning large scales and provide the language of internal programming to conduct vulnerability of any type. This application has been used for many years and is a process that can find any vulnerabilities in the servers. It classifies the system resources and allocates all the

enumerable values. Then it detects all the probable threats and reduces the vulnerabilities by giving proper priorities.

The intruder is an essential vulnerability scanner to prevent the issues of cyber security and identify any weaknesses in the system servers. This tool helps to save time as it proactively scans any new threats in the server and offers an interpretation system to identify all the unique threats. This tool's main positive aspect is the support staff's quality. It has a chat app that can ease various quotations, and the device has the comprehensiveness of all the outputs. It helps to identify all the vulnerabilities, and it takes several actions to fix them.

According to,[22] Zed Attack proxy is a great tool for analysing static code, and cybersecurity companies have used it to detect all the security problems in principle; it helps to fix the issues of vulnerability. This tool can highlight several suspicious codes that have developed in the server system, and it provides feedback on security during the review of the code. It also can identify several technical debts and fix the vulnerabilities in the application in the code. It can detect bugs faster and give feedback to the developers to enhance the quality of the code.

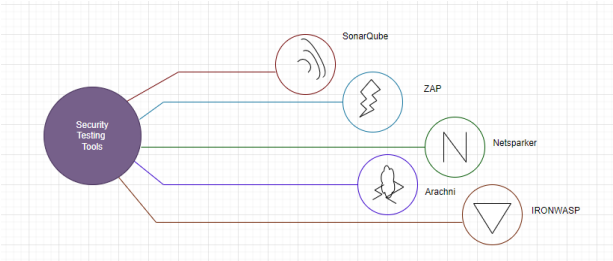

Figure 5: Security Testing Tools

Source[22]

RESEARCH METHODOLOGY

Research Overview

Research methodology basically follows the measurements of the research processes, and it perfectly channels both the identification and completion of possible important areas which have been considered in the proposed research topic. The methodology of this research work has been discussed here by the researchers to implement specific data and continue the flow of narration of this research. The researcher has continued this research by following proper research philosophy, research approach, research design, data collection processes, and data analysis process.[23] Different techniques and tools that are used in this research are also

proposed in this methodology section. The researcher in this research follows "*the positivism research philosophy*", "*the deductive research approach*", "*the descriptive research design*", "*the secondary data collection processes*", and "*the qualitative data analysis processes*" to continue the research work. So, the research project is completely organised through sequential processes that are defined on behalf of the scope of the project, research method, and analysis of all the collected data.

RESEARCH METHODS

The method in this research work has been followed in the vicinity of the ***mixed research method*** because both primary as well as secondary data have been used to carry on the research work. All the information that has been collected is the secondary qualitative data. This secondary methodology has helped the researchers to accumulate, classify, and evaluate all the published articles which will be available from various internet resources and libraries. The secondary research proposes certain questions as well as focuses on some hypotheses.[23] This research topic is based on the establishment of cyber security test platforms and cyberattack practices, which perform with the assistance of internet connectivity. The secondary research work relates to internet connectivity, and the data analysis process points out the critical viewpoints used in security implementation measurements. The entire research method highlights the specific orientation of the current research issues.

Research Philosophy

The researcher in this research work follows the *"**positivism research philosophy***" are not, and it will propose a clear, brief, and concise discussion that does not use any kinds of descriptive stories. Any interpretation is not allowed because of its value-free nature. Some common theories and basic concepts are applied based on the research objects. Nowadays, cyber security attacks are increasing day by day, and it covers a range of situations within very short periods. The main concept for which the researcher carries on their knowledge consists of genuine decisions.[23] The key feature of this positivist research philosophy is to use clear, brief, and concise discussion, which does not utilise any descriptive stories. It dismisses an individual's importance which proposes subjective values and experiences. Finally, positivist research philosophy ensures that researchers make perfect predictions based on both social and society-based changes. Positivism basically holds the idea that empiricists observe natural processes. The basic characteristics of positivism are to propose valid knowledge and identify the facts of the collected information. So the strength of this

positivist research philosophy is to be a pioneer in the first scientific study of the proposed topic.

