Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

- Cyber Security Test Platform
- Triple Validation of IP Reputation
- Multi-Seller E-commerce Site
- Integrating Security Operation Center

Discovering Thoughts, Inventing Future

VOLUME 24 ISSUE 1 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 24 Issue 1 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

Editorial Board

Global Journal of Computer Science and Technology

Dr. Stefano Berretti

Ph.D. in Computer Engineering and Telecommunications, University of Firenze Professor Department of Information Engineering, University of Firenze, Italy

Dr. Abdurrahman Arslanyilmaz

Computer Science & Information Systems Department Youngstown State University Ph.D., Texas A&M University University of Missouri, Columbia Gazi University, Turkey

Dr. Lamri Sayad

Ph.d in Computer science, University of BEJAIA, Algeria

Dr. Tauqeer Ahmad Usmani

Ph.D in Computer Science, Oman

Dr. Hazra Imran

Ph.D in Computer Science (Information Retrieval), Athabasca University, Canada

Dr. Magdy Shayboub Ali

Ph.D in Computer Sciences, MSc in Computer Sciences and Engineering, BSc in Electronic Engineering, Suez Canal University, Egypt

Dr. Nurul Akmar Binti Emran

Ph.D in Computer Science, MSc in Computer Science, Universiti Teknikal Malaysia Melaka, Malaysia

Dr. Asim Sinan Yuksel

Ph.D in Computer Engineering, M.Sc., B.Eng., Suleyman Demirel University, Turkey

Dr. Anis Bey

Dept. of Computer Science, Badji Mokhtar-Annaba University, Annaba, Algeria

Alessandra Lumini

Associate Researcher Department of Computer Science and Engineering University of Bologna Italy

Dr. Rajesh Kumar Rolen

Ph.D in Computer Science, MCA & BCA - IGNOU, MCTS & MCP - MIcrosoft, SCJP - Sun Microsystems, Singhania University, India

Dr. Rajneesh Kumar Gujral

Ph.D in Computer Science and Engineering, M.TECH in Information Technology, B. E. in Computer Science and Engineering, CCNA Certified Network Instructor, Diploma Course in Computer Servicing and Maintenance (DCS), Maharishi Markandeshwar University Mullana, India

Dr. Aziz M. Barbar

Ph.D. IEEE Senior Member Chairperson, Department of Computer Science AUST - American University of Science & Technology Alfred Naccash Avenue Ashrafieh, Lebanon

Dr. Federico Tramarin

Ph.D., Computer Engineering and Networks Group, Institute of Electronics, Italy Department of Information Engineering of the University of Padova, Italy

Dr. Chutisant Kerdvibulvech

Dept. of Inf. & Commun. Technol., Rangsit University Pathum Thani, Thailand Chulalongkorn University Ph.D. Thailand Keio University, Tokyo, Japan

Dr. Roheet Bhatnagar

Ph.D in Computer Science, B.Tech in Computer Science, M.Tech in Remote Sensing, Sikkim Manipal University, India

Contents of the Issue

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 24 Issue 1 Version 1.0 Year 2024
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Defending Cloud Web Applications using Machine Learning-Driven Triple Validation of IP Reputation by Integrating Security Operation Center

By NW Chanka Lasantha, Ruvan Abeysekara & MWP Maduranga

IIC University of Technology

Abstract- This paper will present an innovative system method of IPR (IP Address Reputation) validation with the assistance of clause of (ML) machine learning for discovering malicious IPs, while also viewing the importance of security of installed applications on AWS (Amazon Web Services) servers. The ML, SANS and AbuseDB datasets that were verified are being integrated through the Wazuh Security Operation Centre (SOC) stage to consume issues at the log ingesting IP address-related level. Having integrated extraction of IPs Wazuh agents, the output does match MITRE ATT&CK framework-filtered IP address from the Wazuh SOC. These algorithms and models based on natural language processing will flag suspicious patterns across IPs through the process of machine learning and prevent the event of a cyberattack at the time. This integration not only boosts cybersecurity information through a single point source of distribution, but it also provides security finds and other resources to prove and maintain awareness against malicious IPs.

Keywords: SOC, ML driven IP reputation validation, AWS WAF auto defense, ML powered extended validation, MITRE ATT & CK framework-filtered IP address.

GJCST-E Classification: ACM Code: D.4.6, K.6.5

Strictly as per the compliance and regulations of:

Defending Cloud Web Applications using Machine Learning-Driven Triple Validation of IP Reputation by Integrating Security Operation Center

NW Chanka Lasantha [α], Ruvan Abeysekara [σ] & MWP Maduranga [ρ]

Abstract- This paper will present an innovative system method of IPR (IP Address Reputation) validation with the assistance of clause of (ML) machine learning for discovering malicious IPs, while also viewing the importance of security of installed applications on AWS (Amazon Web Services) servers. The ML, SANS and AbuseDB datasets that were verified are being integrated through the Wazuh Security Operation Centre (SOC) stage to consume issues at the log ingesting IP address-related level. Having integrated extraction of IPs Wazuh agents, the output does match MITRE ATT&CK framework-filtered IP address from the Wazuh SOC. These algorithms and models based on natural language processing will flag suspicious patterns across IPs through the process of machine learning and prevent the event of a cyberattack at the time. This integration not only boosts cybersecurity information through a single point source of distribution, but it also provides security finds and other resources to prove and maintain awareness against malicious IPs. The final solution includes using the maximum amounts of bad IPs blocking in the 'IP-List' of AWS WAF and, if they are added to the Blacklist automatically, checking them through an automatic ML-based signature validation process.

Keywords: SOC, ML driven IP reputation validation, AWS WAF auto defense, ML powered extended validation, MITRE ATT & CK framework-filtered IP address.

I. Introduction

The implication of the discrete web application defences could be a source of great difficulties. The most vital element in defence from bots is the reduction of machine-learning-based bot traffic, which also has a leading role in the protection of real IP addresses. Proposing that strategy, early detection of IP defence compromising is possible, and evaluated only neutral ML bots' versions are used for analytical analysis. In this area, the most prominent modern element is designated on-demand IP addresses. The security featuring machine-generated digital keys provides them with a sign of comprehensive protection. [1] ML technology is the core functionality of this process which is also underpinned by advanced algorithms. To supplement the IP Reputation Monitoring, Smarter measures to find out if web applications are blocking other cybersecurity measures are being implemented. [2] To be specific, this is a system made of many complex layers. To do this very well it uses neural networks, machine learning, and all the skills it can gain from the large language models (LLM). These models are very effective, and their operations involve the extraction of actionable data from the database and records, with IP details. The robustness of the system is meant to be increased this way by integrating complete security frameworks and databases established controls, as well as MITRE ATT&CK framework [3], Hence there is an array of approaches that work together to intercept and block any explanations of malicious IP addresses which ultimately solidifies the effectiveness of the automated defence mechanisms using the Wazuh SOC Logs, which is a highly advanced platform that processes and stores logs. [4] With this merging, signatures based on the techniques of machine learning can be used on an ad hoc basis to guarantee a real-time production of ML-driven signatures. The proactive cognitive system exhibits the connection of machine learning and cybersecurity, it offers a clever and dynamic solution to the fast-moving landscape of security needs in web applications.

II. Background

a) Importance of IP Reputation based on MITRE

IPR serves well the indication purpose of when a network is to be accounted for a prime target of hackers. A problem arises through which WAF is thrown out of its comfort zone and it should deal with network protection applications. The reputation is the rating which is the most important for programs of this kind. It serves as the basis for decision-making about the entry and removal of the IP traffic. [5] The most dangerous consequences of non-IPR incidents can be divided into five groups spamming, bot activities with harmful intent, DoS attacks, injection attacks, and occasional use of this source for botnet operations. In the application of IPR, it is not merely a tool for adding to the known risks but also a motivator for exploring the possibilities. This is to say that is the underlying cause of cutting into network and services average. In the IP carrying a bad reputation security attacks are regarded and it is well

Author α: Faculty of Graduate Studies, IIC University of Technology, Phnom Penh 121206, Cambodia.
e-mail: chanaka.lasantha@gmail.com
Author σ: Faculty of Graduate Studies, IIC University of Technology, Phnom Penh 121206, Cambodia. e-mail: ruvan@iic.edu.kh
Author ρ: Department of Computer Engineering, General Sir John Kotelawala Defence University, Sri Lanka.
e-mail: pasanwellalage@kdu.ac.lk

known to signal a potential for bad activity. Consequently, great care should be observed in the elimination of such IPs. [6]

Also, the latter is associated with the most accurate IPR since self-introduction can be monitored and scored using interactive personal relationship features. As they assemble data for courts to use in investigations and to conduct IP tracking, they also prevent the organization from being tampered with by malicious activities. This approach's fundamental aspect represents the proactive defence that is the key concept of the MITRE ATT&CK framework and the high point is it emphasizes the importance of data protection would help organizations be conscious of the key sources of threats by fixing their attention on malicious controls and data system and that would consequently lead to efficient organizational business continuity with interruptions. [7]

b) Challenging on Traditional IPR

The IPR Validation, the main traditional method is mainly to search IP addresses in directories and blacklists which increases behavioural analysis. Nevertheless, this method of data collection omits most of the pre-validation procedures that are prerequisites for a stable dataset meant to be useful for training ML models. Selection lists are mostly loaded through honeypots, spam traps, and regular event logs. The scores look at an IP-address reputation for certain behaviour. [8] Also, The IPR is decreased by this system 'reputation sink,' where IP reputations become not relevant over time without the continuous, real-time validation of the multi-layer approach. [9] This asymmetry led to the impossibility of coping with cyber threats just merely by the databases, which necessitates a constant update process of the databases is essential. Tribulation of such an approach leads to many false positives and negatives consequently making the traffic management inadequate. The problem is pronounced by the deficiency of ML algorithms' accuracy and the application of the metadata that is either out of date or inaccurate concerning the IP addresses. [10]

III. Existing IPR Architectures

a) Mitre Freamwork baed for IP Attacks Detections

The pre-attack patterns determined in enterprise knowledge bases also add a lot of value in terms of tracking adversary tactics, techniques, and procedures to ensure that an incident can be well responded to, and the attack repelled. Uncaught and disruptive activities by availing themselves of what the adversaries use to penetrate competitive networks must be brought to understanding and unveil an essential topic of the monitoring methods and ways to fix impacts by using the MITRE ATT&CK framework. [11] Given this architecture, it is a comprehensive and quick-access knowledge by providing exclusive information on the present-time procedures of the enemies against real-life scenarios. This assists in building, in the private sector the government, and the cybersecurity community strong programs to monitor the threats. [12]

b) Prevention Technologies for IP Address-based Attacks

One of the hardest things about cybersecurity is tracking and stopping cyber-attacks at the IP address levels which was solved by one of researched blacklists and tools such as AIPRA, which combined ML with geolocation data to figure out what's not relevant for regions and countries in usual working time range of humans. But problems such as false positives, and maintenance of the fast-changing nature of its enemy continue to an accurate validation process. ML can help AIPRA systems immensely while cutting-edge algorithms and effective data processing, combined with the optimization of models which increase accuracy while reducing false positives, keep it up to speed on new threats. [13] This strengthens cybersecurity defences on IPR, while the security of the LAN The MAC and IP addresses, computer names, IP conflicts and MAC mismatches are most important to reduce attacks from bad IPR vectors in securing network traffic and assets and spoofing risk over digital infrastructure. Such that, the spoofers forge these identifiers to masquerade as IPR validation systems. [14]

c) Traditional Bot Traffic Tracking Techniques

The applications of Residential IP Proxy (RESIP) facilities are becoming more and more popular cases of web scraping and other criminal actions such as relocating behind the reserves of residential IPs where the detection is prevented. Two additional datasets indicate the functioning of RESIP where its figures are highlighted only with the four providers but not with differences concerning them. [15] They suggested an operational scheme that can automatically compare accounts with shared characteristics. Besides, overall, five campuses undertook vulnerable RESIPs' investigation, showing attacked hosts and unlawful acts. [16] This study can shed light on and address the security chances that this growing sector is attributed to. RESIPs, which are a new grey-area business, provide a shield from scrutiny by using other people's computers in their homes to complain about illegalness and recruitment ways. [17] Also, it proposes RETRO detection, a technique that captures the sequences of flows using a compromised device, raising the operational opacity of these services. While it optimizes a server-side detection method for RESIP connections, dropping false negative outcomes that result from mobile proxies. [18]

d) AI Models for IPR Detection Capabilities

IP Starting with the fundamentals of IP protocol to the daily activities on the internet such as surfing the web and emailing, Internet resources are indispensable, which urges security professionals to use IP addresses for risk assessment. This work makes use of cross-protocol telemetry on a large scale to classify malicious IPs and make ML interpretability because of which this approach is more effective. [19] The results reflect that there is zero error in identifying malicious IPs. To mitigate against the rising cyber dangers, The duo proposed a mixture of different attributes which involved Dynamic Malware Analysis, Cyber Threat Intelligence, ML and Data Forensics. [20] This technique comes with a reputation of IP, groups 'zero days', and closely as well as automatically analyzes damage, degree of risk, and impact. This model takes while factoring in the conventional network and geo-contextual information, thus enhancing threat assessment and enabling the detection of unlawful behaviour, especially in cyber-space that has HTML encoding. [21]

e) NLP for Enhanced Threat Detection Using ML

The growing trend of IoT-devices interconnectedness has resulted in an uptick in intrusions. IDS or IPS systems are a type of security solution that monitors and detects system violations. [22] Nonetheless, a holistic synchronousness in new developments and model limitations means that a new security framework is required. [23] On the part of this survey AI techniques such as machine learning and deep learning seem as most relevant solution with hybrid design efficient intrusion detection/prevention emphasizing. It considers their viability, setbacks and real-time issues. securing IoT, ML and big data analytics have profound effects on it. [24] This is where they come in. This investigates IoT vulnerabilities, uses ML for cyber-vulnerability assessment, and analyzes ML-based intrusion detection solutions. It provides an example of a real-world testbed which is used for the design of IDS, demonstrating that Machine Learning is capable of intrusion detection in computer networks. However, this study the literature on the topic of anomaly-based intrusion detection systems driven by ML/DL, pushing the boundaries to unleash the full potential of ML-based systems, examining open issues efficiency. [25]

f) BlackEye IPR Framework

Algorithms Blacklisting malicious IP addresses is an essential tool for IT systems' protection. The decision-making is based on looking at packet traffic data and the behavioural history of users. Still, the holding of domain experts for blacklisting is on but ML is on the way and just awakes to maturity. This is solved by making the Black Eye framework based on which the different ML methods are used accordingly to achieve superior results. The analysis shows that the multistage method, which is achieved by data cleansing and classification with logistic regression or random forest, leads to the best results. Real-world data evidenced a near-90% less incorrect blacklisting compared to the expert performance. By the same token, our model accelerates the time-to-blacklist, significantly cutting the lifetime of malicious IP addresses on average by 27 days. It can be considered a breakthrough in the process of protecting the IT system concerning blacklisting and redesigning the efficiency and accuracy of the system security. [26]

IV. Capabilities and Limitations

a) MITRE ATT&CK Framework Boundaries

The MITRE ATT&CK (MITRE Adversarial Tactics, Techniques & Common Knowledge) framework which motivates the cybersecurity industry nevertheless has multiple challenges like the lack of clarity, incomprehensive comprehensiveness and dynamics of rapid knowledge that may dismantle especially new or inexperienced security personnel leading to the framework's apparent underutilization. The configuration's information studies involve mass data analysis, but the demand is higher than normal, automation is lacking in most organizations, and the framework will cause more burnout on SOC than it can handle. Defence against the Dark Arts is also afflicted by standardization issues because some sub-techniques are either too niche or incomplete existing problems that comprehension and application are difficult. Similarly, by its charter to capture only documented cases, it can sweep under the radar of inaugural threats and their occult threats thus, limiting its efficacy in preempting threats. [27]

b) IPR Validation and Prevention Using ML

Malicious IPs will not be allowed to access the system hence the IT security will remain under. BlackEye uses ML and after researching it has been proved that a two-staged solution with some preprocessing to be followed by either logistic regression (NR) or Random Forest (RF) is effective to a ratio of only 15% blacklisting false alarms. Furthermore, the Tower uses Ridger heightening to get a 5% higher precision. BlackEye, by integrating and quickly iterate through ML on heterogeneous logs. With the help of this neural ML method, accuracy would be improved and the time to blacklist would substantially be reduced. More upstream work is accomplished through the application of deep learning in the identification of risks. [28]

c) IPR Validation of Public Databases using ML

The exact rate at which cyber-attacks are rising is a result of more individuals, groups, and corporations connecting online. Old-fashioned blacklists work, but they could be improved by shaking off two of the broken records. unverified data and stale data. First, these

issues were solved by the AIPRA (Automated IP Reputation Analyzer Tool). This action is in the form of verification by comparing the domains or IP addresses indicated whether they are on the list of blacklisted that is commonly used in several indexes. The AIPRA first evaluates if there might be any malicious activities at these URL addresses and comes up with a weighted probability that indicates how much it is possible. Also, a geolocation-based artificial intelligence concept was made a component of AIPRA since this way the system could be trained to recognize a wider spectrum of threats. When the Report produced this result, it had not yet been identified as being on any list to the public. [29]

d) MAC Address Spoofing LAN Attack Validation

The security problems of Local Area Networks (LANs) are being constantly dynamically generated. Nevertheless, it is a meticulous method of decoding how the hacker achieves such an objective by spoofing both his MAC and IP address to lift LAN internet accounts from unauthorized users, which seems very hard for the account administrator to monitor. Further, ensure that such protections are implemented, and the brute root of any untoward act must be cut off, this can secure oneself an Advanced IP Scanner or MAC Address Changer and prevent outside attacks but also an IP address itself a gateway lest it sneak it being the facilitator. Two main factors that can force crooks to get involved in such frauds are the financial strain and the constant need to make fast money. When at the hacker's stage, the administrator is moving to the progress of the attack by exploiting the user and the ISP's routers' default passwords. [30]

e) Detecting Malicious IP by Cross-Protocol Analysis.

The system of reputation trust takes real-time data into ML machine processes to become a way of enhancing security through the cloud. Such a system will function around powerful algorithms which would recognize and destroy malware websites. In contrast, the system's defence is through source code encryption and obfuscation, hence operating using the same common IP reputation key across providers and in a consistent manner to protect the system from being a target. New components and augmentation methods of data have made pre-processing features useful and groups to choose a threat feature. The system, which ensures false positives and negatives also, employs error analysis and explainability to get enhanced precision. It demonstrates network IP using port 53, so the DNS traffic goal is accompanied by a figure of improvement for the incremental model that is tailored for enhanced flexibility and efficiency. Despite this, the main issues associated with the small data size including label as quality or accuracy of the labels on the big models, are being considered. Firstly, we can understand deeply how the reputation alongside the rating lines of the users mutually binds with the tendency of response modification over time and, as a result. [31]

f) Detection of malicious traffic by learning IP Reputation

Based on the use of adaptable and modular technology in ML, it is a lightweight solution that works in such a way that the old approaches are not completely replaced. The approach of our study in line with the present methods aiming to control the list of IP addresses of spam mail and the flow of the campus network is different because of the application of a higher method. Sites tagged as dangerous and those tagged as malicious are scorned but the ones whose intention is unknown continue to operate freely and the assaults are not thwarted. Yet, such a feature is practical with no warning limit to the common hosting, thus the more this favourable gesture is done the better outcomes it's likely to achieve. Whilst the intelligence services exert their efforts to attain the upper hand, it is the adversaries that show the power of adaptation and are changing their tactics that the real problem is. Most importantly, the offence has the supreme edge for the unforeseeable. [32]

V. Main Methodology of Poporsed Solution

a) Components Of Methodology

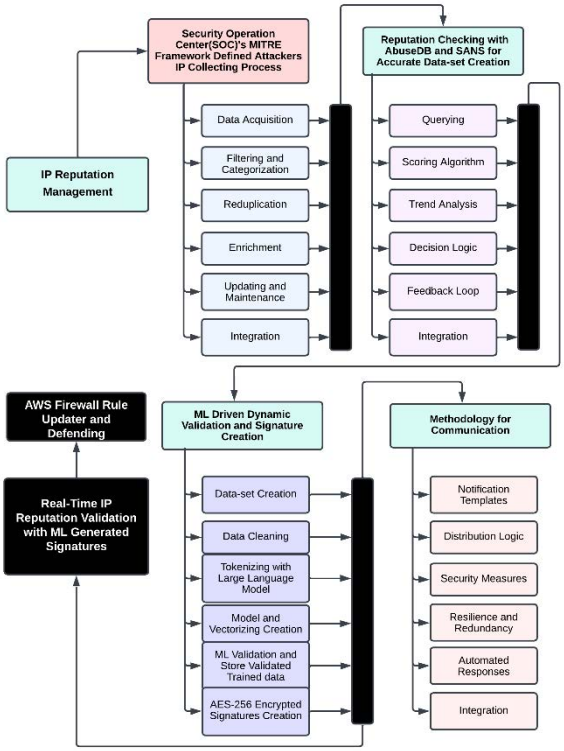


Figure 1: Methodology

b) SOC Attackable IP Collection and Analysis

Figure 1 shows the data collection phase IP address scope that is consecutively given by MITRE ATT&CK logs with REST API connection from multiple units in the SOC system. The logs contain the information of the cloud system, flow as well as the server. An early part of the first move was the classification of IPs as trusted, suspect, or unknown habitats that will eventually set up data sets for matching them in a confirmation process. Single IP deduplication method and ultimately the proliferation of research. The best psychological assessment can be due to geolocation IP information, individual behaviour history, and diagnostic criteria which are stated in these modules. The databases become erroneous only if they are not appropriately revised and have the old data changed at certain fixed intervals. Interfacing with the machine consists of sketching the assembly system from the IPs, therefore, the real-time generation of the IP enables the system to produce these just risen or risked IPs. Followingly, this stage will determine WAF logs metadata to find IP addresses and domain names while focusing on extracting specific required features to make sure algorithms can work properly, then; anomaly detection is made on domain name feature Plus IP address (IPR) to make comprehensive attention to areas of anomaly signs. Besides, it does the essential functions of the concealed dangers that are not always obvious and integration and moving on to security states.

c) IP Reputation Checking and Primary Dataset Creation

This procedure starts with AbuseIPDB API being connected to the recently revised IP reputation data [33] and then calling SANS API that is needed for a second recheck for the dedicated scoring algorithm of the bad metadata such as final score being blacklisted, reports number and the reason for the reports to be given. [34] This very algorithm moreover actually shows its face and shows the way that every IP address can have a certain weight by this score-based method and severity levels by unstructured raw data to the structured dataset.

d) ML Driven Signature Creation and IP Validation

In the beginning, the ML model is classified as being a signature to the validated datasets with filtration and tokenization being selected and then random forest was chosen as the ML model. The second part will be the production of vectors that will be generated after the training of a model has been completed. Ultimately the processing is done, individuals will be a bit nervous about their data so when the file is made it is going to be saved into a folder that is safe to store it in and this data is verified to be true. The next step in the final

process is an AES-256 Encryption signed with an ML-driven signatures generation method. [35] Such volatility erodes the monetary authority's ability to set policies and makes the currency regime less stable. In addition, it applies the appropriate signature detection method by querying the MySQL database.

e) Automatic AWS Firewall Rule Updater for Defending

The system creates alerts varying in level of danger as well as differentiates communications based on a user's role in the organization. It also includes an automated response protocol that can quickly update settings such as firewall IP- Blacklist rules if not already exist and add them to the Web Access Control List to block rapidly when it is validated as an attacker IP address during the validation process within a certain period without affecting legal sites for a grouped period. As a result, real attackers will only be blocked for a while which will prevent damage to the target system that is vulnerable to attack.

