ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

Integration of Cyber Threat Intelligence and machine Learning for Phishing Detection: A Review

Aishabanu Multani[1*]; Santosh Saha[2]

[1*]Asha M. Tarsadia Institute of Computer Science and Technology, Uka Tarsadia University, Surat, Gujarat, India
0009-0000-8319-1524

[2]Asha M. Tarsadia Institute of Computer Science and Technology, Uka Tarsadia University, Surat, Gujarat, India
0000-0002-0479-6750

Publication Date: 2026/05/30

Abstract: The dynamic change in the nature of various cyber threats, especially the threat of phishing, has identified the limitations of traditional security solutions such as rule-based systems, signature-based systems, etc. Cyber Threat Intelligence has emerged as an effective security practice that provides contextual information on threat actors, techniques, etc., whereas Machine Learning has also emerged as an effective security practice that offers solutions to automated threat detection using data analysis patterns. Although both of these security practices have immense potential, the integration of both has not yet been explored, as seen in the existing literature on the integration of both security practices to offer effective security solutions, especially against the threat of phishing. This paper has been designed to offer an extensive review of the existing literature on the integration of Cyber Threat Intelligence, Machine Learning, and security solutions, especially against the threat of phishing, as seen in the literature from 2016 to 2025.On the other hand, the comparative analysis of the challenges identifies the need to address the issue of unstructured sources of intelligence, the problem of limited interoperability, the issue of scalability, the problem of lack of explainability, and the problem of insufficient validation of the solutions in the real world. Moreover, the current models of phishing detection, despite their high benchmark accuracy, have limitations related to their adaptability, multilinguality, and adversarial robustness. With the identified research gaps, this review highlights the importance of developing semantically enriched CTI solutions, knowledge graph-based solutions, Large Language Model-based solutions, and adaptive learning-based solutions to facilitate the development of explainable and real-time solutions to the problem of cybersecurity.

Keywords: *Cyber Security, Cyber Threat Intelligence(CTI), Machine Learning, NLP/LLMs, Phishing detection, threat detection*

How to Cite: Aishabanu Multani; Santosh Saha (2026) Integration of Cyber Threat Intelligence and machine Learning for Phishing Detection: A Review. *International Journal of Innovative Science and Research Technology*, 11(5), 2483-2494. https://doi.org/10.38124/ijisrt/26may787

I. INTRODUCTION

In this digital era, cybersecurity has become a more important concern. The quick advancement in technology has expanded the attack surface, which is a crucial problem for industries and government organizations as well[1]. Classic security approaches are inefficient for sophisticated attacks such as phishing, ransomware, and zero-day attacks. Cyber Threat Intelligence (CTI) has became a crucial part of Cybersecurity to address these types of complications.

Cyber Threat Intelligence refers to gathering knowledge to understand the attacker's wants and predict future attacks [2]. CTI is an evidence-based understanding that provides context, mechanism, indicators, and advice on both existing and emerging tasks. CTI establishes a proactive element of cybersecurity[1]. CTI can acquire from various sources. These sources can be categorised into internal and external sources. They include open-source intelligence(OSINT), dark-web, log files, etc.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

Machine Learning is rapidly becoming a base of modern cybersecurity, offering advanced capabilities to combat evolving threats. From intrusion detection and anomaly recognition to anti-phishing and anti-ransomware measures, ML-based solution accelerate threat detection and improve its accuracy. ML, allowing automation, scalability, and flexibility, enables security systems to process huge and complex data in real-time, and offer better and more preemptive protection against cybersecurity threats.

Integrating Cyber Threat Intelligence with Machine Learning is becoming a key strategy in cybersecurity threat detection. CTI improves understanding by using data about threat actors, their methods, and the different types of phishing threats.

In other hand, ML provides the processing and analytical capabilities which are necessary for the analysis and interpretation of large and significant datasets.A combination of both allows for real-time, automated, and predictive defensive response.

Typical detection systems depend on static rules, blacklists or signature-based mechanisms that are less effective against several new variants of cyber threats. Meanwhile, Cyber CTI offers structured, contextual information about adversaries, Their Tactics, Techniques and Procedures(TTPs) and Indicators of compromise (IOCs). However, the effectiveness of Cyber Threat Intelligence (CTI) is limited by its poor interoperability, which hinders its ability to provide useful, real-time intelligence.