RESEARCH APPROACH

*The "**deductive research approach***" has been used to highlight the procedures that the researcher selects to analyse, collect, as well as interpret the data. It helps the researchers to determine the success behind the research work and maintain the overall standards of the research. This research approach has been used to support the researchers to remain confirmed about the existing theories. The deductive research approach proposes the possibility of delineating casual relationships in the middle of variables and concepts. In the case of qualitative research work, the researcher applies the theory with a "*top-down approach*" for analysing the collected data. It basically helps to continue the research works from general to more specific.[24] The benefit of this kind of deductive approach is to explain the variables and concepts which are interrelated with both causes and effects of the research. It also helps to measure both concepts and ideas of the research work that are possibly reached to a broader extent.

Research design

Research design is basically the blueprint of the entire research process. The researcher in this research study follows the "***descriptive research design***" to point out and address all the possible issues which may arise during the research and data analysis processes. The proposed research design is basically a type of research design that focuses on obtaining any systematic information to describe a situation, phenomenon, or population. This descriptive research design provides permission to the researchers to explain and learn the value of more variables in the absence of any casual and valuable hypotheses. The researcher proposes this research design with the aim of systematically and accurately explaining the situation of the current research work,[24] The main purpose behind this research work is to define, describe, and validate the findings of the research works, which helps both the researchers and future readers of this research work to obtain a focused description of the current phenomena along with proper analysis and interpretation of the research findings.

RESEARCH DATA COLLECTION

For this research study, the ***mixed research approach*** has been utilised, and for that reason, both primary and secondary data have been employed. The main research has yet to be evaluated as the essential part of obtaining innovative data; rather, the narration has been

followed via a secondary literature review, and primary data will be analysing those extracted parts. For gathering secondary data, articles have been chosen from various secondary resources, concluding ***IEEE Xplore***, ***google scholar***, and with this other internet resources. Research topic-based suitable keywords have been used so that it can be easy to obtain relevant information and provide proper justification based on the cyber security-based platform development.[25] The utilised keywords have been chosen, such as ***cyber-attack***, ***platform***, ***cyber threats*** and so on. The articles published before 2019 have yet to be considered relevant for this research process. As technological innovations are constantly developing, due to that reason, to provide current information, it is important to obtain current data also. The citation index of every research article was measured properly to ensure research credibility. The strategies for the primary research approach have been analysed by utilising different models that support the prevention of cyber attack activities. The main purpose of operating the secondary data collection process

Used tools and techniques

The model has been utilised in simulating the power grid utility in terms of tools and techniques. As the power system simulator, it will help in creating the simulation environment in constructing the models through flow cases of the power system. For the graphical user interface, the RSCAD can be used in developing the power system models with the help of a simulator. Within the submission level, these IEDs can communicate with the RTDS using digital inputs. Referring to the "IEC 61850 GOOSE protocols", the RTAC process can be found with SCADA measurements. This RTDS can also communicate with the control servers in compiling the DNP3 and IEC 61850 protocols.[30] This RTDS also can be interfaced along with the substation control while using the hardwired connections. Therefore the ethernet connection also has been used in managing the hardware or similar type of communication also.

RESEARCH DATA ANALYSIS

For a research process, the data analysis technique is an essential part that should be followed properly stepwise. The researcher follows a "*qualitative data analysis*" process to evaluate all the collected data. It has come to know that this type of research data analysis process In choosing the secondary data analysis process, the related testing results in terms of cyber security also have been compared. The main purpose of data visualisation is to depict the observation result properly through various graphs, charts, and with these other types of

visualisation tools. This ISSAC setup also delivers the SCADA network within the enterprise level along with the computing nodes [29]. Nevertheless, this ISAAC has been used in simulating organisational models consisting of CPS. Similarly, connectivity can also be made between branch campuses and research laboratories.

Comparison of 5 to 6 research papers

Citation	Title	Results
(Khandker *et al.*, 2021)	Cybersecurity Attacks on Software Logic and Error Handling Within ADS-B Implementations: Systematic Testing of Resilience and Countermeasures	In this research paper, the concern has been laid on detailing the test platform and attack along with the utilization and experimental set reflected in the result. In the process of experiments, 36 varied ADS-B. In combination with host, hardware and software. Even around 2107 test samples were accumulated, among them, 966 of which were actual aeroplanes while 11141 were spoofed aeroplanes of attackers. There was a clear evaluation of the high-power attacks that were much easier to detect. On the other hand, low-power ones were critical to being detected and even erroneously prone.
(Oyewumi *et al.*, 2019)	ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed	In the paper, the concern has been laid on utilizing the ISAAC's SCADA visualization, along with the cybersecurity abilities, to form the experimental results. The experiments manage the evaluation of the network information and incorporate accumulation packet stream via ISAACs interaction channel at a DoS attack. This experiment leads to the ML framework for data-related health monitoring. The result reflected the process of developing resilience and threat assessment of CPS, detecting stealth cyber attacks against state removal as well as application. In the process, a dignitary visible wall-mounted display has been implemented within the "Power lab-tested firm" while utilizing the "IRIG-B" synchronization" digital clock having SEL-3401. This tends to give time with an accuracy rate of around ±100ns. The result outlined the current use of ISAAC; when significantly integrated, ISAAC will form CPS research as well as the educational capability of the regions around Idaho. Idaho CPS Smart Grid Cybersecurity Testbed of surrounding