VI. Algorithm used in the Proposed Solution

The computer algorithm technology to the existing security algorithms and setups, technology which can execute the parameters but there are chances of involving errors and lower setup time that increases setups. AWS Secrets Manager is being utilized as a credential secret retrieval solution verifying and ensuring that the company is at the required security level and the predefined security practices are being followed. Immediately after that, they created a customized abuseDB, SANS, and the model-learning mechanism for the IP Reputation analysis process. It has two noticeable points as to why ML-based technology is a better choice compared to rule-based systems in the MITRE ATT&CK logs the first pro is the ability to understand the context and find a pattern in the cases in which rule-based systems were not able to do it well. This way it brings in dynamic signatures and spots bad IP actors quickly and easily.

Furthermore, this process works out ML's limitations and will make lives for intelligent machines that are alive and evolve. On the other side, this layer operates as a second line of security systems which are used to identify threats before they can even take place. As for the NPL detection strategy, the automated creation and regular check-up of Abuse IPDB API and SANS API query results accompanied by the third layer of the final validation method could also play an important role in boosting NPL detection quality and is important. Maintenance is optimized and overload that leads to a system failure is tried to mitigate in this way in whole system performance.

VII. Experimental Proposed Solution

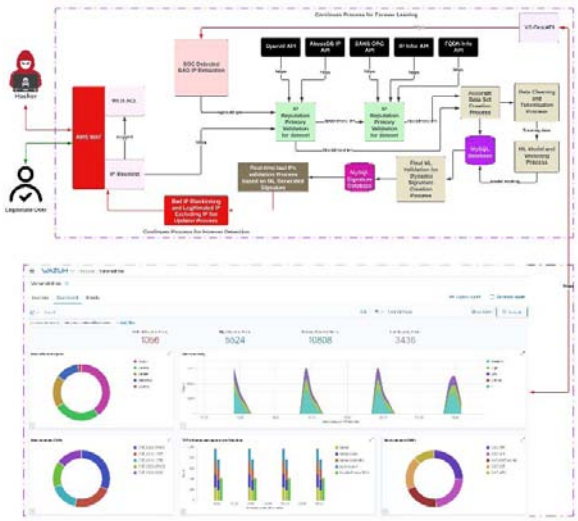


Figure 2: Experimental Setup

Figure 2: provided appears to be a detailed schematic of a security system for cloud web applications, integrating machine learning with IP reputation validation to enhance cybersecurity measures. At the top, icons differentiate between a hacker and a legitimate user, indicating the types of traffic that the system must differentiate between. The AWS WAF serves as the initial barrier, applying rules through a WEB ACL to regulate incoming traffic. The system includes a process for real-time bad IP blacklisting, which employs various APIs such as Open AI, Abuse IPDB, SANS ORG, IPInfo, and FQDN Info to gather intelligence on IP reputations. This intelligence is then processed through machine learning validation, which dynamically updates the IP signature database. The process of data cleaning, tokenization, vectorizing,

and machine learning modelling is depicted, suggesting the preparation and utilization of data to train the system to continuously identify and respond to threats. This is supported by the ongoing "Forever Detection" process, indicating an adaptive security posture. Figure 2: there's a security dashboard, such as a tool such as Wazuh SOC, displaying various security metrics. This includes the number of detected vulnerabilities, the severity of alerts, and the distribution of these alerts across different security agents. Graphs show the trend of security events over a certain period of days regarding IP data, while additional charts detail the most common vulnerabilities identified by their CVE identifiers.

VIII. Outcome of the Solution

a) ML Validated Data with Predictions

Table 1: Sample section of ML-validated final test data

Aws Acco-Unt Id	Re-Gi-On	Ip Address	Total Repo-Rts	Abuse Confide-Nce Score	Is Whit-Eliste-D	Attack Proba-Bility
xx	xx	121.162.210.148	379	100	0	attacker
xx	xx	124.107.37.84	0	0	1	not_attacker

Through employing the IP verification model, the data obtained from the resolve is illuminated in Table 1. It stands out from the other algorithms by the fact that it uses report data to create reputation scores, where the number of reports, how recent, and the confidence that they are abuse reports are all considered. To combat this, we developed whitelists and blacklist IPs to shield ourselves from the high-risk IPs. These IPs also displayed their cases with malicious activities, for instance, they were signed to port scanning or brute force attack.

b) ML Validated IP Abuse Score

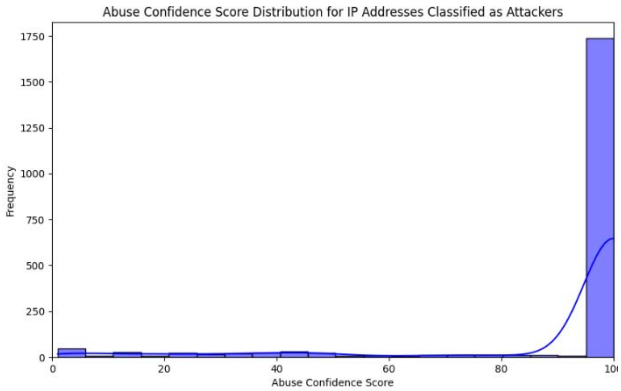


Figure 3: Abuse score Illustration

Figure 3 shows that the DB API models were ratified to be IP Abused, Plotting the virtual curve of Abuse Confidence Score that began with 80 and ended with 100 proves that our reporting system is intensified with the passing days. Confidence of reports increases especially from credible sources. This rises very possibly because the algorithm relates more highly to reported unusual IP addresses, severe admins taking greater weight. IPs with the high risk may end up with a loop of additional monitoring when the system fails to achieve a good level of attack-reducing mechanisms for these IPs. Organizations, with a cushion effect, may opt for such formulas that give higher results to the IP nearing the maximum with the scores being concentrated at the top end, or 100, signifying a strong consensus about the risk of a given IP. Therefore, it is expected that the frequency of scores at the upper end of the scale will rise sharply.

c) ML Definitions

Precision is calculated as:

$$Precision = True\ Positives\ /\ (True\ Positives + False\ Positives)$$

Recall is calculated as: [36]

Recall = $True\ Positives$ / ($True\ Positives$ + False Negatives)

The F1 Score is the harmonic mean of Precision and Recall and is calculated as: [37]

F1 = (2 * Precision * Recall) / (Precision + Recall)

The False Positive Rate (FPR) is calculated as: [38]

FPR = FP/ (FN+FP)

d) Overall RF ML Predictions

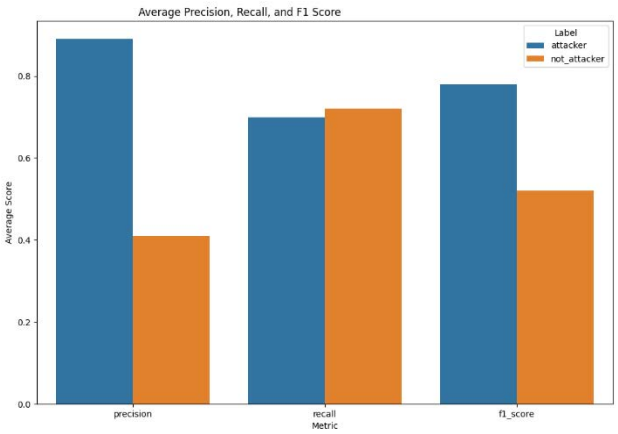


Figure 4: Overall ML Predictions

Figure 4 shows that precision stats measure the subtle of sensitivity or accuracy of positive predictions. To summarize, the model predicted a successful attack in which the actual attacker situation. For the group predicted "attacker", the precision is very high around 1 implying that the model is most of the time right when it predicts an attack. The accuracy for the term "not_attacker" is a bit lower, which signifies a high prediction accuracy for the same. Also, Recall Retrieval's mission is to discover all the cases that are of significance to all the points in the dataset. For the "attackers" class, the recall outperforms the precision, however, this is to keep the recall above 0.9 which demonstrates that the model can identify most of the actual attackers.

The "class" of the "not_attacker" recall is nearly the same as for the "attacker" class, indicating that the model is as good at detecting instances that are not attacks as those which are. Additionally, The F1-score signifies the harmonic arithmetic mean of precision and recall. It is just one measure that considers the accurateness and the pullback of a classifier and expresses these results into a single metric. If the classifier has a high sensitivity, it is more likely to avoid false positives. in other words, it is accurate. Overall, the model is not unbalanced as a high F1 score is observed for both "attacker" and "not_attacker", making the model execute much better than expected.

e) Overall RF Correlation Matrix Heatmap

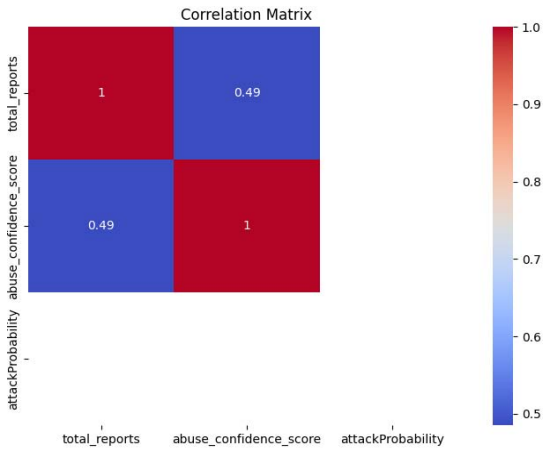


Figure 5: Correlation Matrix Heatmap

Figure 5 visualizes the correlation matrix using the heatmap plot. A Correlation Matrix is simply a table with Correlation Produced between different variables. Every row of the table visualizes the problem of how the two variables are connected. The range is from 1 to 1 for its units. If two variables are strongly (near 1 or -1) related it is indicative of a high correlation between those two. When the correlation is close to 0 it indicates that there is a zero linear relationship.

Also, the diagonal represents the relationship between each variable and itself. The correlation of a variable with itself is always 1, which equals perfect correlation. The relationship between abuse_ confidence_score and total_reports is about 0.51, meaning along the linear relationship, when one variable increases, the other variable also tends to increase, but to a lesser extent which would be a perfect linear relationship, and the correlation would be bigger, 1.

In addition, the heatmap uses colour intensity to represent the strength and direction of the correlation. The heatmap uses colour intensity to represent the strength and direction of the correlation. The dark color would be used to represent a negative association nonetheless there are no negative values in the matrix. The depth of colour corresponds to that of the strength of the relationship, with the contrary being darker shades representing those of stronger relationships. On the colour bar, you see on the right the values of the correlation coefficients that stand for heatmap colours are given. The value of colour ranging from red to white and from white to blue shows that closer to 1 value is the red colour while lower the value is close to -1 value, which is the blue colour.

f) Overall RF Confusion Matrix

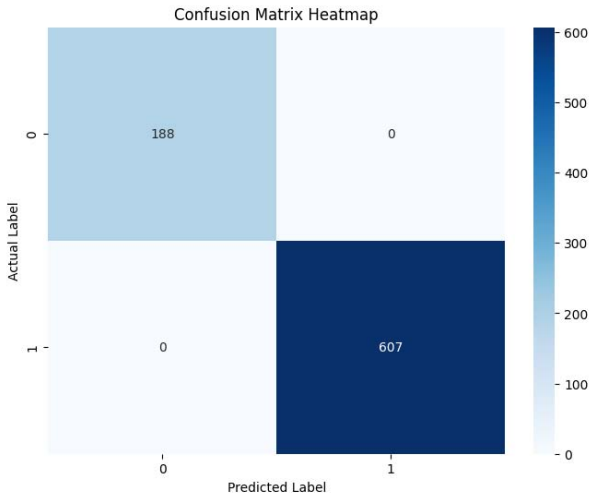


Figure 6: Confusion Matrix

Figure 6 shows the heatmap of the confusion matrix for a binary classification model. The labels on the y-axis are the real ones, and on the x-axis are the anticipated ones. The figure below highlights the fact that it has been determined that 188 true negative examples (U-L) and 607 true positives (U-R) have been correctly classified. Instead of false positives and false negatives, as shown in the top-right and bottom-left cells of the matrix being zeros, means that there won't be any misclassifications. The size of the circles is relative to the term occurrence and the darker the tone, the more instances. It will be plausible to conclude that the model attained mean square error which is equal to zero on this data set.

g) RF Tree Visualization

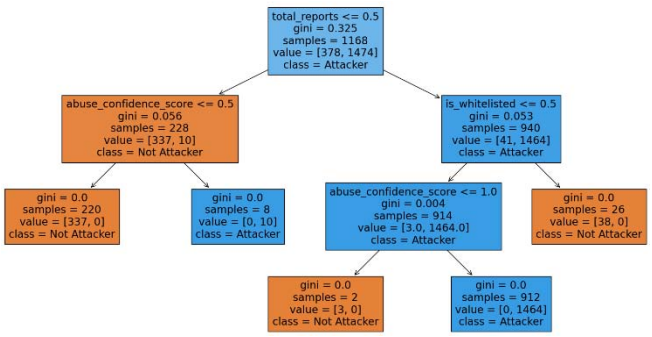


Figure 7: Tree Visualization

Figure 7 describes the decision tree as a representation related to classifying the entities into "Attacker" or "Not Attacker" ones, where we utilize 'total_reports' as a main measure. In case 'total_reports' equals 'abuse_confidence_score', 'abuse_confidence_ score' is evaluated and "Not Attacker" will most probably

be assigned a score of 0.5 or less. For a high 'total_reports', 'is_whitelisted' is the main result maker while the confidences of the entities below 1.0 and non-whitelisted are mostly classified as "Attacker". However, what catches my attention is that the Gini index of numerous leaf nodes is equal to zero which shows an extremely confident model that is prone to misclassification in case of unbalance on the other hand, the model can catch the exceptions as well as distinguishing between them properly, which is a reason for satisfactory results in leaves with not enough samples. In short, it uses total reports',' abuse confidence score,' and 'is whitelisted' as its principal columns showing the situation of the classifier where they shape clear decision paths and strong class differentiation.

h) RF Cap Curve

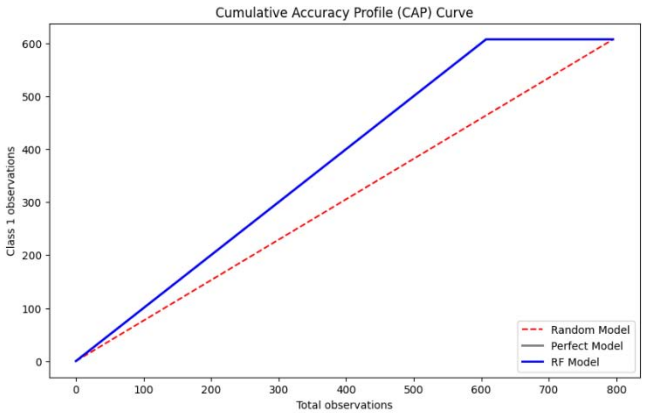


Figure 8: Cap Curve

Figure 8 shows the Cumulative Accuracy Profile (CAP) curve used for the Random Forests (RF) model classification evaluation. The dashed red line is a random model, which may only be able to fulfil similar goals as if there was no model at all. The solid blue line that is perfectly straight and aligned at the top part is the perfect model that gets total accuracy by correctly classifying all the instances of the class at once. In contrast, the RF Model's curve which is another blue solid line shows the model's performance which is superior to random guessing as the curve curves towards the ideal model, demonstrating that it ranks instances of truth consequently better than random guessing. The Diagnostic Accuracy of the RF Model Relevantness is being measured by the Area Under the Curve Calculation (AUC CAP) works very well, which has a value close to 1, and this one is far better than a random approach. The R^2 Model exhibits a pattern of improvement against unintended chance and is approaching the most desired alternative.

i) RF Distribution of Total Reports

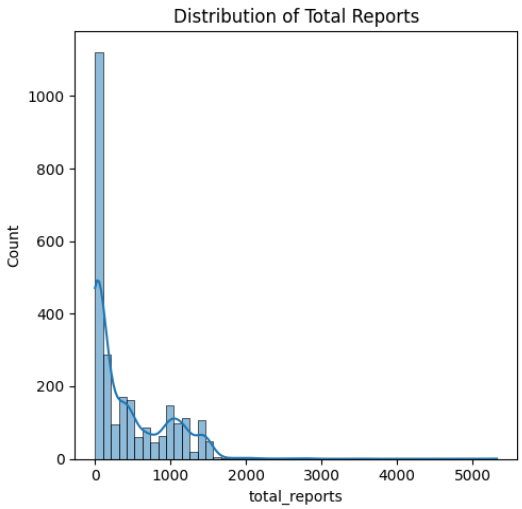


Figure 9: Distribution of Total Reports

Figure 9 shows the histogram together with a kernel density estimate (KDE) in which the distribution of the value "total_reports" is plotted. The y-axis represents values count or items are divided into bins. On the y-axis, data is presented in the form of how often these words are in the analyzed texts. The height of every bar you can see indicates the number of occurrences of the analyzed word in every bin range. The graph illustrates the right-tailed pattern to indicate over the x-axis mark, the greatest number of data exhibits low "total_reports" count, and less and less as we move toward the end of the axis. The KDE line shows the distribution smoothed by connecting the points representing the peaks on the left and the end of the tails indicating some extreme cases with high report counts. This smoothed image indicates the presence of the skew right value with most reports around the centre and the tail on the top side and a single point or few isolated points on the bottom curve.

j) AWS WAF IP-Deny List for Blocked IP Address

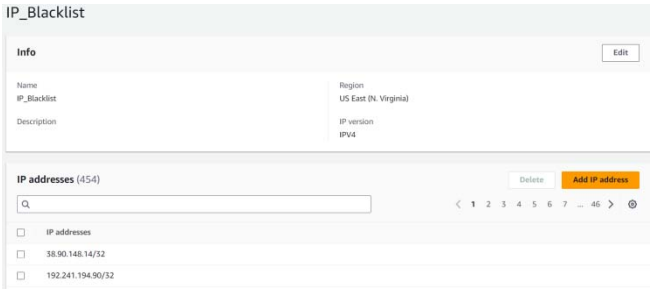


Figure 10: Blacklist over AWS WAF

Figure 10 shows that an automated IP was blacklisted by The IP Reputation validation system accurately minimizing False Positive IP blocking to allow legitimate services not been getting blocked by the AWS WAF in the corresponding IP List section. Also, this solution successfully blocks these kinds of bad attacks by bad actors and automatically blacklines all relevant addresses based on machine learning-in effectively, those related to checking ML-Driven signatures verification process while the solution uses the IP-List section of AWS WAF to automatically blacklist attacks from bad IP addresses.

k) AWS WAF WAF Blocked and Allowed IP Percentage

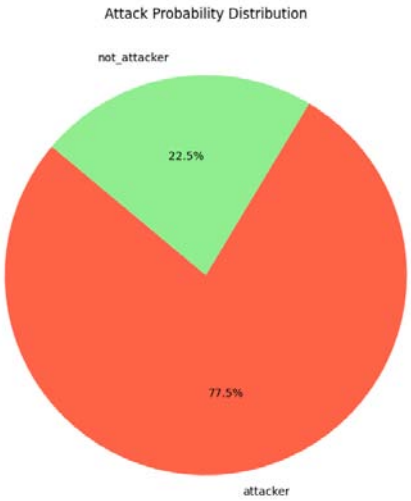


Figure 11: WAF Blocked and Allowed Illustration

Figure 11 shows both blocked and allowed IP address percentages based on a defined period in the WAF IP-Blacklist updated module based on ML prediction auto-generated pie charts as shown above.

IX. Discussion

This is an enhanced solution that the showcase introduces, with strong application value in cybersecurity operations. It can greatly simplify many other aspects of the trust verification process, one prerequisite for network security has to do with IPR. It connects to AbuseIPDB and OpenAI Analytics Engine. This entails checking a database of abuse reports, so the assessments are accurate and topical. This approach quickly selects, verifies, and classifies response data for analysis or combination with other systems. Using its

scalability and automation capabilities, it can track down threats from virtually any IP. However, weaknesses exist such that the use of handle API rate limits is convenient but results in delays when network activity is high that can become a bottleneck. Misses from a lack of sophistication in error handling threaten detection. AbuseIPDB goes down while continuously validated by Trane ML dynamic signatures until API is back to normal if any case has occurred for the API fetch process., and the whole network is exposed. The solution also needs to have resilience (rate limit checks and error logging), but it cannot cover all eventualities.