Most traditional detection systems use static rules, blacklists, or signature-based methods. These don't work against new and changing cyber threats. Cyber Threat Intelligence (CTI) gives you organized information about attackers' Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs). However, it doesn't work very well because it doesn't work well with other tools and doesn't work in real time. Machine Learning (ML) makes CTI better by finding patterns, predicting threats, and putting alerts in order of importance. Models like Multi-Layer Perceptron (MLP) and Large Language Models (LLMs) can make CTI analysis a lot better, as [1] says.

Hence, there are few drawbacks in detecting threat using ML models. Such as it is isolated from intelligence-insigts like attacker context, behavioral patterns and also cross platform indicators, results in reduced interpretability and adaptability. So that the problem is based on lack of unified collaboration between CTI frameworks and ML based threat detection models, particularly for major threats such as phishing threats, where dynamic behavioral and also contextual analysis is crucial.

There is an expanding requirement for a Comprehensive review at the union of CTI and ML. Literature is still fragmented with individual studies concentrating on CTI frameworks, ML models or concrete types of attacks, which makes it hard to develop an united understanding. In addition not much compound knowledge exists concerning the overall efficiency, issues and evolving trends in combining CTI and ML A review can respond to this shortage by integrating insights, highlighting key challenges and proposing directions for further research. Specifically, this paper focuses on applying CTI in reference to certain threats, providing special insight that is necessary for academics and industry.

The Scope of this Comprehensive review includes multiple aspects of CTI and ML. It studies the existing CTI framework and reviews Natural Language Processing (NLP) and Large Language Model(LLM) methods for analysis of intelligence, and ML-driven Security detection and hybrid models also. Particular Focus on the methods, datasets, accuracy metrics and applicability in real-world scenarios, reported in the Literature. Moreover, this review aims to recognise research gaps in existing studies and highlights future scope in possible way to improve the effectiveness of detecting phishing threats using CTI and ML models.

The rest of this review is organized in well-defined sections to deliver a comprehensive and systematic discussion. Section 2 begins with the Background section, which offers basic knowledge and understanding of CTI concepts, the Role of ML in cybersecurity, and the Collaboration of both to detect threats. Section 3 presents the methodology of review, which covers literature selection and classification criteria. Following this, section 4 presents a thematic review of existing studies, organized with CTI frameworks, automation and threat-specific applications. Furthermore, Section 5 highlights research gaps. section 6 proposes future directions to address key challenges. Finally, Section 7 concludes the review by summarising key concepts and the importance of the combination of CTI and ML model for threat detection in real-world studies.

II. BACKGROUND

To lay the groundwork, first, we discuss some basic concepts of cyber threat intelligence and machine learning. To map the advancement, we discuss the evaluation of CTI and ML together and outline the main categories of cyber threats that motivate these advancements. we then highlight the scope and target readers of this paper.

A. Cyber Threat Intelligence

The rapid growth of the digital era has increased cyber threats, making cybersecurity essential for industries and governments. Cyber Threat Intelligence (CTI) serves as a proactive approach by collecting, analyzing, and identifying threats before they cause damage. It provides valuable insights into attackers' Tactics, Techniques, and Procedures (TTPs), helping organizations strengthen their security.This Intelligence can come from sources like open-source data and the dark web.These sources are categorized as either internla or external sources. They include a range of intelligence that covers Open-Source Intelligence, Human Intelligence, and technical Intelligence. There are four types of Cyber Threat Intelligence (CTI), which include strategic, tactical, operational, and technical[2].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

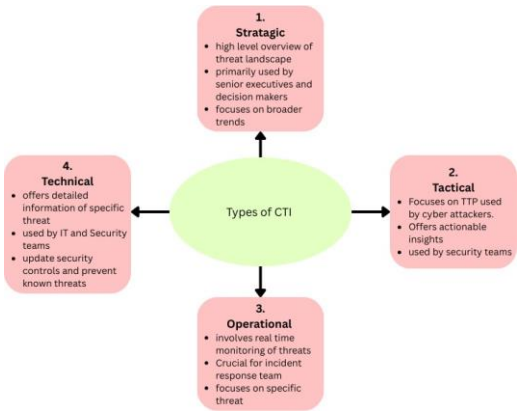

Fig. 1. Types of CTI Diagram

B. *Machine Learning*

The role of Machine Learning in cybersecurity has enhanced the ability to process and interpret threat data. Machine learning methods have been used in different types of ways to find cyber threats.