		that emulated the strength utility.
(Ramirez *et al*., 2023)	PLC Cybersecurity Test Platform Establishment and Cyberattack Practice †	The "PLC Cybersecurity Test Platform" has been analyzed in this research paper. In the test platform, different cybersecurity tools are utilized. "Personal computer running Kali 2022.3" as kernel operating system, which plays like an attacker, and with this ", a personal computer running Ubuntu 22.04" is utilized as the target device. The target device races***ModbusPal v1.6*** for stimulating Modbus communication. Modbus utilizes port 502 for communication, which can be a target for attack exploitation. To identify the Modbus register, Metaploit has the capability to provide requests on individual addresses. Metasploit utilization supports register modification in the chosen target.
(Kim *et al*., 2019)	Cyber-Physical Battlefield Platform for Large-Scale Cybersecurity Exercises	In this research paper, ***a cyber-physical battlefield*** (CPB) platform has been developed that can provide scalability in cybersecurity exercises. For developing the platform, it is essential to conduct an on-site visit to gain better information about the security threats, as well as the working phenomenon of the individual sectors. In operation, CPB can stimulate ICS/SCADA system. This platform's successful application within "Locked Shields 2018" (LS18) provides a shred of strong evidence.
(Munaiah *et al*., 2019)	Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition	For measuring attacker mindset, proper security software should be developed. In this research paper, a multimodal dataset has been chosen during "the 2018 National Collegiate Penetration Testing Competition" to understand the attacker's mind. ***MITRE ATT&CK*** framework is utilized to codify tactics, as well as techniques. Attackers applied various unregistered accesses to handle the user's account. Through the proposed framework, at first, it can be easy to identify ATT&CK's tactics for decreasing attack numbers.

Data validity and reliability

The procedure of the research has been related to the mixed approach to the performance of the study. The researched information has been separated into two kinds of efforts such as

primary and secondary. The secondary literature review was established on the basis of the journals of Google scholars. The researchers have healthily ignored the store of available data and intentional incorporation the data in terms of getting advantages about the research efforts. The dependency of the developed elements is possible to be justified by the efficiency of the considered datasets. The effectiveness of the model could be improved by nourishing a higher amount of information to the logical system within the model of the device. The utilisation of the classification logic has allowed a huge amount of data to actuate and streamline the model into the perfect procedures of detection.

Research Limitation

The procedure of the research has followed an approach of mixed methodology, where it collects its own limitations by gathering the previous hindrances and limitations underlined or highlighted in the articles that are already published. The restrictions or regulations of the secondary literature review are highlighted in the absence of the statistical establishment. The procedure of the ideological similarities to the articles that are published has been erased by the application and establishment of the primary research methodology. The strategy of the primary research has been lacking the statistical justifications steps to describe the efficacy of the model that has been developed, and the process of development and rectification of the types of threats from the dataset have been executed to give the development effort incremental success a justification.

RESULT AND COMPARISON

For testing the different kinds of cyber attacks, the ISAAC facilities have been found to develop the capacity by developing both realistic and practical CPS. Through the potential utilisation, the real-time simulation of cyber attacks has been determined through RADICAL. The different researching areas of modern networks and computing platforms have facilitated it. By delivering a contained and secure environment, it has been used for securing critical infrastructure and experimental analysis also. It has been used in conducting sophisticated cyber attacks by strengthening the necessary infrastructure. In terms of visualisation, the SCANVILLE has been used in delivering real-time data analyses through a total ISAAC testbed.[28] For emulating real-world enterprise, this SCANVILLE has been found as important for infrastructure utility. Therefore, this data visualisation can also be used for trend identification, monitoring the overall system and detecting real-time attacks. This can be assessed in regulating the violations by simulating threats and negative incidents along