X. Future Work

Looking at the upcoming future, a hybrid system will become a key factor in evolving the solution which will be accomplished by the application of the blend of the machine learning techniques Random Forest in collaboration with deep learning ML. [39] With the joint compilation of many works, the power of future predictions can be sharpened, leading to a level of accuracy even with a chance of less than 1%. Using these advanced computations, we can both have highly accurate results in this regard as well as the aspect of a considerable decrease in the time both in the process of detention and in the prevention of any event.

XI. Conclusion

During that thorough research, the proposed option attempts to prove the soundness of reputation validation for cloud firewalls with the help of modern ML-driven technologies. The foundational objective of this research was to find a solution to the shortcomings in the existing cloud-based firewall security mechanisms that usually fail to discriminate between the harmful and innocent firewall rules. The given study suggests a solution by applying a combination of RF algorithm (ML) and deep learning (DL) methods which have not been seen before.

Also, this combination was specifically chosen to leverage the strengths of both methodologies such that ML supplies a provisional predictive precision, whereas DL elevates the model's ability to analyze and distinguish complicated data structures. This technical improvement, however, is of the highest accuracy ever at more than 99%. This great level of accuracy is because of the design of triple filtering architecture into the AWS cloud firewall. This function brings different measures such as several tests and balancing into a system for the IP to check and report on the IP accuracy. This mechanism offers a new propitious approach that separates harmful traffic while leaving those who legitimately want to use the web applications unharmed. The paper shows that the given method can easily be transferred and used for different types of web applications and threats. This adaptability is of utmost importance since the industry always faces the challenge of continually dealing with new cybersecurity threats. They highlight that the systematical method that they have developed is not only a static solution.

Also, this suggests that the dominant role of ML and artificial intelligence (AI) in the creation and implementation of such security programs should be highlighted as well. These technologies provide the groundwork for the expansion and refinement of existing cyber defence capabilities in the face of potential complex cyber-attacks from what this paper has shown us it can be inferred that learning algorithms and neural networks yield a complete turnover of cloud firewall security systems. The reputation validation for the IP of web applications that use clouds is very accurate with this approach, therefore, it lays a solid foundation for protecting against malicious threats for online cloud web applications as well.

Acknowledgement

The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

References Références Referencias

1. P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," *IEEE Access*, vol. 10, no. October, pp. 121173–121192, 2022, doi: 10.1109/ACCESS.2022.3220622.
2. R. Vinayakumar, M. Alazab, S. Srinivasan, Q. V. Pham, S. K. Padannayil, and K. Simran, "A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4436–4456, 2020, doi: 10.1109/TIA.2020.2971952.
3. A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing mitre att&ck risk using a cyber-security culture framework," *Sensors*, vol. 21, no. 9, 2021, doi: 10.3390/s21093267.
4. N. A. Sankar and K. A. Fasila, "Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring," *2023 9th Int. Conf. Smart Comput. Commun.*, pp. 350–354, 2023, doi: 10.1109/ICSCC59169.2023.10334992.
5. N. Usman *et al.*, "Intelligent Dynamic Malware Detection using Machine Learning in IP Reputation for Forensics Data Analytics," *Futur. Gener. Comput. Syst.*, vol. 118, pp. 124–141, 2021, doi: 10.1016/j.future.2021.01.004.
6. H. Manocha, A. Srivastava, C. Verma, R. Gupta, and B. Bansal, "Security Assessment Rating Framework for Enterprises using MITRE ATT&CK Matrix," 2021, [Online]. Available: http://arxiv.org/abs/2108.06559

7. W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, "BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 59, pp. 88–94, 2016, doi: 10.1016/j.jnca.2015.06.013.
8. E. S. Sagatov, D. A. Shkirdov, and A. M. Sukhov, "Analysis of network threats based on data from server-traps," *2019 10th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2019 - Proc. Work.*, pp. 1–5, 2019, doi: 10.1109/NTMS.2019.8763847.
9. S. Benedict, "EA-POT: An Explainable AI Assisted Blockchain Framework for Honeypot IP Predictions," *Acta Cybern.*, vol. 26, no. 2, pp. 149–173, 2023, doi: 10.14232/actacyb.293319.
10. L. Deri and F. Fusco, "Evaluating IP Blacklists Effectiveness," pp. 1–8, 2023.
11. H. S. Sikandar, U. Sikander, A. Anjum, and M. A. Khan, "An Adversarial Approach: Comparing Windows and Linux Security Hardness Using Mitre ATT&CK Framework for Offensive Security," *IEEE 19th Int. Conf. Smart Communities Improv. Qual. Life Using ICT, IoT AI, HONET 2022*, pp. 22–27, 2022, doi: 10.1109/HONET56683.2022.10018981.
12. A. Kuppa, L. Aouad, and N. A. Le-Khac, "Linking CVE's to MITRE ATT and CK Techniques," *ACM Int. Conf. Proceeding Ser.*, 2021, doi: 10.1145/3465481.3465758.
13. J. L. Lewis, G. F. Tambaliuc, H. S. Narman, and W. S. Yoo, "IP Reputation Analysis of Public Databases and Machine Learning Techniques," *2020 Int. Conf. Comput. Netw. Commun. ICNC 2020*, pp. 181–186, 2020, doi: 10.1109/ICNC47757.2020.9049760.
14. S. Goel and S. Kumar, "An improved method of detecting spoofed attack in wireless LAN," *1st Int. Conf. Networks Commun. NetCoM 2009*, pp. 104–108, 2009, doi: 10.1109/NetCoM.2009.75.
15. A. Tosun, M. De Donno, N. Dragoni, and X. Fafoutis, "RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows," *Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron.*, vol. 2021-Janua, 2021, doi: 10.1109/ICCE50685.2021.9427688.
16. E. Chiapponi, M. Dacier, and O. Thonnard, "Inside Residential IP Proxies: Lessons Learned from Large Measurement Campaigns," *Proc. - 8th IEEE Eur. Symp. Secur. Priv. Work. Euro S PW 2023*, pp. 501–512, 2023, doi: 10.1109/EuroSPW59978.2023.00062.
17. X. Mi *et al.*, "Resident evil: Understanding residential IP proxy as a dark service," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2019-May, pp. 1185–1201, 2019, doi: 10.1109/SP.2019.00011.
18. E. Chiapponi, M. Dacier, and O. Thonnard, "Poster: The Impact of the Client Environment on Residential IP Proxies Detection," *Proc. ACM SIGCOMM Internet Meas. Conf. IMC*, pp. 712–713, 2023, doi: 10.1145/3618257.3624993.
19. Y. Huang *et al.*, "Detect Malicious IP Addresses using Cross-Protocol Analysis," *2019 IEEE Symp. Ser. Comput. Intell. SSCI 2019*, pp. 664–672, 2019, doi: 10.1109/SSCI44817.2019.9003003.
20. R. Maurya, "Analyzing the Role of AI in Cyber Security Threat Detection & Prevention," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 11, pp. 514–519, 2023, doi: 10.22214/ijraset.2023.56510.
21. A. Z. Faridee and V. P. Janeja, "Measuring Peer Mentoring Effectiven," *Am. J. o*, vol. 15, no. 2, pp. 7–22, 2020.
22. R. Ganeshan, C. S. Kolli, C. M. Kumar, and T. Daniya, "A Systematic Review on Anomaly Based Intrusion Detection System," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 981, no. 2, 2020, doi: 10.1088/1757-899X/981/2/022010.
23. A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Syst.*, vol. 189, p. 105124, 2020, doi: 10.1016/j.knosys.2019.105124.
24. M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, 2019, doi: 10.1109/JIOT.2019.2912022.
25. Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.
26. D. Jeon and B. Tak, "BlackEye: automatic IP blacklisting using machine learning from security logs," *Wirel. Networks*, vol. 28, no. 2, pp. 937–948, 2022, doi: 10.1007/s11276-019-02201-5.
27. R. Al-Shaer, J. M. Spring, and E. Christou, "Learning the Associations of MITRE ATT CK Adversarial Techniques," *2020 IEEE Conf. Commun. Netw. Secur. CNS 2020*, vol. 1345, 2020, doi: 10.1109/CNS48642.2020.9162207.
28. D. Jeon and B. Tak, "automatic IP blacklisting using machine learning," *Wirel. Networks*, vol. 28, no. 2, pp. 937–948, 2022, doi: 10.1007/s11276-019-02201-5.
29. N. Usman *et al.*, "Intelligent Dynamic Malware Detection using Machine Learning in IP Reputation for Forensics Data Analytics," *Futur. Gener. Comput. Syst.*, vol. 118, pp. 124–141, 2021, doi: 10.1016/j.future.2021.01.004.
30. S. Shaw and P. Choudhury, "MAC address spoofing," *Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015*, pp. 347–350, 2015, doi: 10.1109/ICACEA.2015.7164728.
31. Y. Huang *et al.*, "Graph neural networks and cross-protocol analysis for detecting malicious IP addresses," *Complex Intell. Syst.*, vol. 9, no. 4, pp.

3857–3869, 2023, doi: 10.1007/s40747-022-00838-y.
32. D. Ocampo, F. B. C, D. Castillo, T. M. L, and M. A. N, "A New Local Area Network Attack through IP and M," pp. 198–205, 2013.
33. "AbuseIPDB - IP address abuse reports." https://www.abuseipdb.com/ (accessed Mar. 06, 2024).
34. "SANS Institute." https://www.sans.org/cyber-security-training-overview/?msc=main-nav (accessed Mar. 06, 2024).
35. P. Kumar and S. Rana, "Development of modified AES algorithm for data security," *Optik (Stuttg).*, vol. 127, pp. 2341–2345, 2016, doi: 10.1016/J.IJLEO.2015.11.188.
36. A. M. Carrington *et al.*, "Deep ROC Analysis and AUC as Balanced Average Accuracy, for Improved Classifier Selection, Audit and Explanation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, pp. 329–341, 2021, doi: 10.1109/TPAMI.2022.3145392.
37. Z. Wen, R. Zhang, and K. Ramamohanarao, "Enabling Precision/Recall Preferences for Semi-supervised SVM Training," *Proc. 23rd ACM Int. Conf. Conf. Inf. Knowl. Manag.*, 2014, doi: 10.1145/2661829.2661977.
38. C. K. I. Williams, "The Effect of Class Imbalance on Precision-Recall Curves," *Neural Comput.*, pp. 1–5, 2020, doi: 10.1162/neco_a_01362.
39. J. Zhang and S. Li, "A Review of Machine Learning Based Species' Distribution Modelling," *Proc. - 2017 Int. Conf. Ind. Informatics - Comput. Technol. Intell. Technol. Ind. Inf. Integr. ICIICII 2017*, vol. 2017-Decem, pp. 199–206, 2017, doi: 10.1109/ICIICII.2017.76.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 24 Issue 1 Version 1.0 Year 2024
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cyber Security Test Platform Establishments and Cyber-attacks Practice

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

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.

GJCST-E Classification: LCC Code: QA76.9.A25

Strictly as per the compliance and regulations of:

Cyber Security Test Platform Establishments and Cyberattacks Practice

Dr. Chetanpal Singh [α], Ass. Professor Rahul Thakkar [σ], Jatinder Warraich [ρ], Numan Ahmed [ω] & Vimal B. Patel [¥]

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.

I. Introduction

a) 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.

Author α σ ρ ω ¥: e-mails: Chetanpal.singh2@rmit.edu.au, rahul.thakkar@vit.edu.au, Jatinder.warraich2@rmit.edu.au, Numan.ahmed@rmit.edu.au, vim_patel84@yahoo.com

b) 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.

c) Research Aims & 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.

d) 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?

e) 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.

II. Literature Review

a) 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.

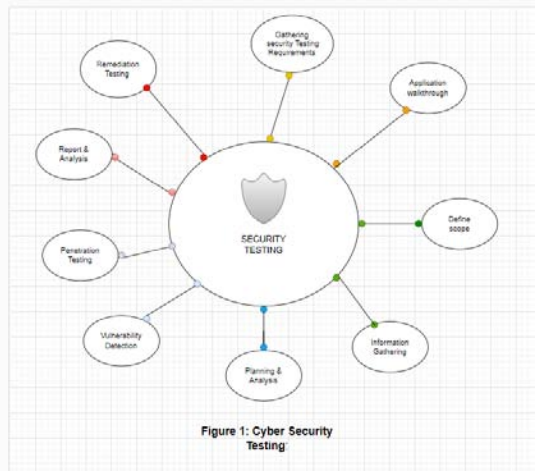


Figure 1: Cyber Security Testing

Source: [9]

Figure 1: Cyber Security Testing

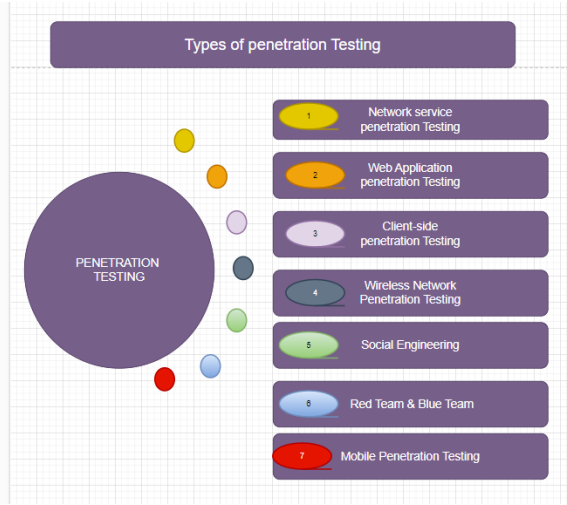
As per the opinion of [9], a breach in the security of the servers can expose the personal and essential information of companies across the wo; It is considered a serious issue and has a strong impact on the financial conditions of the companies. Cybersecurity is very much essential to protect the business 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.

b) Essentiality of Cyber Security Test Platforms aand 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.



Source: [13}

Figure 2: Penetration Testing

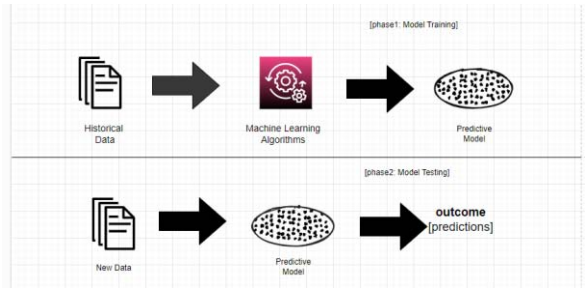
From the opinion of some authors [13], in North American blackouts, the lack of system awareness is considered to be the main reason behind the blackouts, which highlights the essentiality of the analysis of cyber-attacks in terms of maintaining a reliable and stable power supply operation. The cyber 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.

c) 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.

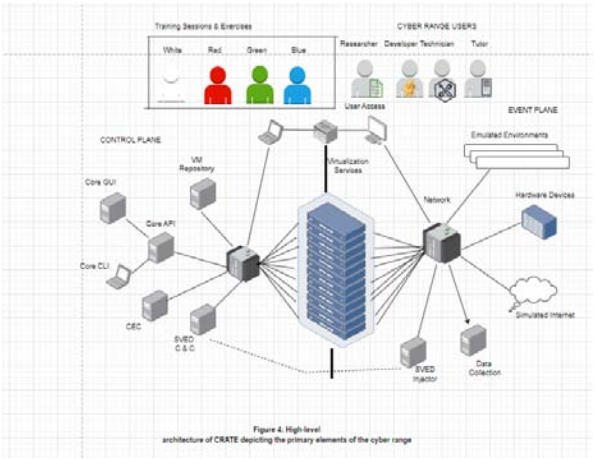
From the opinion of [17], in the present days, machine learning modelling has been applied in a practical way, especially in the matter of cyber security.



Source: [17]

Figure 3: General Structure of the ML-Based Predictive Model Considering both the Training and Testing Phase

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.



Source: [18]

Figure 4: High-level Architecture of CRATE Depicting the Primary Elements of the Cyber Range

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.

d) 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.

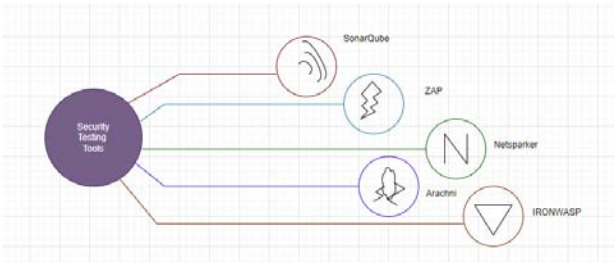
Vega is a web security scanner and a web security testing platform, and it helps to test web application securities. The application of Vega helps to identify any SQL injection and also other vulnerabilities in the server of any company. It helps to find cross-site scripting which can be reflected or 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.



Source: [22]

Figure 5: Security Testing Tools

III. Research Methodology

a) 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.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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

g) 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.

h) 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-BImplementations: System-atic 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.

i) Data Validity and Reliability

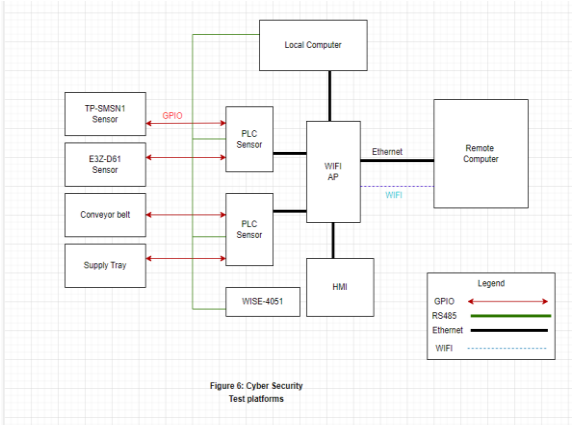
The procedure of the research has been related to the mixed approach to the performance of the study. The researched information has been separated into two kinds of efforts such as primary and secondary. The secondary literature review was established on the basis of the journals of Google scholars. 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.

j) 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.

IV. Result & 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.



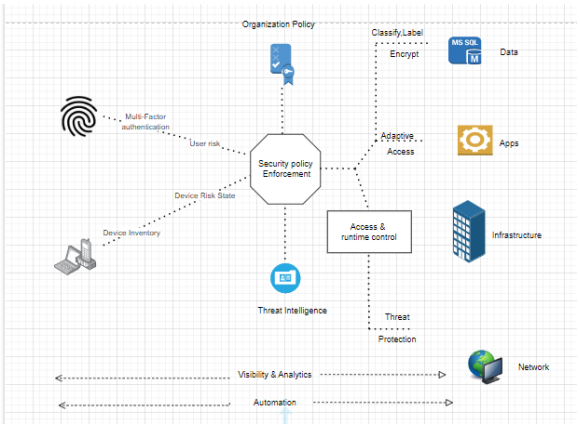
Source: [28]

Figure 6: Cyber Security Test Platforms

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.



Source: [18]

Figure 6: Cyber Security Statistics

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 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 Références Referencias

1. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards Insighting Cybersecurity for Healthcare domains: A comprehensive review of current practices and trends. *Cyber Security and Applications*, 100016.
2. Ahmadi, A., Nabipour, M., Taheri, S., Mohammadi-Ivatloo, B., & Vahidi Nasab, V. (2022). A new false data injection attack detection model for cyberattack resilient energy forecasting. *IEEE Transactions on Industrial Informatics*, *19*(1), 371-381.
3. Sun, C. C., Cardenas, D. J. S., Hahn, A., & Liu, C. C. (2020). Intrusion detection for cybersecurity of smart metres. *IEEE Transactions on Smart Grid*, *12*(1), 612-622.
4. Gasiba, T., Lechner, U., Pinto-Albuquerque, M., & Porwal, A. (2020). 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 6* (pp. 67-83). Springer International Publishing.
5. Karagiannis, S., Maragkos-Bel Maps, E., & Magkos, E. (2020). 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.
6. Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., ... & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, *20*(24), 7148.
7. Aldawood, H., & Skinner, G. (2019, 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* (pp. 110-115).
8. Hanif, Y., & Lallie, H. S. (2021). 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*, *67*, 101693.
9. Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organisational Cybersecurity Journal: Practice, Process and People*, *1*(1), 24-46.
10. Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1), mzaa117.
11. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, *105*, 102248.
12. Karimipour, H., Dehghantanha, A., Parizi, R. M., Choo, K. K. R., & Leung, H. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *IEEE Access*, *7*, 80778-80788.
13. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.
14. Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., ... & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, *20*(24), 7148.
15. Awamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., & Al-Rawashdeh, G. (2020). Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology*, *63*(5), 7894-7899.
16. Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. *Digital War*, *1*, 164-170.
17. Sarker, I. H. (2022). Ai-based modelling: Techniques, applications and research issues towards automation, intelligent and smart systems. *SN Computer Science*, *3*(2), 158.
18. Gustafsson, T., & Almroth, J. (2021, 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.
19. Thaqi, R., Vishi, K., & Rexha, B. (2022). Enhancing Burp Suite with Machine Learning Extension for Vulnerability Assessment of Web Applications. *Journal of Applied Security Research*, 1-19.
20. Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). A Survey on Web Application Penetration Testing. *Electronics*, *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 2021, Virtual Event, December 8–9, 2021, 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. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, *105*, 102248.
23. Newman, M., & Gough, D. (2020). Systematic reviews in educational research: Methodology, perspectives and application. *Systematic reviews in educational research: Methodology, perspectives and application*, 3-22.
24. Ryder, C., Mackean, T., Coombs, J., Williams, H., Hunter, K., Holland, A. J., & Ivers, R. Q. (2020). Indigenous research methodology–weaving a research interface. *International Journal of Social Research Methodology*, *23*(3), 255-267.
25. Hafidz, M. A., & Elihami, E. (2021). Learning The Nonformal Education Through Research Methodology: A Literature Review. *Jurnal Edukasi Nonformal*, *2*(1), 47-55.
26. Fowler, D.S., Bryans, J., Cheah, M., Wooderson, P. and Shaikh, S.A., 2019, 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)* (pp. 1-8). IEEE.
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., 2019, February. Isaac: The idaho cps smart grid cybersecurity testbed. In *2019 IEEE Texas Power and Energy Conference (TPEC)* (pp. 1-6). IEEE.
28. Khandker, S., Turtiainen, H., Costin, A. and Hämäläinen, T., 2021. 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*, *58*(4), pp.2702-2719.
29. Munaiah, N., Rahman, A., Pelletier, J., Williams, L. and Meneely, A., 2019, September. Characterizing attacker behavior in a cybersecurity penetration testing competition. In *2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)* (pp. 1-6). IEEE.
30. Matheu-García, S.N., Hernández-Ramos, J.L., Skarmeta, A.F. and Baldini, G., 2019. Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards & Interfaces*, *62*, pp.64-83.
31. Ramirez, R., Chang, C.K. and Liang, S.H., 2023. PLC Cybersecurity Test Platform Establishment and Cyberattack Practice. *Electronics*, *12*(5), p.1195.
32. Kim, J., Kim, K. and Jang, M., 2019, May. Cyber-physical battlefield platform for large-scale cybersecurity exercises. In *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1-19). IEEE.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 24 Issue 1 Version 1.0 Year 2024
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

MERN Stack-based Multi-Seller E-Commerce Site

By Azizul Hakim Rafi

Abstract- In almost every way, web development has been getting better and better over the last ten years. During this time, a number of frameworks and libraries came out, which made it much easier and faster to make a web app. Over the last decade, the LAMP stack (Linux, Apache, MySQL, and PHP) and Java-based applications have dominated web development. It was challenging for a single developer to construct a web application by using these stacks because of how complex they were. As the field of web development matured, MERN-an acronym for "MongoDB," "Express," "React," and "Node JS"-emerged as the dominant stack in 2023. Due to the relative simplicity of the technologies comprising this stack, a single developer may effectively handle both the front-end and back-end of the application. MongoDB, which is a no-SQL database; Express, which is a framework of Node JS used in back-end development; React, which is a JavaScript library used in front-end development; and NodeJS, which is an environment for JavaScript; these are the components that make up the MERN stack.