The author in [2]. stated that machine learning algorithms can improve the analysis of CTI by identifying patterns, predicting potential threats, and prioritising alerts based on their severity. for example, the application of machine learning model such as MUlti-Layer Perceptron (MLP) or Large Languages Models (LLMs) for CTI report processing.

C. *Integration of CTI and ML model*

CTI and ML approach make a powerful technique together where CTI represents rich and diverse method intelligence and ML method allows for adaptive automated and scalable analysis. This integration allows not only enhances situational awareness but also provide predictive defense against evolving cyber threats.

D. *Targeted Readers*

This review is mainly aimed at a wide ranging audience, including both academic and industrial professions. This study is helpful to academic research scholars, graduate students from the domain of cybersecurity, Artificial intelligence, and data science. They will find value in the framework, methods and datasets. Cybersecurity professionals, including threat intelligence analysts, security engineers, etc. may benefit for the implementation of CTI and ML for threat detection for real-world defense. Moreover, this paper can be beneficial for industries and other organisations also to understand the automated and intelligence–driven cybersecurity solutions.

III. METHODOLOGY

In this study, we conduct a literature review of certain relevant existing studies. This process going through various steps, which are as follows: step-1: Identifying the Research scope, step -2: Literature Search Strategy, step-3: Inclusion and Exclusion Criteria. Step-4: Screening and Selection papers, step-5: Data extraction and categorisation, step-6: Comparative analysis, step-7: Visualisation and Tables, step-8: Evaluation and Research gaps. Classification is shown in the figure.

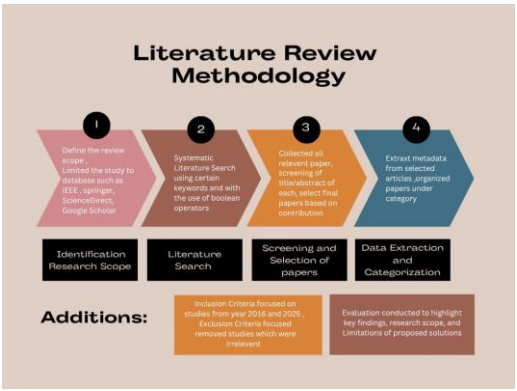

Fig. 2. Methodology Diagram

- Step-1: Initially we first clear the research scope, which focuses on CTI-frameworks, ML-based phishing detection. comprehensive Literature was managed by search across various databases such as IEEE, Springer, Google Scholar, ScienceDirect, and MDPI.
- Step-2: Relevant keywords such as “Cyber threat intelligence”, “Cyber security Incident response”, “Role of Machine Learning in Cyber Security”, “Threat Detection using CTI”, “Threat Detection with ML model”, “TTP mapping” were searched using Boolean operators to ensure studies are relevant to this research scope.

review conducted based on CTI approaches and ML models to detect different types of threats. This review shows how the CTI framework and ML model are useful for detecting different types of threats.

- Step-3: The Inclusion and Exclusion criteria were highlighted. Inclusion criteria focused on papers published in year 2016-2025. Furthermore more it considered that are relevant to CTI approaches and ML models for thrat detection. Exclusion criteria focuses on remove those studies that are non-relevant or only theoretical knowledge apart from CTI and ML models.
- Step-4: Initial screening was performed for the title and abstract of these studies and duplicates and irrelevant articles were removed. Furthermore detailed review was conducted for selected final papers based on contribution to CTI and ML approaches to extract details.
- Step-5: Following that, this step includes Data extraction and categorization of all these studies for better understanding. Extracted relevant metadata such Author name of article, Method used in studies, key findings duting the study, Accuracy of proposed solution, and Limitations.