with their happenings. ISSAC has been found in the delivery of realistic emulation environments in case of comparative validation and testing. Combined with the multiple CPS research approaches, it has been used in investigating vulnerabilities and assessing and exploiting their impact. Emulating the SCADA network has also been used in facilitating the experimental environment, which has been used within the cyber-defence training curriculum. Regarding remote utilisation, the ISAAC testbed can be used to expand the completed designs and plans across the State of Idaho. In connection with this, the OSI layer two can be referred to as the Tunneling protocol of the Idaho Regional Optical Network (IRON). Integrating the IRON and VLAN has helped enable the testing through the growth of the additional laboratories. In terms of CIA confidentiality, integrity and availability have been installed within the ISAAC network, which has played an important role against cyber attacks.

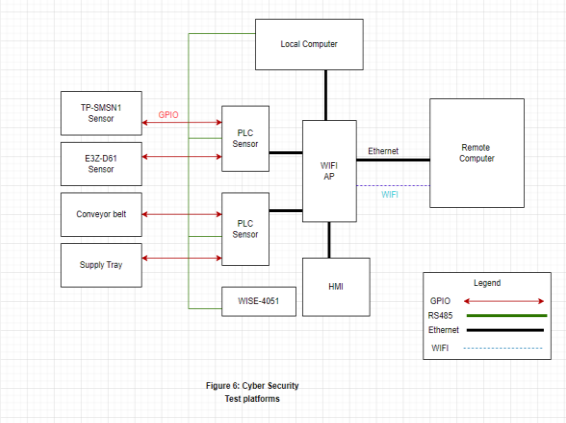

Figure 6: Cyber Security Test platforms.

Source[28]

This ISAAC network might also be classified into subtypes to create a digital-level defence. Both the De-Militarized and VLANs have been found to have stringent access control policies for developing performance and security. Hence each of the VLANs has been found to have explicitly- defined access control. Nevertheless, for delivering perimeter-level defence, the ISAAC firewalls also can be used to prevent direct ingress and egress connections between the external networks. In defending both infiltration and exfiltration, the configured control list can be shared.[26] Within the reverse proxy mode, the statistical engine features and web proxy can be refereed with restricted and controlled access. This web proxy can eliminate the risk of direct exposure of ISSAC to the internet. The IDS has been used for intrusion detection to integrate the Switched Port Analyzer and port monitoring. By using the

NIDS, an authorised network might be reviewed in revalidating the experimentation. In the case of node re-imagination, virtual machine endpoints and instances can be combined along with the operation system. Through maintaining the modified security updates, a web proxy server can be used within the infrastructure of PoT, SCANVILLE and RADICAL.

In contrast to this, there are multiple studies also have been found on the securing of the DAS- B security. Considering the different studies, this can be categorised between two kinds of studies: broadcast authentication and localization verification. The RF communication defences have been explored in measuring the effectiveness of the PLS techniques. Referring to the RSS- Distance model, the signal attenuates in travelling through space. To distinguish the real aircraft, the spoofing unit has been set up through random transmission of the fake "ADS-B 1090ES" signals by encoding the random positions. Letting the spoofing set up, the receiver has been found to receive both the real and spoofed calls. For a defined ADS- B massage, a setup also has been calculated in calculating the 3D distance between the receiver and the aircraft. In case the real-time RSS and retrieved RSS have been as close enough, then only the aircraft can be considered legitimate. Regarding this, the RFF has been found to suffer from both fluctuations and noise. According to the tolerance level, the attacks are found in using multiple power levels, which are medium power attacks, low power attacks and high power attacks.[27] For defending, the Doppler shift can be used in measuring the frequency wave motion between the receiver and transmitter.

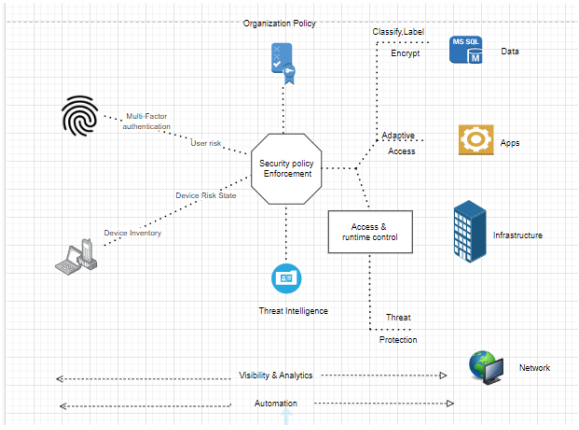

Figure 6: Cyber Security statistics.