Keywords: *react, node.js, javascript, express.js, MERN stack.*

GJCST-E Classification: *LCC: QA76.76.H94*

Strictly as per the compliance and regulations of:

MERN Stack-based Multi-Seller E-Commerce Site

Azizul Hakim Rafi

Abstract- In almost every way, web development has been getting better and better over the last ten years. During this time, a number of frameworks and libraries came out, which made it much easier and faster to make a web app. Over the last decade, the LAMP stack (Linux, Apache, MySQL, and PHP) and Java-based applications have dominated web development. It was challenging for a single developer to construct a web application by using these stacks because of how complex they were. As the field of web development matured, MERN-an acronym for "MongoDB," "Express," "React," and "Node JS"-emerged as the dominant stack in 2023. Due to the relative simplicity of the technologies comprising this stack, a single developer may effectively handle both the front-end and back-end of the application. MongoDB, which is a no-SQL database; Express, which is a framework of Node JS used in back-end development; React, which is a JavaScript library used in front-end development; and NodeJS, which is an environment for JavaScript; these are the components that make up the MERN stack.

The main goal of this thesis is to learn about the MERN stack and build a fully working multi-vendor e-commerce web application that is a laptop reselling platform. This application has a user-friendly interface, sign-up, and login systems that are JWT (JSON Web Token) secured. JWT is used to protect every API that this app uses. So that users don't have any problems, it's now easier to buy and sell used laptops. The interface and functionality of this app are designed with the user's ease of use in mind. The beta version of this is already completed and hosted in the server.

Keywords: react, node.js, javascript, express.js, MERN stack.

I. Introduction

In 1989, while working as a fellow at Europe's CERN Laboratory, Tim Berners-Lee proposed a computer platform that would make it easier for scientists working in different regions of the world to work together. For this reason, in 1990, the Hypertext Markup Language (HTML) was developed. The primary building block that was used to construct the World Wide Web and is still in use today is the Standard Generalized Markup Language (SGML) served as the primary inspiration for the development of HyperText Markup Language (HTML). Programmers were provided with the tools necessary to design web page layouts that could be viewed and interacted with wherever on the web thanks to the norm. [1]

In today's globally linked digital environment, organizations need tools that allow for global growth. An organization would be severely lacking without a web application. There are several benefits to having a robust online presence, including increasing exposure to your brand and facilitating online sales. Now that firms are establishing themselves online, a web application is essential for reaching international audiences. Despite the rise of mobile apps, a well-built online application is still vital to meeting modern business requirements. Websites are now thought of as cross-platform apps because their style and content can be changed. Programmers were able to create and share information more easily and share information with businesses when they made Web applications. [2]

This thesis has two sections. The first section is more theoretical, and it explains the rationale behind each of the technologies utilized to create this website. The thesis's second section delves into the nuts and bolts of putting the e-commerce web app into action.

This thesis focuses on the development of a Multi-vendor E-commerce web app for reselling secondhand laptop computers. This app has three user types: admin, seller, and buyer (by default). Where sellers may list their old laptops for sale and buyers can book them first. Stripe payment handles payment integration. According to their roles, various types of users will see a unique set of dashboard options. The website's database houses all of its data, which is then processed by the server and shown by the app.

II. Introduction to Mern Stack

The MERN Stack is a set of robust and reliable technologies that may be used to build scalable master web applications, complete with server, front-end, and database components. Building full-stack computer applications can be done much more quickly and easily with the help of JavaScript. The MERN Stack is an open-source technology that provides a user-friendly, comprehensive JavaScript framework for building dynamic, dynamically responsive applications and webpages.

The 3-tier Architecture system at MERN is mostly made up of three layers:

- As a front-end tier, the Web
- The server is in the middle.
- The database is the backend.

Author: e-mail: rafiazizul96@gmail.com

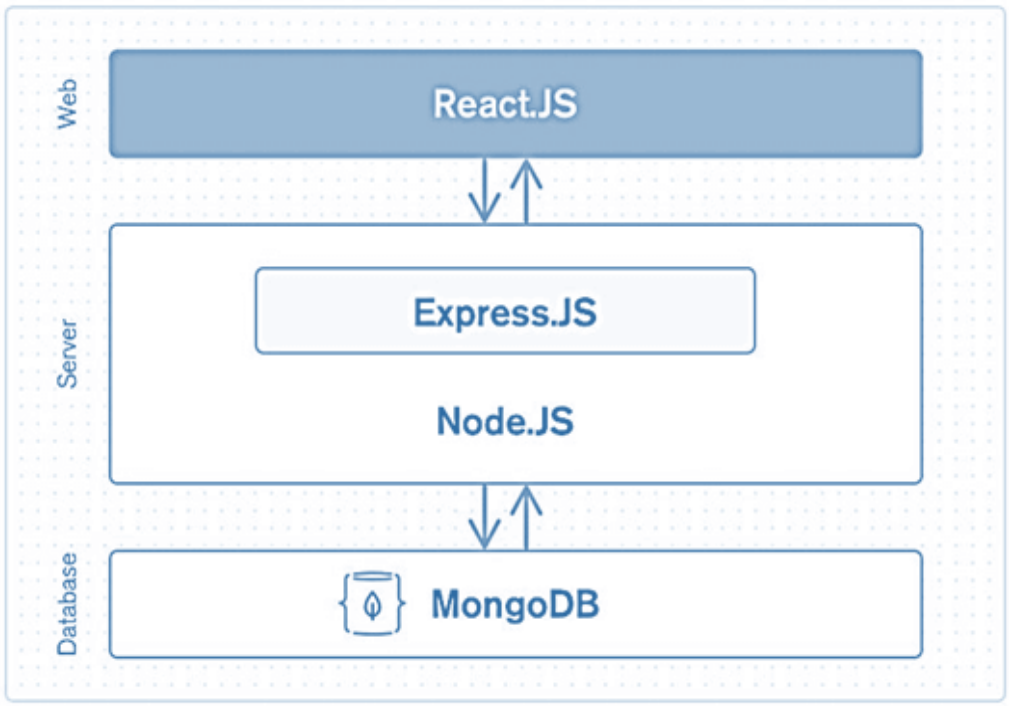


Figure 1: MERN Architecture

- *Front-End Tier*- The MERN stack's front end is almost entirely built on top of React.js. It is a well-liked front-end JavaScript library that is freely available to the public. It is well-known for its ability to produce interactive client-side applications. With React, you can build sophisticated user interfaces out of simpler building blocks. It also links those intricate user interfaces to the server-side information stored there. Both mobile apps (using React Native) and online apps (using React) can be built with React. React facilitates and supports code reuse, which has several advantages and saves a lot of work. It allows users to build complex web applications that dynamically update their website's content without requiring a page refresh.
- *Server or Middle Tier* - It's the next layer down from the top and is managed mostly by Express.js and Node.js, both of which are part of the MERN stack. Because Express.js maintained the Server-side framework within the Node.js server, both parts manage it simultaneously. One of the most popular JavaScript frameworks for backend development is called Express.js. It makes it considerably simpler and easier for programmers to launch powerful APIs (Application Programming Interface) and web servers. In addition to this, it enhances the capabilities of the HTTP (HyperText Transfer Protocol) objects that are available in Node.js. On the other hand, Node.js is a vital component in its own right and is an essential component overall. Outside of a web browser, you may execute JavaScript by using this server environment, which is available for free and uses open source. Because it is constructed on a foundation of JavaScript, Node.js is a potent tool that can be used for fast constructing online services and mobile applications.
- *Database as Back-End Tier* - A database's major job is to store information relevant to your application, such as content, statistics, information, user profiles, comments, and so on; this important component of the MERN Stack was developed by MongoDB. The primary function of its data storage is security. It keeps meticulous records, which it returns to the user at their request. The database serves as its primary storage medium. To ensure that users can always access their data in the event of a system failure, it creates a copy of their data in many locations. This suggests that the relational table model is not at the foundation of MongoDB. On the other hand, it offers a novel approach to information storage and retrieval. As the most widely used open-source document-oriented database, Mongo DB is a type of database known as a NoSQL (NoSQL or Non-Structured Query Language). NoSQL often refers to a non-relational database that stores data without a predefined structure or standard relational tables. MongoDB is a document-oriented document store, as opposed to a relational database's rows and columns. [3]

Why choose MERN stack

- *Open-source technology*- Because it is an open-source code that is being built upon by technology specialists throughout the world, MERN is favored by startups. The MERN stack is an open-source framework for developing high-performance websites and online applications. Because there is no vendor lock-in with open-source software, there will be no additional hurdles to go through if you ever decide to make a switch or upgrade.
- *You can find free samples online*- You may save a ton of time by using one of the many free templates you can get online. Customizing a theme would have taken three times longer than downloading one. If you have any problems along the process, professionals will be there to support you. There are online forums for many platforms where you may ask questions and obtain comments on your code from other developers who are also using that platform. Having knowledgeable guides to lead the way makes learning a breeze.
- *Easy to use*- With such thorough documentation, implementing the underlying technology is a breeze. Its accessibility and ease of use make it a great option for those just starting out in the field of web development. It might be difficult for developers to select which of the numerous accessible tools is worth their time. Because there are fewer pieces to these instruments to learn and master, they are more straightforward to pick up and utilize. A MERN stack project is a great place to start if you're new to web programming since it provides a solid foundation in the fundamentals without overwhelming you with advanced concepts straight away. [4]

a) Node.js

Simply referred to as "Node," the JavaScript runtime environment is compatible with multiple operating systems. Programmers don't have to go through the trouble of learning two new languages because JavaScript can be applicable to both client and server-side application development. This is because Node is so widely utilized for server-side development. Despite its many misnomers, Node is only a JavaScript runtime and not a programming language or framework for creating applications.

The V8 JavaScript engine is included in Node, the same engine that is utilized by Google Chrome and other web browsers. It is a cross-platform application that can operate on macOS, Linux, Windows, and other operating systems because it is developed in C++. JavaScript code is interpreted and carried out by the engine. It is possible for it to function outside of the context of a browser by having it embedded in a C++ application or by having it built as a stand-alone program. The V8 engine conducts a just-in-time (JIT) compilation of JavaScript, which speeds up execution.

```
// index.js

const http = require('http');

const hostname = '127.0.0.1';
const port = 3000;

const server = http.createServer((req, res) => {
  res.statusCode = 200;
  res.setHeader('Content-Type', 'text/plain');
  res.end('Hello, programmer!');
});

server.listen(port, hostname, () => {
  console.log(`Server running at http://${hostname}:${port}/`);
});
```

Figure 2: Here is a Sample of a Node.js-Compatible JavaScript File

The Figure 2. shows how to write a simple JavaScript file (index.js) for the Node system. The HTTP (Hypertext Transfer Protocol) package for Node.js is loaded at the beginning of the script. The module has many classes and methods for putting together an HTTP server.

After installing Node JS in your device, you can run the program by the command “node index.js”. The JavaScript code tells Node to do two very simple things:

- When a browser on the local machine connects to http://localhost:3000, it will show a message. The message says, "Hello, programmer!"
- When the command is run, send a message to the console. The message says, "Server running at http://127.0.0.1:3000/."

How does Node.js works

A Node program is run by a single process. In contrast to the majority of server-side programs, Node.js does not initiate a new thread for each request. So, a Node server can handle thousands of connections at the same time without having to deal with problems caused by threads running at the same time or the extra work that multithreading brings. Node.js is driven by events and runs in the background. The usual approach of receive, process, send, wait, and receive is not used when writing code for the Node environment. Instead, Node uses an event loop to handle requests as they come in and stack up in the event queue. Small requests are handled one after the other without waiting for answers.

This is a change from the most common models, which run bigger, more complicated operations and handle multiple threads at the same time, with each thread waiting for the right answer before going on.

Ryan Dahl, who made Node.js, says that it has a big edge over these other models. Node doesn't stop I/O (input/output) processes like older methods do. This is due in large part to the fact that Node methods don't directly do I/O, which helps get rid of the chance of stopping. Blocking only happens when synchronous methods are used in the normal Node library, but this is more of an exception than the rule. This makes Node a good choice for real-time apps with a lot of work going on at the same time.

Node is thought to be easy to learn, just like JavaScript. It is used by a lot of people and has a big, busy group of users who support it. Node is also asynchronous, event-driven, and doesn't block, which means it can handle the kind of real-time concurrency that is widespread in many web apps and online services today. Node works well for real-time apps like chats, live services, Internet of Things (IoT) services, and single-page apps. [5]

i. *Node.js Server Architecture*

Rather than waiting for one operation to finish before starting another, Node.js allows applications to continue working despite input/output delays. The technique is known as asynchronous I/O.

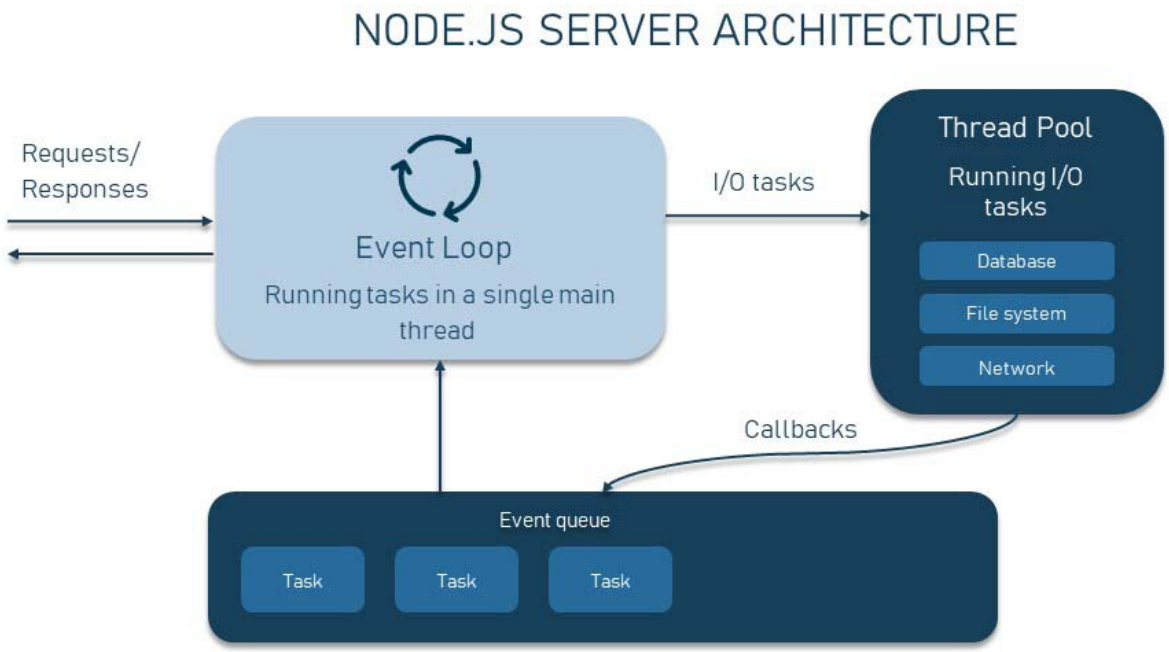


Figure 3: The Inner Workings of Node.js

Non-blocking, I/O and request processing that doesn't wait - Imagine that a function needs to get data from the network, handle it, and then return the result. In the world of synchronous operations, this means that the program would have to wait until the function gets data and does its work, which would block other activities.

Callback and promises- Callbacks are functions that are called when I/O operations have finished. They can be added to the event queue and served in the main thread once it's clear. Callbacks can be nested in other callbacks, which makes code more complicated and can lead to "callback hell," which we'll talk about below.

Event Loop- pulls in fresh callbacks and checks the event queue for pending requests after previous tasks have completed. The cycle starts over again after that. [6]

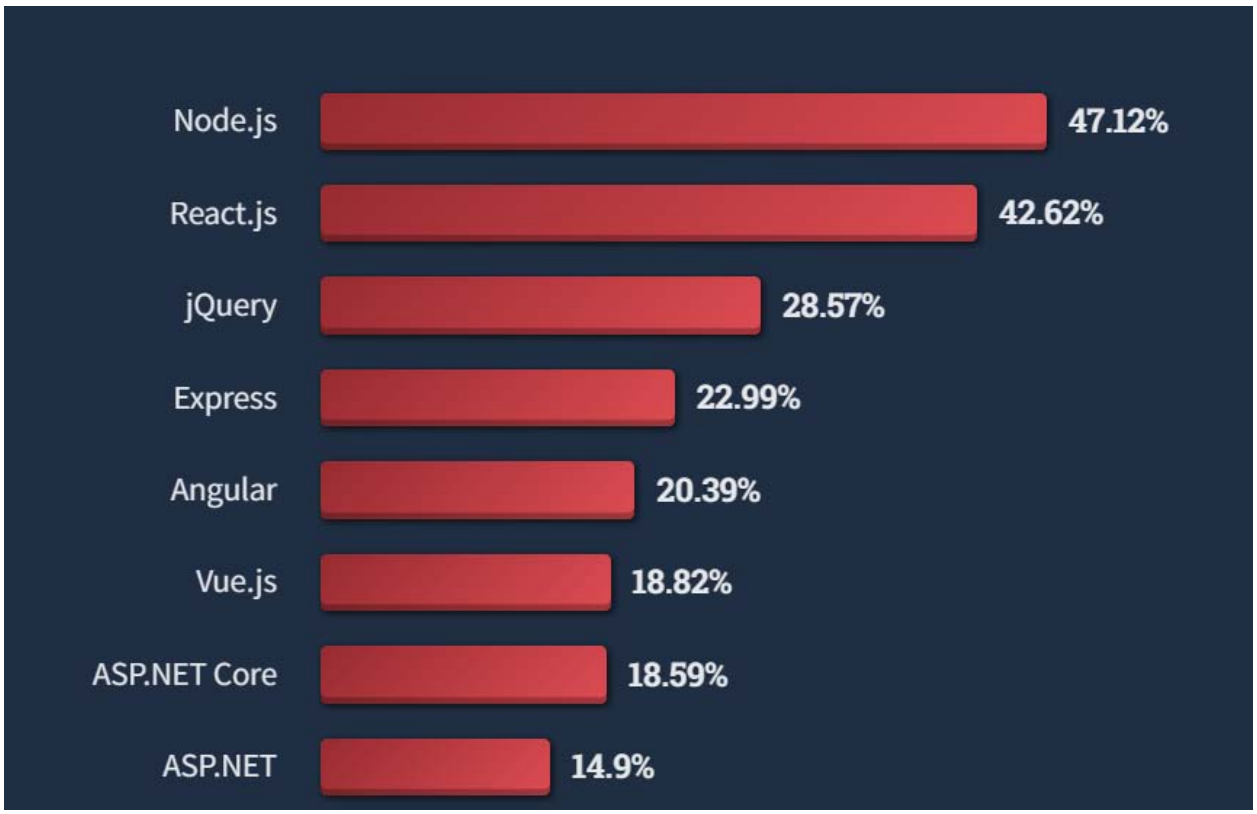


Figure 4: Stack Overflow Survey [7]

Figure 4. shows Professional Developers and students of computer programming utilize the web technologies Node.js and React.js most frequently.

ii. *Node Modules*

Node.js modules are functionally independent chunks of code that communicate with third-party programs. Any number of files or folders can make up a module. Modules are used a lot by programmers because they can be reused and because they can break up a complicated piece of code into doable chunks. The http module is one of the most often used core components since it can be used to build an HTTP client. [8]

iii. *Node Package Manager (NPM)*

Node Package Manager is what "npm" refers to. It's a repository and reference guide for applications written in JavaScript. To facilitate package installation and dependency management, npm also provides command-line utilities. Over 11 million developers rely on npm since it is free and easy to use. One may even call it significant. They are free and widely used because of their open-source nature. Over a million packages may be found on npm. [9]

There are two ways that NPM may carry out the operation: globally and locally. When NPM is run in global mode, it affects all Node.js apps on the computer, whereas when NPM is run in local mode, it only impacts the application in that directory. The node_modules subdirectory contains all the NPM-installed modules. Express.js will be installed in the root folder of your project by the command *npm install express*. The ExpressJS folder will be created within the node_modules folder where the installation will take place. The bundle is included in the package.json file in

the property dependencies. We can use a package by using require function along with module name

$ npm install <module name>

const express = require('express') [10]

In a JavaScript/Node project, the package manager (here, npm) generates a package.json file that serves as the project's root directory. A package.json file may be created with the help of the npm init command. After that, you'll be prompted to provide some metadata about your project, such as:

- Name – project name
- Version - latest major release.1.0.0, 1.2.3, etc.) minor.patch format
- Description – project description
- License - the terms of the license that governs your project, so others may understand how they might make use of it.