Further more selected articles were organized in different categories based on their primary focus area. Core categories are Cyber Threat Intelligence, Machine Learning in Cybersecurity, Collaboration of CTI and ML, and Specific threat detection.

- Step-6: After thw Data extraction and categorixation, Comparative analysis was conducted for better understand the key findings from the papers and identified major research gaps and limitations.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

- Step-7: Moreover, Tables and graphical representations are designed for visually understand the trends and outcomes and limitations of the articles. Following that evaluation was executed to highlight key findings, certain research gaps, and accuracy of existing studies.

IV. LITERATURE REVIEW

This section provides a brief overview of existing research in phishing detection and cybersecurity. Various approaches, including heuristic, blacklist, and machine. learning-based techniques, have been explored to identify malicious URLs. The review establishes the foundation for the proposed system by highlighting key developments in the field.

The reviewed literature has been systematically organized into four distinct thematic categories to ensure clarity and structured analysis. The first category includes core Cyber Threat Intelligence (CTI) papers, which focus on threat data collection, analysis, and intelligence-sharing mechanisms. The second category comprises. machine learning-based cyber threat detection studies that utilize various algorithms for identifying malicious activities. The third category covers research that integrates CTI with machine learning techniques to enhance threat detection capabilities. Finally, the fourth category focuses specifically on phishing and related threat detection approaches, emphasizing URL-based and web-based attack identification. This categorization facilitates a comprehensive understanding of existing work and highlights the progression toward intelligent and hybrid detection systems.

Fig. 3. Paper Categorization Diagram

A. *Cyber Threat Intelligence Based Study*

Samtani et al.,\cite{ref3} explores the technique for AZSecure Hacker Assets Portal. It represents key portal functionalities like asset searching, browsing, and downloading, source code visualization and code comparison analytics and interactive CTI dashboards. This Solution aims to offer a proactive CTI and malware portal by collecting and analyzing malicious assets. It utilizes CTI and a malware analysis portal. It has a drawback also, which is that it uses only cosine similarity on a limited selection of source code.

Rastogi et al.,[4] presents an open-source malware ontology that allows the structured extraction of information and knowledge graph generation specifically for threat intelligence. It also demonstrate the annotation process using this solution on example threat intelligence report. It's core feature is highlighting Malware, IOCs and threat actor. It uses Malware reports as datasets. Thus, it has limitations which includes the system requires continued instantiation with annoted malware threat reports to build knowledge graphs.

Gao et al.,[5] introduce a new method that automates and improves cyber threat hunting. The system combining Cyber Threat Intelligence(CTI) with Natural Language Processing(NLP). It addresses the problem of identifying sophisticated attacks by connecting two different resources: open source cyber threat intelligence reports and large system audit logs to streamline automated extraction of indicators of compromise. Evaluation shows accurate results, achieving a 96.6 score for extracting attack details. This method also has limitations, including attacks on a few systems that are not captured by system auditing or considered by this framework.

Ejaz et al.,[6] investigated methods for the visual analysis of cyber threat intelligence (CTI) data. This research involved the examination of CTI reports to uncover concealed trends and interconnections. This work underscores the utility of machine learning techniques in identifying patterns and extracting valuable insights from CTI datasets. This provides a basis for more complex analytical approaches. This study highlights limitations that Trained models are limited to predicting known cyber threat actors and malware.

Li. et al.,[7]represent a system that automatically builds a technique knowledge graph from unstructured cyber threat intelligence. This study proposes a viable solution to get structured threat intelligence. Solution uses a methodology that is Natural Language -processing and graph alignment to highlight attack behavior from unstructured threat intelligence. To gain this, it used the CTI reports datasets. This evaluation shows that this system can extract an attack graph and report accurately. It shows accuracy about F1: 0.887-0.896. hence it has drawbacks also which include High false-positive rate in technique identification.

Irshad et al.,[8] conduct a research study which aims to develop a mechanism to attribute or profile cyber threat actor (CTA) by extracting feature from CTI reports. Moreover jt define a method which extracts feature from unstructured CTI reports by using natural language processing (NLP) techniques. It uses technique which is NLP and Attackvec using unstructured CTI reports. Its main feature is to show TTPs and malware features. It shows that there are problems, like how CTI from different security vendors is not organized, which makes it hard to get useful and meaningful information.