Source[18]

Additionally, the Doppler shift can be added with an ADS-B signal for verification of the velocity along with the aircraft position. For the coordinated attack types, the ADS- B messages can be found with the bodies such as FAA, RTCA and ICAO. For making defences

against other types of attacks, effective software can be detected through data fluctuation. In implementing the developed logic for alerts, the above notification can occur through aerospace- arrived ways of handling and notifying of alerts. Configuring the signals can be displayed by displaying the threshold and delivering the sensible defaults.[7]

V. CONCLUSION

In the present day, most organisations are facing a lot of threats due to the dangerous effects of cyber attacks, where such threats have strengthened the potentiality of losing or misplacing vital and confidential organisational information. So, with a major focus on such difficulties, the paper has done its best to describe the importance of cyber security testing and practising cyber attacks. The purpose of the cyber security testing utilised several tactics and methodologies in order to measure the effectiveness of the cyber security strategy against the possible risk that can be faced by the security system of the systems. Here the paper has identified the vital vulnerabilities that have been utilised in the industry and organisation in an active way in terms of launching cyber attacks. The report has discussed the significance of the automation system, giving reference to ML, AI and other methods and techniques. ML is estimated to provide support in analysing and predicting dangerous activities like malware, phishing, authentication attacks, application attacks and so on; while considering this, several companies have improved their systems with the implications of machine learning. The integration of AI has the ability to attack the way to test cyber security attacks as a mandatory process to utilise the cyber security tools. As technology is becoming regularly updated, the establishment of AI-based cyber-attack platforms also needs to be periodically updated, and for this reason, more future work on this topic has been required to point out the roles and significance of future research works.

Besides this, the importance of AI in the current cyber security testing and cyber attack practice is small. AI in cyber security has erased the tasks that are meant to be time-consuming; here, by scanning information, rectifying the possible threats and decreasing the false positives to extract the non-threatening activities, AI technologies are supporting organisations. The paper has reflected the usage of AI and ML technologies in such a way that it has got evidence of the expertise of the technologies in terms of focusing on the more vital or critical tasks. However, the paper has found it quite difficult to fix the number of environments that will be run simultaneously due to its dependency on size and

organisational complexity to be emulated. So, in future research of the paper, this matter will get a concentration while researching and discussing the topic or study.

ACKNOWLEDGMENT

I would prefer to express my absolute gratitude towards my professor, for the valuable advice, supervision and guidance from early phase of this research. I am extremely grateful for attainment of the constant support throughout the research. I am additionally thankful to all the participants those contributed in several ways towards this research, also humbly acknowledge all contribution.

REFERENCES

1. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. Towards Insighting Cybersecurity for Healthcare domains: A comprehensive review of current practices and trends. *Cyber Security and Applications*, 2023; 100016.
2. Ahmadi, A., Nabipour, M., Taheri, S., Mohammadi-Ivatloo, B., & Vahidi Nasab, V. A new false data injection attack detection model for cyberattack resilient energy forecasting. *IEEE Transactions on Industrial Informatics*, 2022; *19*(1): 371-381.
3. Sun, C. C., Cardenas, D. J. S., Hahn, A., & Liu, C. C. Intrusion detection for cybersecurity of smart metres. *IEEE Transactions on Smart Grid*, 2020; *12*(1): 612-622.
4. Gasiba, T., Lechner, U., Pinto-Albuquerque, M., & Porwal, A. Cybersecurity awareness platform with a virtual coach and automated challenge assessment. In *Computer Security: ESORICS 2020 International Workshops, CyberICPS, SECPRE, and ADIoT, Guildford, UK, September 14–18, 2020, Revised Selected Papers*, 2020; *6*(67-83). Springer International Publishing.
5. Karagiannis, S., Maragkos-Bel Maps, E., & Magkos, E. An analysis and evaluation of open source capture the flag platforms as cybersecurity e-learning tools. In *Information Security Education. Information Security in Action: 13th IFIP WG 11.8 World Conference, WISE 13, Maribor, Slovenia, September 21–23, 2020, Proceedings 13* (pp. 61-77). Springer International Publishing, 2020.
6. Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., ... & Bellekens, X. A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, 2020; *20*(24): 7148.