Sometime if we need to update a package, we can do it by giving the command "npm update <package name>". Following command will update the package to latest version available. [9]

```
{
    "name": "laptopcity",
    "version": "1.0.0",
    "description": "",
    "main": "index.js",
    "scripts": {
        "start": "node index.js",
        "test": "echo \"Error: no test specified\" && exit 1"
    },
    "keywords": [],
    "author": "",
    "license": "ISC",
    "dependencies": {
        "cors": "^2.8.5",
        "dotenv": "^16.0.3",
        "express": "^4.18.2",
        "jsonwebtoken": "^8.5.1",
        "mongodb": "^4.12.0",
        "nodemon": "^2.0.20",
        "stripe": "^11.1.0"
    }
}
```

Figure 5: Package.Json File of Laptop City (Multi-Vendor E-Commerce Web App)

Figure 5 shows all the packages use in this e-commerce project under dependencies property such as cors, dotenv, stripe etc.

b) Express.js

The most widely used web framework for Node.js is called Express.js. People have called it the de facto standard server platform for Node.js because it is used to make web apps and APIs.

Building a Node.js application's backend from start can be hard and take a long time. Writing the business logic for an application is what really matters, but developers waste time on mundane tasks like setting up ports and route handlers. When creating online applications, developers can save time with tools like Express.js.

i. *Handling Requests*

Web applications have traditionally relied on a web server to passively await HTTP requests from clients. In response to an HTTP request, the server will pass control to the route handler it determines is most appropriate. Creating a route handler from scratch in Node is often not the easiest thing to do. Express, fortunately, has features that allow you to define which function is invoked in response to a certain combination of HTTP verb (GET, POST, PUT, etc.) and URL pattern (Route).

Figure 6: An Express Server Demonstrating Routing in Express

The following figure is a code snippet example of an Express route. Express is a web application framework, and this line of code declares that all GET requests to the /greeting route will be processed by a function that returns "Hello World!" to the client.

ii. *Middleware*

Express is an opinion-free system, which means that it doesn't tell writers how to organize their code. Instead, it lets them do it however they want. One place where this lack of a point of view is clear is in the use of software. Middleware lets tasks be done on requests and replies as they move through the routes. Express apps use it a lot. Middleware can be used at both the application level and the route level, and it can also be linked to other pieces of middleware. You can add almost any suitable software to the request handling chain, and you can do it almost any way you want.

Express provides us with several built-in middleware such as express .static, express. json etc.

```
// middleware
app.use(express.json()); // parses json payloads

function verifyJWT(req, res, next) {
    const authHeader = req.headers.authorization;
    if (!authHeader) {
        res.send(401).send({ message: 'Invalid authorization ' });
    }

    const token = authHeader.split(' ')[1];
    jwt.verify(token, process.env.ACCESS_TOKEN_SECRET, (err, decoded) => {
        if (err) {
            res.send(403).send({ message: 'Forbidden Access ' });
        }
        req.decoded = decoded;
        next();
    });
}

// get categories
app.get('/categories', verifyJWT,  async (req, res) => {
    const query = {};
    const categories = await categoriesCollection.find(query).toArray();
    res.send(categories);
});
```

Figure 7: Express app Demonstrating Middle Functions

Typically, an Express route will include middleware and a route handler function. The example that follows demonstrates an Express router that applies middleware to every HTTP GET request sent to the /categories route. To determine if a user has a valid JWT before allowing access to the /categories route, a middleware function called verifyJWT is utilized in this case. The verifyJWT middleware will run when a user navigates to the /categories URL, and then the user will be given access to the API data if the user has valid JWT. [11]

c) *MongoDB*

MongoDB's document-oriented NoSQL design makes it well-suited for storing massive datasets. MongoDB stores information not on tables but in collections and documents. Documents, which are comprised of key-value pairs, are the primary unit of data storage that may be utilized while working with MongoDB. Collections are like the tables in a relational database since they hold collections of documents and activities. The database known as MongoDB first appeared somewhere in the middle of the 2000s.

i. *MongoDB Features*

- Each database has its own collections, and those collections have their own documents. The number of fields in each document may vary. Each file may have a unique size and include varying amounts of information.
- Developers will find the document structure more familiar since it mirrors the way they build classes and objects in their preferred programming languages. In contrast to tables, developers typically claim that their classes have a hierarchical structure based on key-value pairs.
- In MongoDB, a predefined schema is not required for the rows (or documents). The fields may be made dynamically instead.
- The data format of MongoDB makes it easy to store arrays and represent complex structures like hierarchies.
- Environments built on top of MongoDB scale quite well. Clusters have been defined by businesses all over the globe; some of them use 100 or more nodes and store millions of records in their databases.

ii. *Key components of MongoDB Architecture*

- *_id*- This field is required for all documents in MongoDB. The _id column in a MongoDB document stores a unique identification. The _id field is the primary key in the document's database. If the _id column is not supplied while creating a new document in MongoDB, the database will construct one automatically. Each document in the collection will be given a random number between 1 and 24 by Mongo DB.

- *Collection* - A group of MongoDB records is called a collection. When working with RDMSs like Oracle or Microsoft SQL Server, a collection may be thought of as a table. A set is contained entirely inside one database.
- *Database* - Like a table container in a relational database management system, this one store collections. Separate directories and files are created on the file system for each database. There may be more than one database on a MongoDB server.
- *Document* - In MongoDB, a "document" refers to an individual record in a collection. In turn, the document will be made up of labels for fields and their associated data.
- *JSON* - JavaScript Object Notation describes this format. This format is designed to make it easy for humans to read and understand structured data. Many languages now have built-in support for JSON. [12]

iii. *MongoDB Data Modelling*

A fully functional database system cannot be created without first creating a data model. Data models are mostly used to provide visual information about the potential link between two or more data elements. Petabyte-scale data repositories, which contain data from across corporate divisions and teams (including sales, marketing, and beyond), will rely heavily on the layout/design.

Adding new data models or restating the definitions of existing ones is a continual and dynamic process that necessitates many feedback loops and direct interaction with the stakeholders.

Skillful data modelling requires the use of formalized schemas and procedures to guarantee a consistent, repeatable, and reliable method of managing an organization's business operations and its data resources.

When experts in the data industry begin the process of constructing data models in MongoDB, they are faced with the decision of whether or not to embed the information or to keep it distinct in a collection of documents. As a result, there are two different ideas involved in effective MongoDB data modelling:

1. *The Embedded Data Model* - Data modelling in MongoDB that's built right in When there is a connection between two data sets, data modelling is used, specifically a denormalized data model. As a result, documents may maintain a unified structure thanks to the embedded data model's established links between data pieces.
2. *The normalized Data Model* - Relationships between data components or documents are modelled with the use of object references in a normalized data model. Because of the efficiency gains from using this approach, many-to-many connections may be recorded with little repetition of information. [13]

iv. *MongoDB Atlas*

MongoDB Atlas is a novel, multi-cloud database solution that has been crafted by the proficient developers of the company. With Atlas, you can build scalable, high-performance, global apps on any cloud platform with no effort because to its simplified database deployment and management. [14]

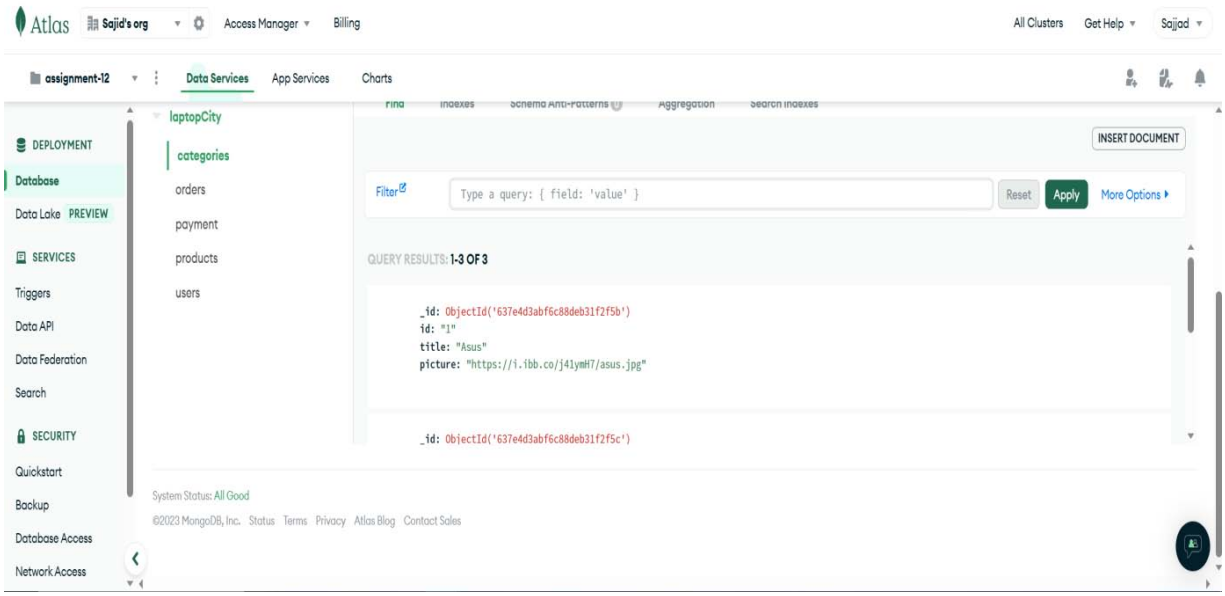


Figure 8: Screenshot of the MongoDB Atlas

v. *Advantages and disadvantages of MongoDB*

The reasons MongoDB is favoured by majority of developers are:

- *Developer UX*- MongoDB was designed to provide programmers a pleasant experience while making applications. They like that this database works with several languages, including Ruby on Rails, Python, PHP, Swift, Scala, Rust, and JavaScript. MongoDB also provides its users with top-notch technical assistance. With the cloud-hosted version of MongoDB, Atlas, the database's use has become even more intuitive.
- *Scalability and Transnationality*- Scalability is one of the best things about MongoDB. Thanks to its scale-out architecture, you can create apps that remain stable despite sudden increases in user volume. As a result, the workload is dispersed across a large fleet of less powerful but cheaper computers. Because MongoDB has come up with so many new ideas, it can handle a huge number of read and write tasks. Sharding in MongoDB makes it possible to store information groups in one place even though the information itself is saved on many computer clusters. This is very different from the relational database design, which is limited because it grows to make computers faster and more powerful as it grows.

Nothing is perfect, with many advantages as mentioned above, MongoDB have some limitations

- *Joins not Supported* - MongoDB is not like a linear database in that it doesn't allow joins. Still, you can use the joins method by adding it to your code by hand. But it could slow down the process and hurt efficiency.
- *High Memory Usage* - Each value-key pair in MongoDB is given a name. There is also data redundancy since joins are not functional. This causes memory to be used more than it needs to be. [15]

d) React.js

Facebook developed the React.js framework, which is a JavaScript framework and tool It is free for anyone to use. It's used to create real-time user interfaces and online applications with a fraction of the code required by standard JavaScript.

Using react, we partition the user interface of the application by developing a number of reusable components. Each component is a stand-alone portion of the user interface; nevertheless, the combination of numerous components results in the whole user interface.

In an application, the primary duty of the react component is to manage the view layer, similar to the role of the V in the model-view-controller (MVC) paradigm. It does this by offering the best and most efficient way to display. React.js recommends that developers divide up complex user interfaces into smaller, more manageable pieces that can be reused independently. By doing so, the ReactJS framework improves upon the DOM manipulation capabilities of JavaScript while maintaining their speed and efficiency. This makes it possible to load web pages faster and make web applications that are very active and flexible. [16]

React.js History

In 2011, Facebook had a lot of users and had to do something hard. It wanted to give people a better experience by making an interface that was livelier and more sensitive, as well as fast and high-performing.

One of Facebook's software workers, Jordan Walke, made React so that it could do just that. React made the development process easier by giving developers a more organized way to make dynamic, interactive user experiences with reusable parts. [16]

Why use React.js

- *Dynamic applications can be created easily*- When compared to JavaScript, where coding can rapidly become difficult, react simplifies the creation of dynamic web apps by requiring less code and offering greater functionality.
- *Improved Performance*- The creation of web applications is sped significantly thanks to React' s utilization of Virtual DOM. Virtual DOM compares the current states of the components to their earlier states and changes only the parts of the Real DOM that have changed. So, this increases the page speed and performance as with every change the page doesn't rerender This is different from how most web applications work, which update all of the components again.
- *Reusable Components*- Every React project is made up of components, and most applications have many. These components come with their very own set of controls and logic, and they may be used in a variety of places across the application. Because of this, the amount of time needed to create the application is drastically reduced, and the quality of the code produced is much improved. [17]

i. *Virtual-DOM*

The genuine Document Object Model (DOM) is replicated in its entirety as the virtual DOM. When the state of a application changes, the real Document Object Model (DOM) does not change. Instead, the virtual DOM is changed in its place.

When new UI elements are added, a fake DOM that looks like a tree is made. Each part of this tree is a branch. A new virtual DOM tree is created whenever the state of one of these parts shifts. Next, the newly

constructed tree is "diffed" against the existing virtual DOM tree.

Once this is complete, the virtual DOM will determine the most efficient means by which to implement these modifications in the real DOM. This ensures that as little of the original DOM as feasible is used. This means that making changes to the actual DOM will be easier and quicker.

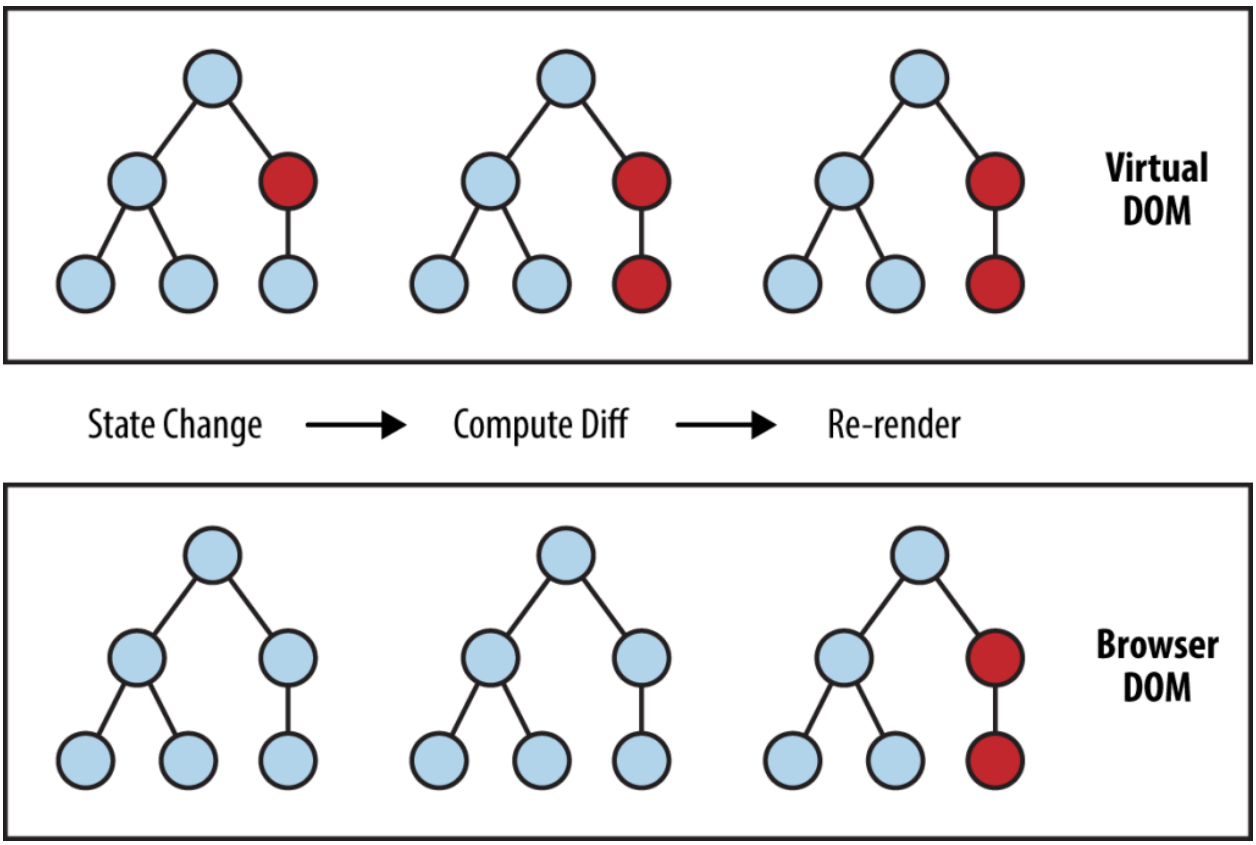


Figure 9: Virtual Dom and Diffing Process

In figure 9 Nodes that have changed is denoted in red circles. These nodes represent the changed UI components. [18]

ii. *JSX (JavaScript XML)*

An add-on for React known as JSX, which stands for "JavaScript XML," enables users to write JavaScript code in a format that is visually similar to HTML. To put it another way, JSX is a syntax that is utilized by React and is comparable to HTML. It is an extension of ECMAScript that enables HTML-like grammar to coexist alongside code written in both JavaScript and React. The syntax is used by preprocessors, sometimes known as transpilers, such as babel, to convert code that is similar to HTML into normal JavaScript objects that a JavaScript engine can read.

Like regular HTML, JSX uses properties with HTML elements. The way properties are named in JSX is different from how they are named in HTML. For example, a class in HTML becomes className in JSX because class is a protected term in JavaScript. [19]

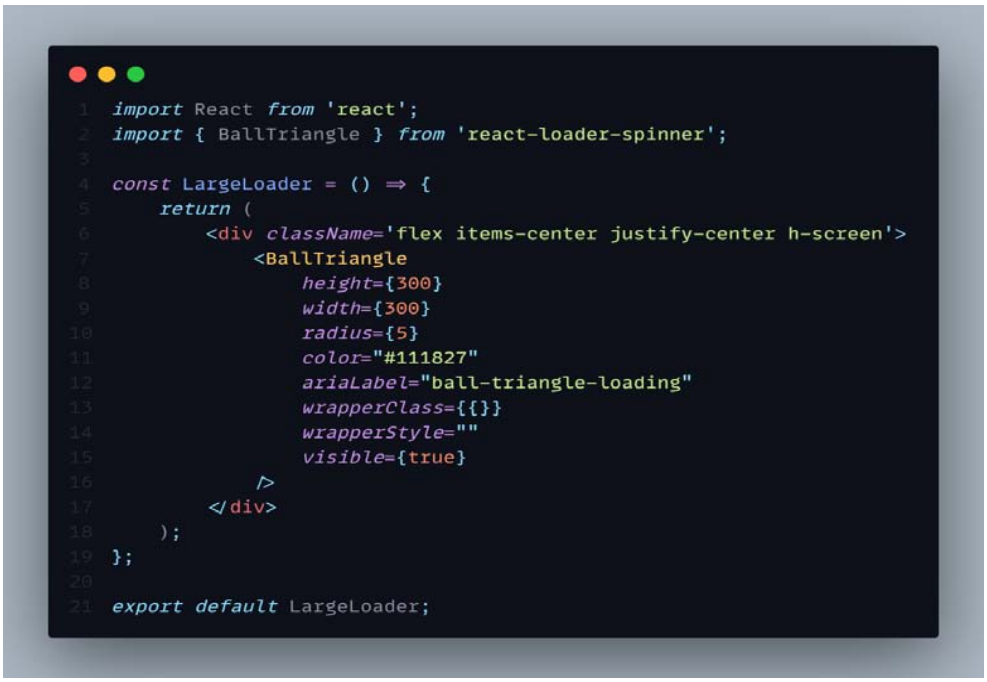
```jsx
// Payment.js
const Payment = () => {
    const product = useLoaderData();

    const { name, productName, price } = product;

    return (
        <div className="w-[85%] mx-auto mt-10">
            <Helmet>
                <title> Payment - Laptop City </title>
            </Helmet>
            <div>
                <h1 className="text-4xl font-extrabold text-center">Pay for you Product</h1>
                <h1 className="text-center text-xl font-bold mt-3">
                    Congratulations {name} for buying{' '}
                    <span className="text-[#00A4CF] font-extrabold text-2xl">{productName} </span>
                    at a reasonable price of <span className="text-green-700">৳{price}</span> taka
                </h1>
            </div>
```

Figure 10: A JSX File in React Application

iii. *Components*

Previously for a single page application developer had had to write thousands of line of code. Those application followed traditional DOM structure which made debugging code a complex process. For a single error, developer had had to check each line of code and make the necessary changes. So that component-based approach was made to overcome this problem. By component approach it means breaking down the whole application into small components.

Components are the most important parts of a React program. It makes it much easier to build user interfaces. Each component is in the same place, but it works separately from the others. They all come together in a parent component, which is the final UI of your app. [20]



```jsx
import React from 'react';
import { BallTriangle } from 'react-loader-spinner';

const LargeLoader = () => {
    return (
        <div className='flex items-center justify-center h-screen'>
            <BallTriangle
                height={300}
                width={300}
                radius={5}
                color="#111827"
                ariaLabel="ball-triangle-loading"
                wrapperClass={{}}
                wrapperStyle=""
                visible={true}
            />
        </div>
    );
};

export default LargeLoader;
```

Figure 11: A Loader Component

iv. *Pros and Cons of the React*

React.js Advantages

- *Component based architecture*- React components are a highly sophisticated portion of a web page that can be independently produced, maintained, and even reused. They were made possible by the introduction of these components. Your web page can be broken up into several different components, each of which is capable of functioning on its own. Any one of them can be updated independently of the others. This allows for a great deal of modularity and flexibility in the way that it may be used with other parts of the web application to enhance its functionality.
- *Hight Performance*- The ability to dynamically load information in response to user input without reloading the entire page is made possible by React' s component-based architecture, making it ideal for building scalable Single Page Applications. However, this might not be ideal. Imagine being required to update DOM after every change that was brought about by the user's interaction on the web page. If your webpage is complicated and have multiple UI elements, it might result in a significant speed decrease.
- To get around this problem, React uses a concept called Virtual DOM, which is essentially a replica of your actual Document Object Model. All the changes brought on by user interaction or other events are now handled by the virtual DOM before the real DOM is updated (if the intelligence of React deems it necessary, of course).

React.js Disadvantages

- *High Pace of Development*- This is probably the most talked about reason not to use React. React is not only a tool that is growing quickly, but it is also changing quickly, which means that its developers have to change the way they write code. Customers in many fast-evolving sectors are eager to adopt more dependable technology and solutions. Again, this relies on the team's level of expertise and their ability to win clients over to the idea of using React.
- *Not a full-featured framework*- Developers don't enjoy what they may have in a fully equipped framework like Angular, despite the fact that React is a powerful JavaScript library with a set of interactive and helpful capabilities necessary to create large-scale apps. If you look at the MVC (Model View Controller) architecture, react only manages the view part. You will need more packages and tools to work with Controller and Model. The resulting code could not be well-structured or follow any particular patterns. While more organized and manageable solutions may be found in frameworks like Angular, which offer the full set of MVC features. [21]

III. Implementation of Laptop City – a Multi-Vendor e-commerce Web Application

a) Project Overview

Laptop City is a C2C (Consumer-to-Consumer) online retailer. E-commerce that is of the consumer-to-consumer (C2C) variety refers to any electronic transactions of products or services that are carried out between individual customers. In most cases, these dealings are executed by utilizing the services of a third party, which is responsible for providing the digital marketplace in which the deals are executed. Multiple merchants can list and sell their used Laptops on the Laptop city platform. [22]

Laptop City is an online marketplace for the purchasing and selling of reconditioned laptops. This website caters to one of three distinct categories of users. There is a choice for the user role throughout the registration process. If a user wishes to sell things on this Laptop City platform, they can opt to take on the "Seller" position instead of the "Buyer" role, which is the default setting.

Laptops can be booked and purchased by users having the buyer role. Stripe has been incorporated into the payment system. Users that have the seller role have the ability to add products, delete products that they have uploaded, and advertise their own products. If a product is being advertised, it will be displayed on the advertise section in home page; however, if there aren't any product for advertisement, the advertisement section won't be visible. The Product will be automatically removed from the application once the product is sold out. Admin are a special category of user. The administrator can see who has the Buyer and Seller roles and can remove them from the database if necessary. The admin can delete an item that a Buyer has reported.

b) *Home Page*

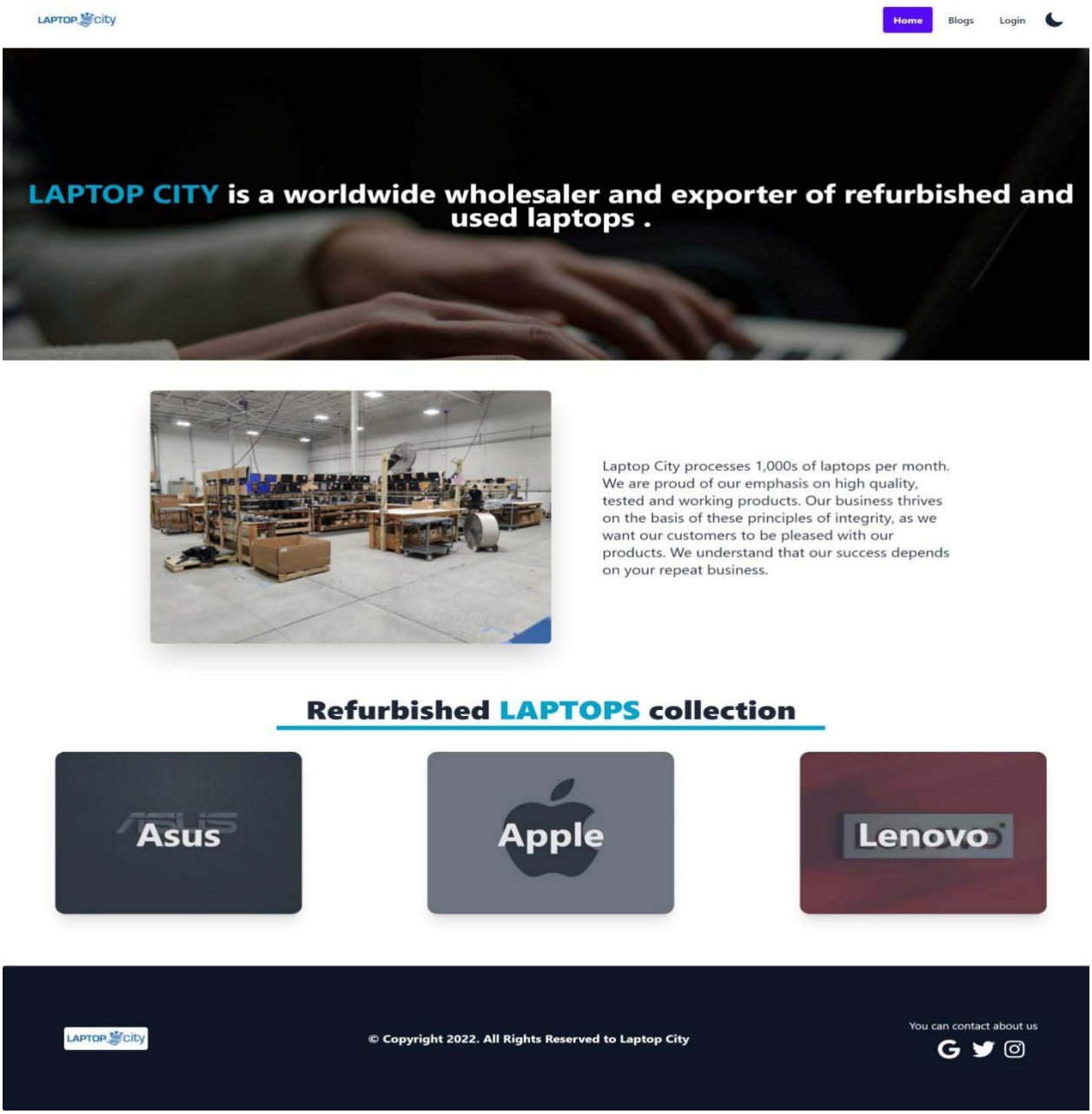


Figure 12: Landing Page of Laptop-City

The app's landing screen is depicted in Figure 12. There are four distinct parts to the homepage, one of which is an advertisement portion that appears only when relevant products are being promoted. Information regarding Laptop City can be found in the first two sections. And finally, the categories part of the reconditioned laptops can be found in the third area. There are just three laptop varieties that can be used with this platform right now. There's Lenovo, Apple, and Asus. The moon icon can be found in the upper right-hand corner of the navigation bar, allowing the user to choose between a dark mood and a light mood. In the event that the website is already set to a dark mood, a sun icon will be displayed; clicking on it will allow you to go back to the light mood. If the user is already logged in, the login button is replaced by a dashboard and a logout option.

Fig 13: Home Component

Figure 13 illustrates the primary home page component, which consists of the Banner, Info, Advertisement, and Categories components respectively. Because the Home page is made up of reusable components, the complexity of the code will be minimized, and it will be much simpler to debug. And each of these smaller components might be utilized wherever we see fit on our own accord.

c) Authentication System

A user's credentials are required for login or registration. Firebase is in charge of all authentication in Laptop City.

Most apps require users to be able to verify their identity. When an app has a user's credentials, it may save their information securely in the cloud and provide them with a consistent, personalized experience across all of their devices. You can ensure that your app's users are who they say they are with the help of Firebase Authentication, a suite of back-end services, developer-friendly SDKs, and pre-built UI components. A wide range of alternative techniques, such as passwords, phone numbers, and huge federated identity providers like Google, Facebook, and Twitter, may all be utilized to successfully complete the authentication process. Firebase Authentication is easy to connect with a custom backend because it uses common protocols like OAuth 2.0 and OpenID Connect and communicates directly with other Firebase services. [23]

i. *Sign Up*

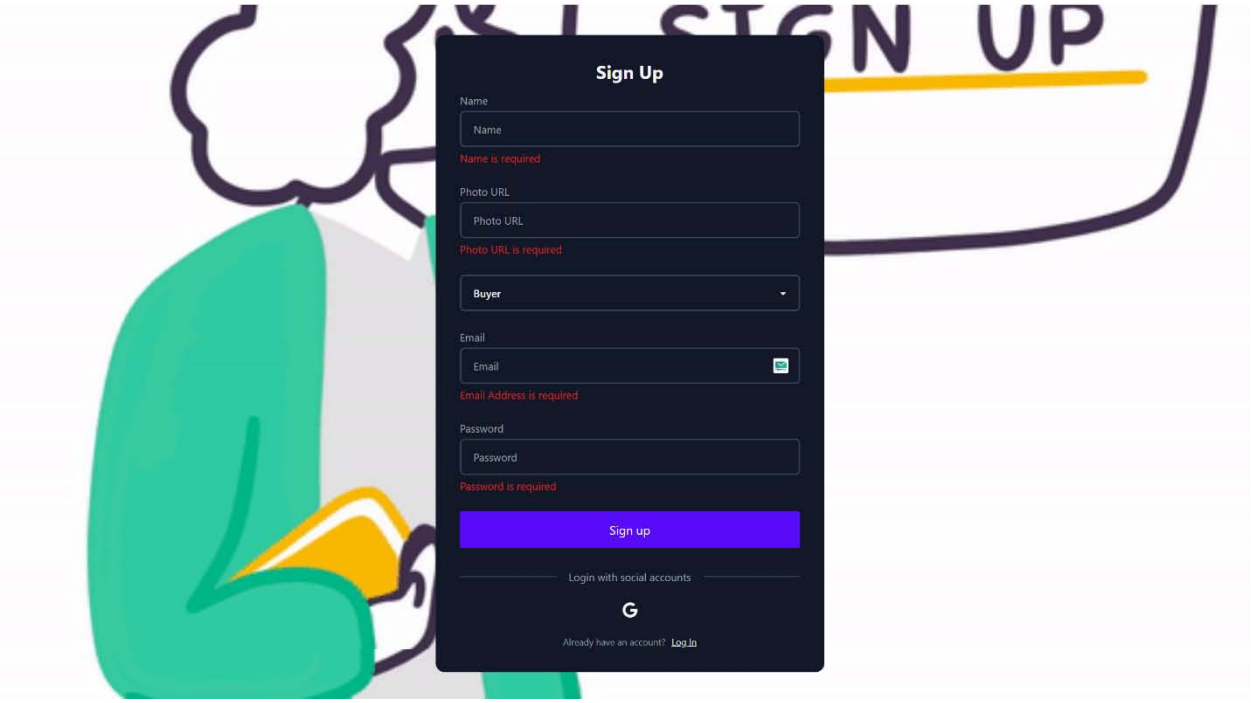


Figure 14: Signup form Screen

Users are required to sign up for an account before they may sell or purchase things in Laptop City. As seen in Figure 14, a user must fill out their name, photo URL, email address, and password boxes before they can register. The "Buyer" position will be assigned to the user by default, although the "Seller" role is an option. The React Hook form is used to do validation on the form. Users can sign up for accounts on this website by selecting the Google Sign Up option by clicking on the Google logo. After providing all of the required information, the user will click the sign-up button; if the sign-up procedure is successful, the user will be returned to the homepage; however, if a problem happens, a toast will be displayed with the error message. If the person has already signed up, they can click on Log in to go to the login form.

```
const handleSignup = (data) => {
    setSignupError('');
    setLoad(true);
    createUser(data.email, data.password)
        .then((result) => {
            const user = result.user;
            toast.success('registered successfully');

            const userInfo = {
                name: data.name,
                email: user?.email,
                role: data?.userStatus,
            };

            updateUserProfile(data.name, data.photoUrl)
                .then(() => {
                    setAuthToken(userInfo);
                    navigate('/');
                })
                .catch((err) => {
                    setSignupError(err.message);
                });
            setLoad(false);
        })
        .catch((err) => {
            setSignupError(err.message);
            setLoad(false);
        });
};
```

Figure 15: Code Snippet for Sign up

Due to the utilization of a React-hook form, there is no requirement for a state for each individual field. After filling out the form with all of the required information and then clicking the Sign-up button, the loader state will be set to true. This indicates that a loader will be displayed during the sign-up process. Next, the function create User, which is provided by firebase, is called, which calls the update User Profile function, which is also provided by firebase. Finally, the update User Profile function will call set AuthToken, which will be responsible for storing the user data in the database and assigning a token that will be kept in the local storage. After successfully registering, the user will be taken to the homepage of the site. In the event that there is a problem, the loading state will be changed to false; thus, the loading process will be halted, and a notice bar will be displayed alongside an error message.

```
const setAuthToken = (user) => {
    const currentUser = {
        name: user?.name,
        email: user?.email,
        role: user?.role,
    };

    fetch(`https://assignment-12-server-pi.vercel.app/users/${user?.email}`, {
        method: 'PUT',
        headers: {
            'content-type': 'application/json',

        },
        body: JSON.stringify(currentUser),
    })
        .then((response) => response.json())
        .then((data) => {
            console.log(data);
            localStorage.setItem('laptop-city-token', data.token);
        });
};
```

Figure 16: Code Snippet of Setauthtoken Function

ii. *Sign In*

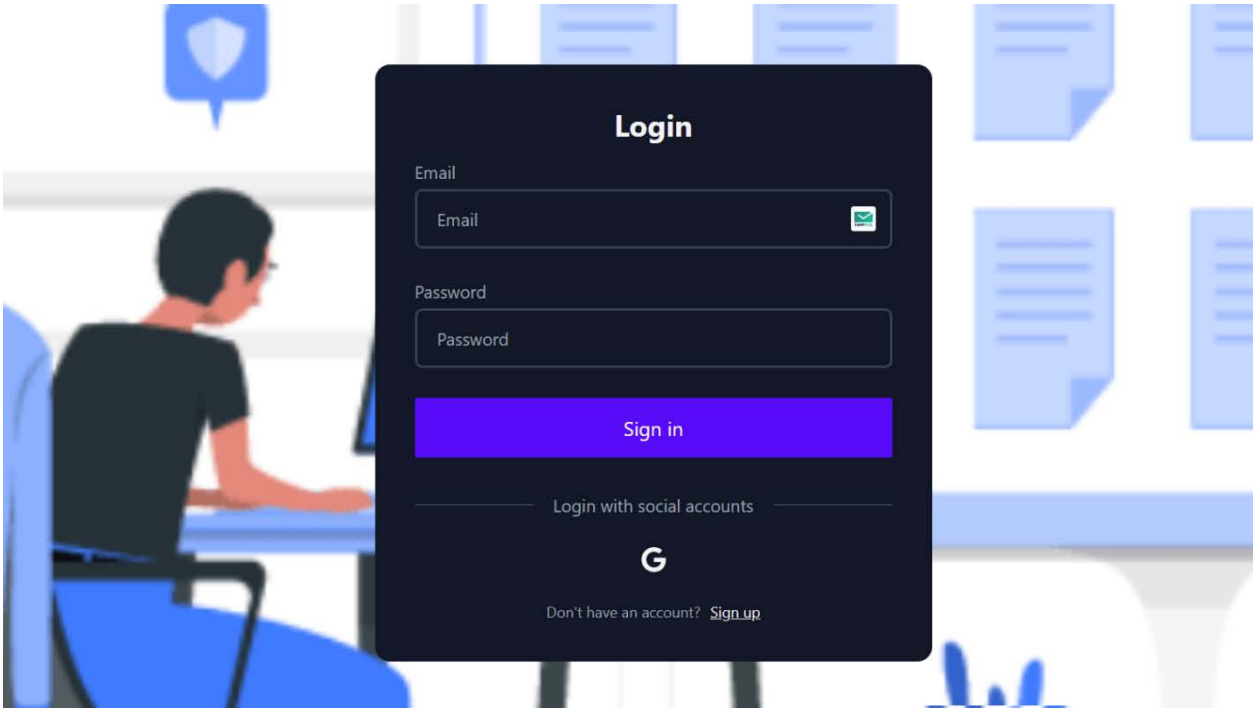


Figure 17: Login form Screen

The sign-up form and the login form are quite identical. To log in, the person only needs to give their email address and password. After successful login user will be redirected to the page they wanted to visit previously.

```
const handleLogin = (data) => {
        setLoginError('');
        console.log(data);
        setLoad(true);
        signIn(data.email, data.password)
            .then((result) => {
                const user = result.user;
                console.log(user);
                const userInfo = {
                    name: user?.displayName,
                    email: user?.email,
                };
                setAuthToken(userInfo);
                toast.success('Login Successful');
                setLoad(false);
                navigate(from, { replace: true });
            })
            .catch((err) => {
                setLoginError(err.message);
                setLoad(false);
            });
    };
```

Figure 18: Code Snippet of Login

After the user has completed all of the required fields, clicking the sign-in button will cause the sign in function to be called. This function requires the user's email address and password as parameters. Next, the setAuthToken function will be called, which will determine whether or not the user exists in the database. If the user is found in the database, a notification bar will appear with a message indicating success, and the browser will then reroute the user to the website that they had intended to visit before.

d) Dashboard

i. *Admin Dashboard*

Figure 19: Admin Dashboard Screen

Figure 19 depicts the admin dashboard, where the administrator can view all sellers and all buyers and delete the records of these sellers and buyers from the database. Additionally, the Admin is able to view all of the items that have been reported and delete them if they so choose.

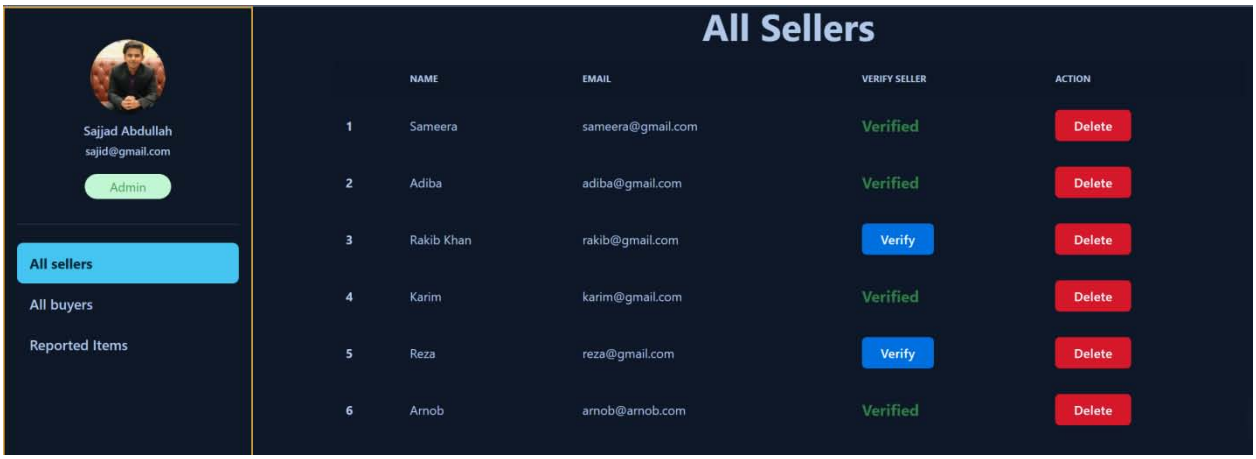


Figure 20: All Sellers Screen

As shown in Figure 20, the admin has visibility over all users who have the "Seller" role. By clicking the appropriate buttons, the admin can delete sellers and verify existing ones.

```
// verify user
const handleVerifyUser = (user) => {
    fetch(`https://assignment-12-server-pi.vercel.app/verify-user/${user._id}`, {
        method: 'PUT',
        headers: {
            authorization: `Bearer ${localStorage.getItem('laptop-city-token')}`,
        },
    })
        .then((res) => res.json())
        .then((data) => {
            console.log(data);
            refetch();
            toast.success(`${user.name} verified successfully`);
        });
};
```

Figure 21: Verify Seller Code Snapshot

The handle Verify User method will be triggered immediately following the clicking of the Verify button. This function will make a call to the API, which has a query parameter for user id. PUT is the approach that is utilized because existing users in the database are the only ones that can be verified. In the event that the specified data does not already exist in the database, the PUT method will generate it, and in this instance, it will update the user data that was previously stored. If the operation was successful, the refetch function will be invoked. This method is supplied by React query, and if it is successful, it will immediately show the update on the screen without requiring the user to refresh the page. The seller's information in the product card will be accompanied by a blue badge if the user has been verified.

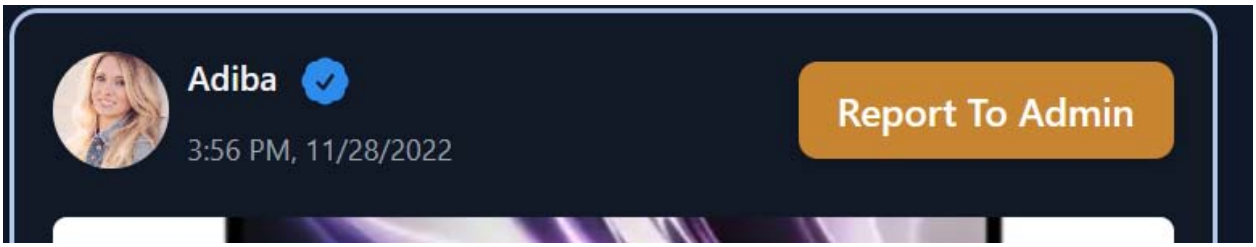


Figure 22: Verified Seller Badge Along with Seller Information

The administrator has access to view all of the products that have been reported and can remove them from the database.