7. Aldawood, H., & Skinner, G. (January). An academic review of current industrial and commercial cyber security social engineering solutions. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 2019; 110-115.
8. Hanif, Y., & Lallie, H. S. Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust. *Technology in Society*, 2021; *67*: 101693.
9. Renaud, K., & Ophoff, J. A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organisational Cybersecurity Journal: Practice, Process and People*, 2021; *1*(1): 24-46.
10. Muthuppalaniappan, M., & Stevenson, K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, 2021; *33*(1): 117.
11. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, 2021; *105*: 102248.
12. Karimipour, H., Dehghantanha, A., Parizi, R. M., Choo, K. K. R., & Leung, H. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*, 2019; *7*: 80778-80788.
13. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, 2021; *21*(15): 5119.
14. Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., ... & Bellekens, X. A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, 2020; *20*(24): 7148.
15. Awamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., & Al-Rawashdeh, G. Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology*, 2020; *63*(5): 7894-7899.
16. Stevens, T. Knowledge in the grey zone: AI and cybersecurity. *Digital War*, 2020; *1*: 164-170.
17. Sarker, I. H. Ai-based modelling: Techniques, applications and research issues towards automation, intelligent and smart systems. *SN Computer Science*, 2022; *3*(2): 158.
18. Gustafsson, T., & Almroth, J. (March). Cyber range automation overview with a case study of CRATE. In *Secure IT Systems: 25th Nordic Conference, NordSec 2020, Virtual*

Event, November 23–24, 2020, Proceedings (pp. 192-209). Cham: Springer International Publishing, 2021.

19. Thaqi, R., Vishi, K., & Rexha, B. Enhancing Burp Suite with Machine Learning Extension for Vulnerability Assessment of Web Applications. *Journal of Applied Security Research*, 2022; 1-19.
20. Altulaihan, E. A., Alismail, A., & Frikha, M. A Survey on Web Application Penetration Testing. *Electronics*, 2023; *12*(5): 1229.
21. Ardo, A. A., Bass, J. M., & Gaber, T. (2022, February). An empirical investigation of agile information systems development for cybersecurity. In *Information Systems: 18th European, Mediterranean, and Middle Eastern Conference, EMCIS, Virtual Event, 2021; 8–9, Proceedings* (pp. 567-581). Cham: Springer International Publishing.
22. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, 2021; *105*: 102248.
23. Newman, M., & Gough, D. Systematic reviews in educational research: Methodology, perspectives and application. *Systematic reviews in educational research: Methodology, perspectives and application*, 2020; 3-22.
24. Ryder, C., Mackean, T., Coombs, J., Williams, H., Hunter, K., Holland, A. J., & Ivers, R. Q. Indigenous research methodology–weaving a research interface. *International Journal of Social Research Methodology*, 2020; *23*(3): 255-267.
25. Hafidz, M. A., & Elihami, E. Learning The Nonformal Education Through Research Methodology: A Literature Review. *Jurnal Edukasi Nonformal*, 2021; *2*(1): 47-55.
26. Fowler, D.S., Bryans, J., Cheah, M., Wooderson, P. and Shaikh, S.A., July. A method for constructing automotive cybersecurity tests, a CAN fuzz testing example. In *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C).* 2019; 1-8.
27. Oyewumi, I.A., Jillepalli, A.A., Richardson, P., Ashrafuzzaman, M., Johnson, B.K., Chakhchoukh, Y., Haney, M.A., Sheldon, F.T. and de Leon, D.C., February. Isaac: The idaho cps smart grid cybersecurity testbed. In *2019 IEEE Texas Power and Energy Conference (TPEC),* 2019; 1-6.
28. Khandker, S., Turtiainen, H., Costin, A. and Hämäläinen, T. Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures. *IEEE Transactions on Aerospace and Electronic Systems*, 2021; *58*(4): 2702-2719.

29. Munaiah, N., Rahman, A., Pelletier, J., Williams, L. and Meneely, A., September. Characterizing attacker behavior in a cybersecurity penetration testing competition. In *2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, 2019; 1-6.
30. Matheu-García, S.N., Hernández-Ramos, J.L., Skarmeta, A.F. and Baldini, G., Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards & Interfaces*, 2019; *62*: 64-83.
31. Ramirez, R., Chang, C.K. and Liang, S.H., PLC Cybersecurity Test Platform Establishment and Cyberattack Practice. *Electronics*, 2023; *12*(5): 1195.
32. Kim, J., Kim, K. and Jang, M., May. Cyber-physical battlefield platform for large-scale cybersecurity exercises. In *11th International Conference on Cyber Conflict (CyCon)*, 2019; 900: 1-19.