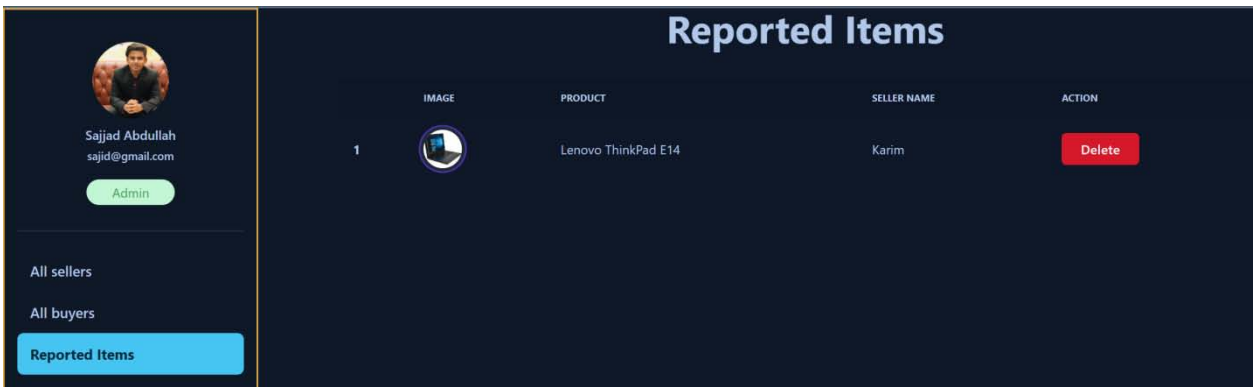


Figure 23: Reported Items Screen

Users can report a product by using the option that says "Report to Admin," as demonstrated in Figure 22. After that, Admin will be able to view the reported items in the manner depicted in Figure 23. The things that have been reported will be laid out in a table fashion and will include all of the pertinent product information, including a picture of the item, its name, the seller's name, and a button to delete the item.

```
const {
        data: reportedItems = [],
        isLoading,
        refetch,
    } = useQuery({
        queryKey: ['reportedItems'],
        queryFn: () =>
            fetch('https://assignment-12-server-pi.vercel.app/reported-items', {
                headers: {
                    authorization: `Bearer ${localStorage.getItem('laptop-city-token')}`,
                },
            }).then((res) => res.json()),
    });
```

Figure 24: Reported Items Fetching Snapshot

As show in figure 24 data is fetched using React query. React Query is a data-fetching tool that helps your React application get, cache, synchronize, and update server state. Before we get into the details of React Query, it is important to know what the server state is. [24]

ii. *Seller Dashboard*

Figure 25: Seller Dashboard Screen

As can be seen in figure 25, a user with the seller role has the ability to both add products and look at all of the products that they have created.

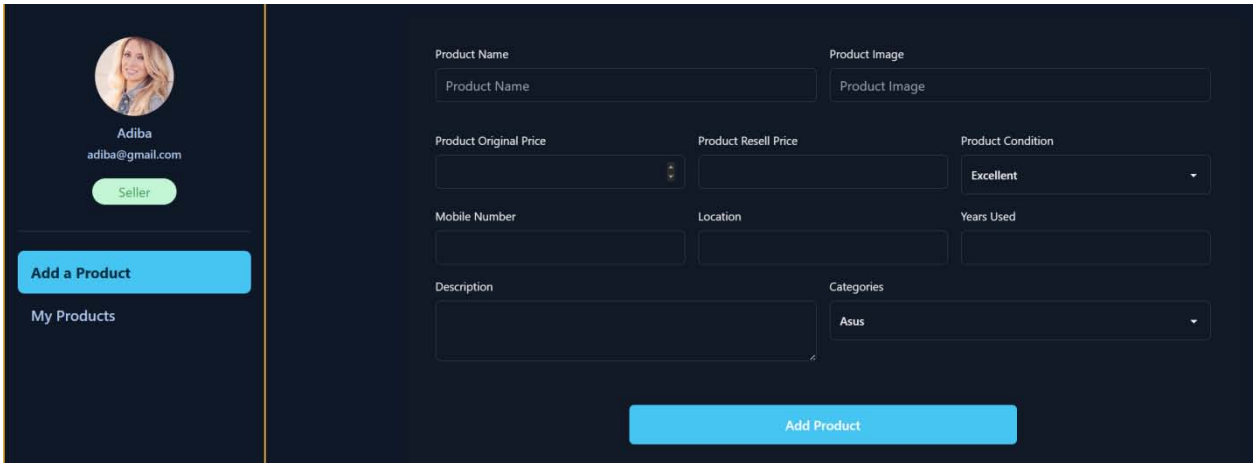


Figure 26: Add Product form Screen

A user with the seller role can add a product by filling out the Add a Product form with the appropriate information, as illustrated in Figure 26. All of this information collected from the fields will be saved in the database, along with the time at which that particular product was developed. Each field in this form must to be filled out by the seller in order to add the product, and none of the entries can be left blank.

```
const handleAddProduct = (data) => {
        const category = categories.find((category) => category.title === data.category);

        const categoryId = category._id;

        const product = {
            productsName: data.productName,
            picture: data.picture,
            originalPrice: data.originalPrice,
            resellPrice: data.resellPrice,
            mobileNumber: data.mobileNumber,
            location: data.location,
            productCondition: data.condition,
            yearsUsed: parseFloat(data.yearsUsed),
            postedTime: date,
            userName: user?.displayName,
            description: data.description,
            category: data.category,
            categoryId: categoryId,
            userEmail: user?.email,
            userPhoto: user?.photoURL,
        };
        console.log(product);
        fetch(`https://assignment-12-server-pi.vercel.app/products`, {
            method: 'POST',
            headers: {
                'content-type': 'application/json',
                authorization: `Bearer ${localStorage.getItem('laptop-city-token')}`,
            },
            body: JSON.stringify(product),
        })
            .then((res) => res.json())
            .then((data) => {
                console.log(data);
                if (data.acknowledged) {
                    toast.success(`product added successfully`);
                    navigate('/dashboard/myProducts');
                }
            });
    };
```

Figure 27: Add Product Code Snapshot

As can be seen in Figure 27, the POST function is implemented since it allows a new document to be generated in MongoDB. In addition to all of the information from the fields of the Add product form shown in Figure 26, the database will also store the time the product was produced, the seller's name, the seller's email address, and a photo of the seller. A toast bar will be displayed with the phrase "product added successfully" if the procedure is successful, and the seller will then be navigated to the My Products page.

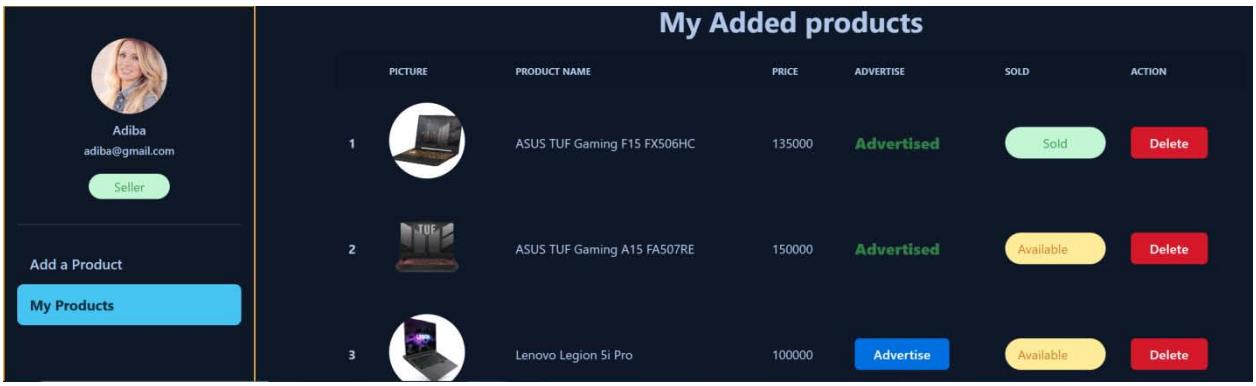


Figure 28: My Products Screen of Seller Dashboard

If the product was added without any errors, the seller will be sent to the page seen in Figure 28 entitled "My products."

My products page includes a table with information about the products, including product image, name, price, and product status (whether the product is sold or available), as well as a delete button and an advertise button. When the advertise button is clicked, the specific product will be displayed in the advertisement section of the home page. The seller is able to delete a particular product by clicking the delete button on the My products page.

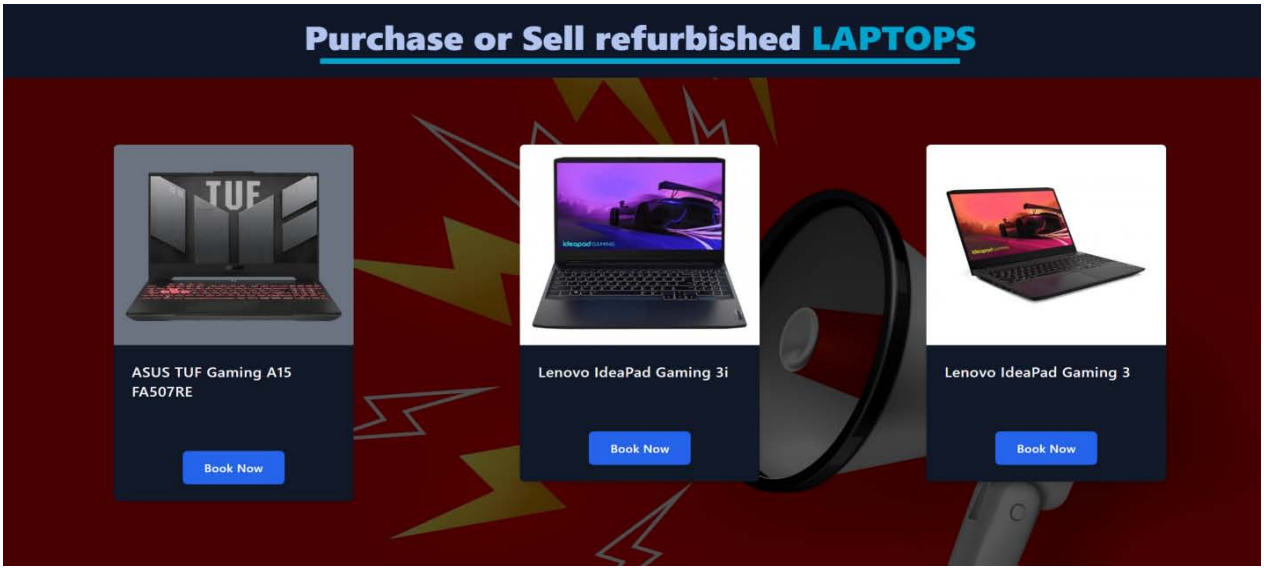


Figure 29: Advertisement Screen

As can be seen in Figure 28, the seller promoted ASUS TUF Gaming A15 FA507RE by hitting the advertise button. As a direct consequence of this, the laptop in question was advertised in the advertisements section in home page. Given that this laptop had not yet been purchased, it was featured in the advertisements section.

3.4.3 Buyer Dashboard

Figure 30: Buyers Dashboard Screen

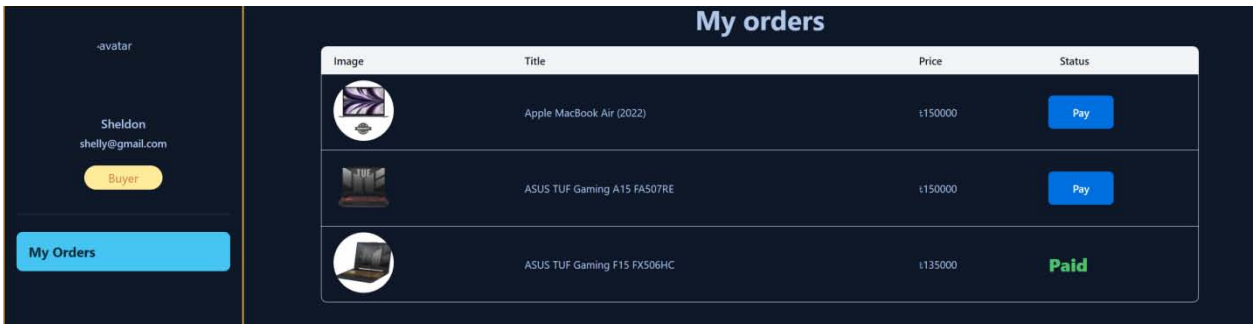


Figure 31: My Orders Page Screen

Users that have the buyer role are able to view all of the items they have booked. Users are required to make a booking for the product before they may purchase a laptop. The product will then be presented in the format of a table, as shown in Figure 31, with information on the product including an image of the product, its name, its price, and a button to make a payment. In the event that the user has already paid for the laptop, the status will be updated to paid rather than displaying the pay button.

e) Products Page

The Products page includes all of the laptops that are relevant to the category that is now selected. If you want to view the product page, you will need to sign in first. If the user has not already registered or logged in, they will be taken to the login page when they attempt to access the product page.

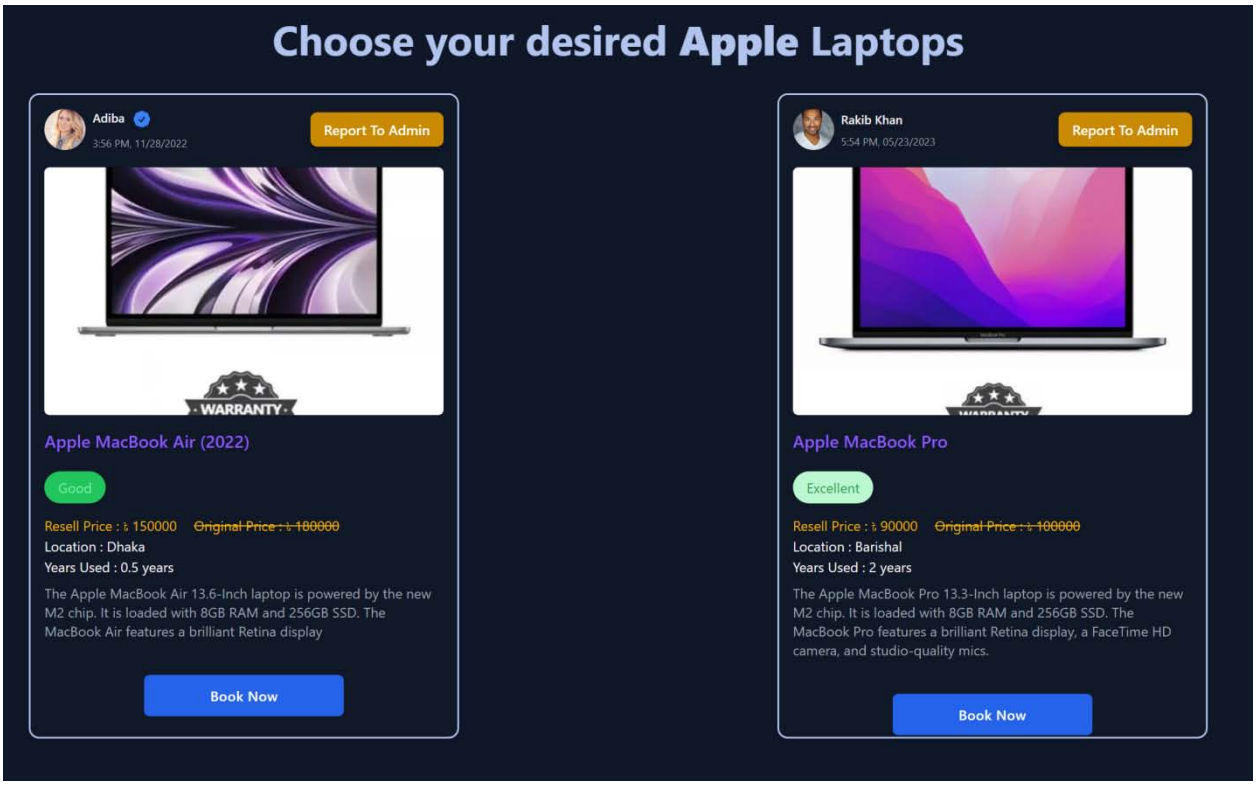


Figure 32: Product Page

As can be seen in figure 32, the products page includes all of the products that are pertinent to the category that has been selected. Each product card has a button at the top of the card that allows the user to report the product to the admin, as well as the seller's image, name, the day and time the product was posted, and so on. In addition, a product image, the product's initial price, its current resell price, its condition, its location, the number of years the product has been used, a brief description of the product, and a book now button is included on a single product card. There will be a blue badge next to the seller's picture if the seller has been verified.

i. *Booking and Purchasing Laptop*

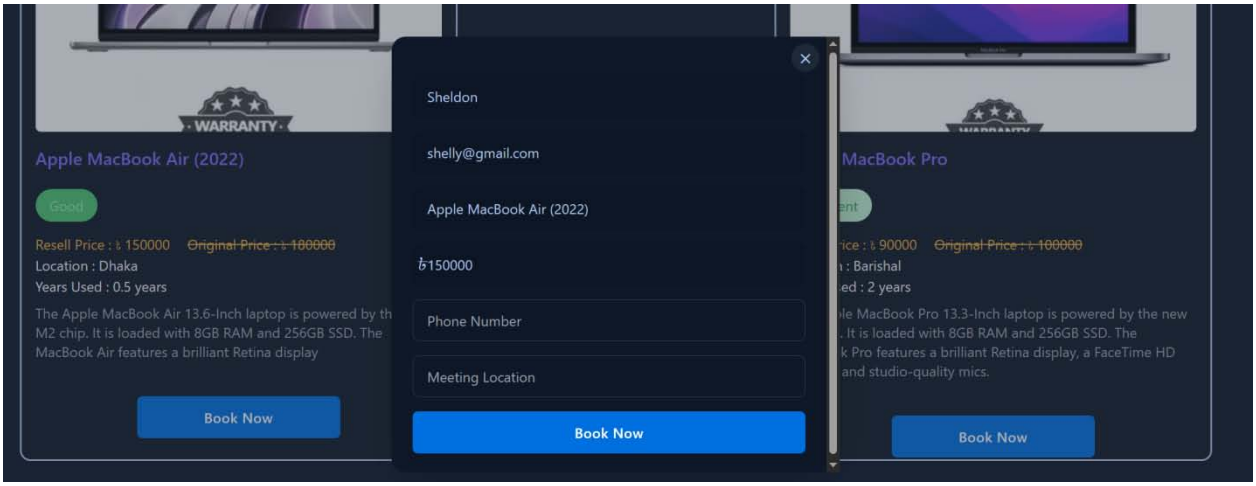


Figure 33: Booking Modal

A user is required to book the laptop in advance by clicking the "Book Now" button to acquire the laptop. When you click the button, a modal window similar to the one shown in Figure 33 will open. The form will have a total of six input fields. It is not possible to alter the user's name, email address, product title, or product price from within the modal. These fields can only be read, and no other actions may be taken on them. However, to book the product, the user is required to supply both their phone number and the location of the meeting.

```
const purchase = {
            name: form.name.value,
            email: form.email.value,
            productName: form.productName.value,
            price: form.resellPrice.value,
            phone: form.phoneNumber.value,
            meetingLocation: form.meetingLocation.value,
            picture: picture,
            productId: _id,
            paid: paid,
            sellerEmail: userEmail,
        };

        fetch('https://assignment-12-server-pi.vercel.app/book-product', {
            method: 'POST',
            headers: {
                'content-type': 'application/json',
                authorization: `Bearer ${localStorage.getItem('laptop-city-token')}`,
            },
            body: JSON.stringify(purchase),
```

Figure 34: Booking Modal Code Snapshot

The data from the input fields of the Booking Modal that can be seen in Figure 33 is saved in the database along with some other product properties. This includes the product picture, the product id, the payment status (whether the product has been sold or not), and the seller email.

Once the user has successfully booked the laptop, the details of their booking can be viewed in the My Orders tab, as illustrated in Figure 31.

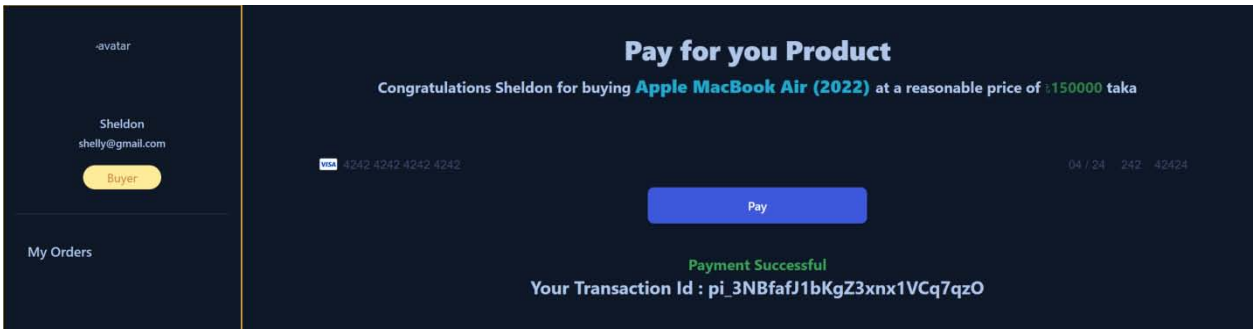


Figure 35: Payment Screen

The user will be redirected to the payment page after clicking the pay button. On this page, the user can finish the payment process by giving the essential information. A message that reads "Payment Successful" will appear on the payment page once the transaction has been completed successfully. Additionally, the transaction id of the user will be displayed. The user's browser will automatically navigate back to the orders page after a 2.5 second's delay.

Payment Gateway (Stripe)

Payment gateway is an essential component of every e-commerce platform and should be included. In this application for laptop city, the payment gateway system known as Stripe is utilized. Stripe is a payment processing service that facilitates the acceptance of various card types and other payment types by online retailers. Because the majority of Stripe's distinctive features are primarily focused towards online sales, the platform is ideally suited for use by companies that generate the majority of their revenue through online transactions. Stripe allows merchants to take debit cards in addition to the more common credit card brands. UnionPay (used in China) is also accepted. Businesses can accept payments from clients using mobile wallets and services that let them make immediate purchases with later payment. Stripe allows users to make payments using a wide range of currencies. A point-of-sale system called Stripe Terminal is made available by the company so that it can take payments in person.

Stripe must submit to an annual compliance report as well as routine security scans and testing in order to maintain its status as a PCI compliance Level 1 service provider, which the company has been audited and certified to achieve. Customers' credit card numbers are encrypted by Stripe, and the decryption keys are stored in a separate location, so the company cannot see them unless special measures are taken. [25]

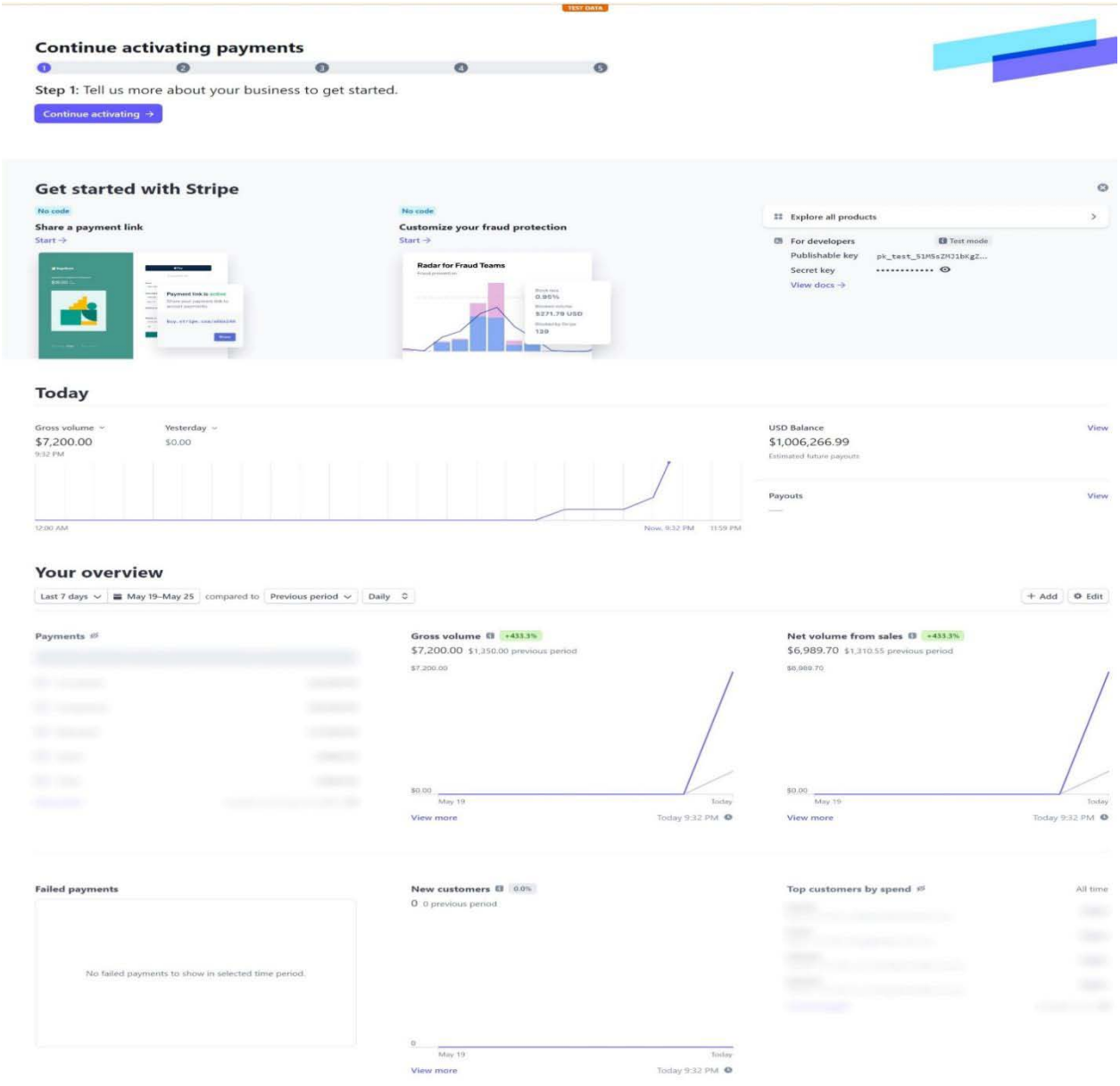


Figure 36: Stripe Developers Screen

In order to use Stripe, Stripe must be installed in both in front-end and back-end. After signing up in stripe, stripe will provide two secret keys for both front-end and back-end respectively. Due to the delicate nature of the topic of payment, these secret keys have been stored in env files.

```
REACT_APP_apiKey = AIzaSyDh7wYhOpOPseXJFYzATgK8Imgi-7VRJl0
REACT_APP_authDomain = laptop-city-3d932.firebaseapp.com
REACT_APP_projectId = laptop-city-3d932
REACT_APP_storageBucket = laptop-city-3d932.appspot.com
REACT_APP_messagingSenderId = 15079879208
REACT_APP_appId = 1:15079879208:web:072e1cdcbeedd7352a3b1d
REACT_APP_PK_STRIPE = pk_test_51M5sZMJ1bKgZ3xnxaq4XegoVudlloIegfR5oeqRyH6kHD3yLWPSWczbtH6cBqfZdYoBGNJMSTHms93nyfVT4UnxO00n0GZiWLJ
```

Figure 37: Snapshot of Stripe Publishable Key in Front-End

Figure 38: Snapshot of Stripe Secret Key in Back-End

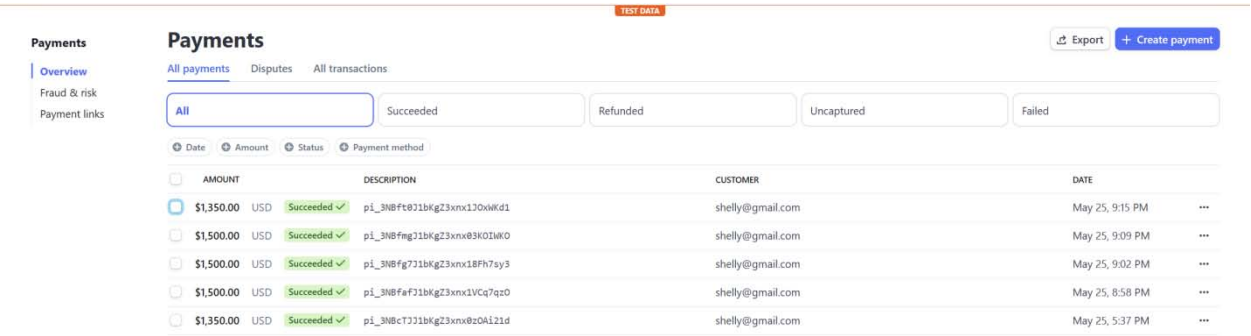


Figure 39: Payment Details from Stripe Payment Gateway

The payment system for the Laptop City app is currently in the testing phase. Therefore, the administrator will not get any legitimate payments. The remaining functionalities, with the exception of the payment mechanism, are operating as expected.

IV. Discussion

The MERN stack was utilized in the development of this Laptop City application. The front end of the application's user interfaces was built using React and Tailwind CSS, a utility first-class framework of CSS. Because the Tailwind CSS was utilized for the sake of styling, there was no requirement for additional CSS files to be utilized. Daisy UI, which is a Tailwind component library featuring various built-in components, was used for the front-end development. This makes it easier for the author, as they are able to only focus on the business logic of the application rather than having to worry about the app's styling.

Express.js is a Node.js framework that is utilized on the back-end and makes the process of developing applications simpler. It also has the function of syntactic sugar, which means that it has significantly streamlined and simplified the code sample. The construction of this application was carried out in two distinct stages, referred to as the front-end and the back-end.

All of the features had to be included in order to meet the intended criteria, but now the application is complete and can meet the needs of small businesses who want to sell secondhand laptops. Stripe requires the creation of a business account before the service can be used for commercial reasons. Since the author constructed the application solely for the sake of their thesis and had no intention of using it for commercial purposes, the author does not have a business account set up in Stripe.

a) Scope for Improvements

Even if all of the planned requirements have been satisfied, there is still a significant amount of room for improvement, particularly in the way components are styled. There was no unique styling applied because the majority of the components came directly from Daisy UI. This meant that the color combination was not influenced in any way. There is room for improvement in the color mix in order to provide a superior user experience.

Even if all of the functionalities that were planned to be introduced have been implemented, there are still some functionalities that can be added for further development.

- Once payment is received, a confirmation email will be sent to the user.
- A seller can submit a request for Admin verification; Admin will then either accept or deny the request.
- Each product has a dedicated details page with reviews and rating.
- Image upload feature for seller in Add a product page.

V. Conclusion

The primary objective of this thesis was to construct a fully functional multi-vendor e-commerce application using MERN stack components such as MongoDB, Express.js, React, and Node.js. This was the major objective of this thesis. In order for the author to

conduct study on these technologies and incorporate them into a project, a respectable amount of time was required. The theoretical underpinnings of each component of the MERN stack have been thoroughly covered, and code snippet snapshots have been incorporated to ensure that readers have a clear mental image of what the code actually looks like. In addition, the author explains how the application operates step by step, complete with images of the user interface (UI) and code snippet snapshots. Readers will obtain a fundamental understanding of how the application functions internally and externally based on these screenshots of the code and the user interface. Readers of this thesis will be able to comprehend why the author opted to conduct research on the MERN stack and then put that research into practice by developing a multi-vendor E-commerce application, as well as why the MERN stack is the most popular stack as of the year 2023.

In the end, the Laptop City was built to everyone's satisfaction. To make the process of buying and selling used laptops simple and trouble-free, a multi-vendor, fully functional e-commerce application with three distinct types of user roles and distinct paths around the dashboard for each of these user roles was developed. This program was developed with the goal of providing users with a superior experience when using the application. The processes of selling and purchasing laptops have been simplified for customers, making it possible for users to successfully navigate their way through Laptop City without the need for any form of instruction or training.

Following extensive research as well as implementation on a project, the author has some perspectives on the MERN stack and the reasons why it ought to be employed to construct a web application. Because the MERN stack is simple to understand, all that is initially required to launch an e-commerce website is a single developer. Since most small businesses have limited funds, it is highly recommended that these businesses build their web applications utilizing the MERN stack. Secondly, the developer is required to become proficient in only one programming language, which is JavaScript, which has a larger community. Third, the environment setup for the project is easy, and these technologies can be used to build high-load projects. In the end, Node.js and Express.js are widely utilized for back-end development in the modern era. They receive a lot of support from the community, and they are also utilized by large businesses such as LinkedIn, Medium, Trello, Netflix, and others.

Abbreviations

HTML	Hypertext markup language
CSS	Cascading Style sheets
API	Application Program Interface
JSON	JavaScript Object Notation
JSX	JavaScript XML
HTTP	HyperText Transfer Protocol
SPA	Single page Applications
NoSQL	Non-Structured Query Language
NPM	Node Package Manager
DOM	Document Object Model
UI	User Interface
UX	User Experience

References Références Referencias

1. C. Emery, "A Brief History of Web Development," Techopedia.com, 2019. https://www.techopedia.com/2/31579/networks/a-brief-history-of-web-development (accessed May 18, 2023).
2. "Why Web Application Development Is Important For Business," Linkedin, Oct. 29, 2021. https://www.linkedin.com/pulse/why-web-application-development-important-business-consultant/ (accessed May 18, 2023).
3. "MERN Stack - Javatpoint,"www.javatpoint.com. https://www.javatpoint.com/mern-stack (accessed May 18, 2023).
4. A. Kapoor, "Benefits of Using MERN Stack," Medium, Nov. 19, 2021. https://enlear.academy/benefits-of-using-mern-stack-7e0c732b5214 (acessed May 18, 2023).
5. R. Sheldon and J. Denman, "Node.js (Node)," WhatIs.com, Nov. 2022. https://www.techtarget.com/whatis/definition/Nodejs (accessed May 18, 2023).
6. Altexsoft, "The Good and the Bad of Node.js Web App Development," AltexSoft, Nov. 08, 2022. https://www.altexsoft.com/blog/engineering/the-good-and-the-bad-of-node-js-web-app-development/ (accessed May 18, 2023).
7. "Stack Overflow Developer Survey 2022," Stack Overflow. https://survey.stackoverflow.co/2022/#most-popular-technologies-webframe (accessed May 18, 2023)
8. Aashitace696, "Node.js Modules," GeeksforGeeks, Jun. 24, 2020. https://www.geeksforgeeks.org/node-js-modules/ (accessed May 18, 2023).
9. N. ABRAMOWSKI, "What is NPM? A Beginner's Guide," CAREERFOUNDRY, Nov. 28, 2022. https://careerfoundry.com/en/blog/web-development/what-is-npm/ (accessed May 18, 2023).
10. "NPM - Node Package Manager," www.tutorials teacher.com. https://www.tutorials teacher. com/nodejs/what-is-node-package-manager (aces- sed May 18, 2023)

11. "What is Express.js?," Codecademy. https://www.codecademy.com/article/what-is-express-js (accessed May 18, 2023)
12. D. Taylor, "What is MongoDB? Introduction, Architecture, Features & Example," GURU99, May 18, 2023. https://www.guru99.com/what-is-mongodb.html (accessed May 18, 2023).
13. Y. Arora, "Understanding MongoDB Data Modeling: A Comprehensive Guide," HEVO, Feb. 10, 2022. https://hevodata.com/learn/mongodb-data-modeling/ (accessed May 19, 2023).
14. "What is MongoDB Atlas? — MongoDB Atlas," www.mongodb.com. https://www.mongodb.com/docs/atlas/ (accessed May 19, 2023).
15. Webandcrafts, "Top Advantages and Disadvantages of MongoDB NoSQL Database," Webandcrafts Blog, Oct. 15, 2021. https://webandcrafts.com/blog/mongodb-advantages-and-disadvantages/ (accessed May 19, 2023)
16. D. Herbert, "What is React.js? (Uses, Examples, & More)," blog.hubspot.com, Jun. 27, 2022. https://blog.hubspot.com/website/react-js (accessed May 19, 2023)
17. C. Deshpande, "The Best Guide to Know What Is React," simplilearn, Feb. 07, 2023. https://www.simplilearn.com/tutorials/reactjs-tutorial/what-is-reactjs (accessed May 19, 2023).
18. M. Hamedani, "React Virtual DOM Explained in Simple English," Programming with Mosh, Dec. 03, 2018. https://programmingwithmosh.com/react/react-virtual-dom-explained/ (accessed May 19, 2023).
19. "ReactJS JSX - javatpoint," www.javatpoint.com. https://www.javatpoint.com/react-jsx (acessed May 19, 2023).
20. "ReactJS Components- javatpoint," www.javatpoint.com. https://www.javatpoint.com/react-components (accessed May 19, 2023).
21. "What are the pros and cons of React," www.knowledgehut.com, Nov. 24, 2022. https://www.knowledgehut.com/blog/web-development/pros-and-cons-of-react (accessed May 21, 2023).
22. "Types of e-commerce | BloomIdea," BloomIdea, 2014. https://bloomidea.com/en/blog/types-e-commerce (accessed May 21, 2023).
23. "Firebase Authentication," Firebase. https://firebase.google.com/docs/auth#:~:text=Firebase%20Authentication%20provides%20backend%20services (accessed May 22, 2023).
24. P. Kumar, "React Query - The what, how & when," WEDNESDAY, Jan. 23, 2023. https://www.wednesday.is/writing-articles/react-query-the-what-how-when#:~:text= React%20 Query %20is%20a%20data (accessed May 23, 2023).
25. R. Murphy, "What Is Stripe, and How Does It Work?," NerdWallet, Mar. 15, 2023. https://www.nerdwallet.com/article/small-busin-ess/what-is-stripe (accessed May 25, 2023).

Global Journals Guidelines Handbook 2024

www.GlobalJournals.org

Memberships

Fellows/Associates of Computer Science Research Council

FCSRC/ACSRC Memberships

Introduction

FCSRC/ACSRC is the most prestigious membership of Global Journals accredited by Open Association of Research Society, U.S.A (OARS). The credentials of Fellow and Associate designations signify that the researcher has gained the knowledge of the fundamental and high-level concepts, and is a subject matter expert, proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice. The credentials are designated only to the researchers, scientists, and professionals that have been selected by a rigorous process by our Editorial Board and Management Board.

Associates of FCSRC/ACSRC are scientists and researchers from around the world are working on projects/researches that have huge potentials. Members support Global Journals' mission to advance technology for humanity and the profession.

FCSRC

Fellow of Computer Science Research Council

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL is the most prestigious membership of Global Journals. It is an award and membership granted to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Fellows are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Fellow Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A FCSRC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Fellows can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Fellows receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Fellows can use the honored title of membership. The “FCSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FCSRC or William Walldroff, M.S., FCSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Fellow members of FCSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All fellows get a dedicated page on the website with their biography.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Fellows receive discounts on future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Fellows get secure and fast GJ work emails with unlimited forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, fellows receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Fellows are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All fellows receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 60% of sales proceeds

Fellows can publish articles (limited) without any fees. Also, they can earn up to 70% of sales proceeds from the sale of reference/review books/literature/publishing of research paper. The FCSRC member can decide its price and we can help in making the right decision.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Fellow members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

Access to Editorial Board

Become a member of the Editorial Board

Fellows may join as a member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. Additionally, Fellows get a chance to nominate other members for Editorial Board.

Career | Credibility | Exclusive | Reputation

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 5 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 10 GB free secure cloud access for storing research files.

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL is the membership of Global Journals awarded to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Associate membership can later be promoted to Fellow Membership. Associates are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Associate Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A ACSRC member gets access to a closed network of Tier 2 researchers and scientists with direct communication channel through our website. Associates can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Associates receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Associates can use the honored title of membership. The “ACSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., ACSRC or William Walldroff, M.S., ACSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Associate members of ACSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Associates receive discounts on future publications with Global Journals up to 30%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Associates get secure and fast GJ work emails with 5GB forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, associates receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Associates are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All associates receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 30-40% of sales proceeds

Associates can publish articles (limited) without any fees. Also, they can earn up to 30-40% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Associate members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 2 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 5 GB free secure cloud access for storing research files.

Associate	Fellow	Research Group	Basic
$4800 **lifetime designation**	$6800 **lifetime designation**	$12500.00 **organizational**	APC **per article**
Certificate, LoR and Momento **2** discounted publishing/year **Gradation** of Research **10** research contacts/day **1 GB** Cloud Storage **GJ** Community Access	**Certificate,** LoR and Momento **Unlimited** discounted publishing/year **Gradation** of Research **Unlimited** research contacts/day **5 GB** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**Certificates,** LoRs and Momentos **Unlimited** free publishing/year **Gradation** of Research **Unlimited** research contacts/day **Unlimited** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**GJ** Community Access

Preferred Author Guidelines

We accept the manuscript submissions in any standard (generic) format.

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from https://globaljournals.org/Template.zip

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at submit@globaljournals.org or get in touch with chiefeditor@globaljournals.org if they wish to send the abstract before submission.

Before and during Submission

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct,* along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author's email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s') names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

Policy on Plagiarism

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors' institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures

- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

Authorship Policies

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

Preparing your Manuscript

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.

Manuscript Style Instruction (Optional)

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11'", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

Structure and Format of Manuscript

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

a) A title which should be relevant to the theme of the paper.
b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
d) An introduction, giving fundamental background objectives.
e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
f) Results which should be presented concisely by well-designed tables and figures.
g) Suitable statistical data should also be given.
h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
j) There should be brief acknowledgments.
k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.

Format Structure

It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

All manuscripts submitted to Global Journals should include:

Title

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

Author details

The full postal address of any related author(s) must be specified.

Abstract

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Keywords

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, “What words would a source have to include to be truly valuable in a research paper?” Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

Numerical Methods

Numerical methods used should be transparent and, where appropriate, supported by references.

Abbreviations

Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

Formulas and equations

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

Tables, Figures, and Figure Legends

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.

Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

Preparation of Eletronic Figures for Publication

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

Color charges: Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

Tips for writing a good quality Computer Science Research Paper

Techniques for writing a good quality computer science research paper:

1. Choosing the topic: In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

2. Think like evaluators: If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

3. Ask your guides: If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

4. Use of computer is recommended: As you are doing research in the field of computer science then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

5. Use the internet for help: An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.

6. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

7. Revise what you wrote: When you write anything, always read it, summarize it, and then finalize it.

8. Make every effort: Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

9. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

10.Use proper verb tense: Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

11. Pick a good study spot: Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

12. Know what you know: Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

13. Use good grammar: Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

14. Arrangement of information: Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

15. Never start at the last minute: Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

16. Multitasking in research is not good: Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

17. Never copy others' work: Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

18. Go to seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

19. Refresh your mind after intervals: Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.

20. Think technically: Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

21. Adding unnecessary information: Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

22. Report concluded results: Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

23. Upon conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

Final points:

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

The introduction: This will be compiled from reference matter and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

The discussion section:

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear: Adhere to recommended page limits.

Mistakes to avoid:

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.
- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

Title page:

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

Abstract: This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

Reason for writing the article—theory, overall issue, purpose.

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

Approach:

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

Introduction:

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.

The following approach can create a valuable beginning:

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

Approach:

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

Procedures (methods and materials):

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

Materials may be reported in part of a section or else they may be recognized along with your measures.

Methods:

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

Approach:

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

What to keep away from:

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

Content:

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

What to stay away from:

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

Approach:

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

Figures and tables:

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

Discussion:

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."

Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.

Segment draft and final research paper: You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

Written material: You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350