Connolly et al.,[9]explores how to use the dark web for cyber threat intelligence, using web-scraping techniques. The motive is to collect malware listings and vendors. This study analyzes market trends, emphasizing that cybersecurity professionals can gain crucial threat intelligence from publicly available data, thus avoiding risks of directly accessing the dark web.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

Mavroeidis et al.,[10]explore how CTI can improve security by providing evidence-based knowledge on threats. This research examined the different standards used in cyber threat intelligence taxonomies. The main focus was on how these standards support organized intelligence sharing and interoperability between security systems. The main problems that were found were a lack of clear definitions, poor integration of taxonomies, limited reasoning abilities, and not enough semantic details. Conclude with CTI ontologies should be modular extensible, and capable of automated analysis and richer, extensible threat knowledge.

Lawall et al. [11] come up with a way to stop ransomware attacks that uses a method that is based on Threat-led cyber threat intelligence. It emphasizes the characteristic of Ransomware TTPs utilizing OSINT and SOCMINT datasets. So, this conceptual study doesn't give any numbers. A drawback of this method is the TTPs do not include severity and potential impact metrics in their scoring.

Trivedi et al.,[1]present a comprehensive framework that offers fundamental concepts of cyber threat intelligence. The study points up a basic understanding of structured methodology. It covers key approaches of CTI such as types of CTI, sources of CTI, and various integrations of CTI, such as AI-driven threat analysis. Moreover, the contribution of this work is a formalized approach to CTI principles, understanding its strategic value in cybersecurity. As this study is based upon conceptual understanding, it did not show any experimental accuracy.

Rosa et al.,[12] introduce a framework designed to monitor harmful channels used in phishing campaigns. It includes a Cyber threat intelligence perspective. The proposed framework is based on combining machine learning with human expertise. Main feature of this solution represents IoCs and attacker infrastructure also it uses Telegram datasets as datasets. Hence it shows issue in scalability persists.

B. ML based study

Naik et al.,[13] presents a method for detecting sql injection attacks using machine learning, along with the integration of a honeypot. It uses ml model XGBoost as a technique also datasets of 30,926 queries, It primarily focuses on implementing a robust data processing pipeline to prepare SQL query features. Also, minimizing false positives and enhancing detection reliability by optimising feature selection and training. It shows accuracy about 99.58 \% hence it has limitations, including that the model does not currently cover modern injective variants.

Apruzzes et al.,[14] represent a study that provides an understanding of the role of ML in the cybersecurity domain. It provides a detailed overview of the benefits, problems, and future challenges of ML in cybersecurity. It also clarifies misconceptions. It also offers a brief summary of their application to detect cyber threats such as Malware, phishing, and Network intrusions. It is a conceptual study, so it does not show any accuracy in numeric. It also represents limitations of the fundamental assumptions of ML.

Table 1: Summary of CTI Papers

Author (Year)	Method	Feature	Dataset	Accuracy	Limitations
Samtani et al. (2016)	CTI & malware analysis portal	Not specified	Not specified	Not specified	Limited to cosine similarity on specific malware families
Rastogi et al.(2020)	Ontology (MAL-Ont)	Malware, IoCs, actors	Malware reports	N/A	Requires continuous annotated data for scalability
Peng Gao et al. (2021)	NLP + TBQL queries	CTI behaviors	System logs (47M)	96.64% (IOC)	Limited to system auditing; depends on CTI text availability
Ejaz et al. (2022)	Exploratory ML	Not specified	CTI reports	N/A	Limited scope; no real-world application focus
Li et al. (2022)	NLP + Graph alignment	Attack behaviors	CTI reports	F1: 0.887–0.896	High false positives; requires manual labeling
Irshad, Siddiqui et al. (2023)	NLP + Attack2vec	TTPs, malware, tools	Unstructured CTI reports	N/A	Limited datasets; unstructured data Complexity
Connolly et al.(2023)	Web scraping	Malware listings, vendors	307K entries	N/A	CAPTCHA issues; limited to public data
Mavroeidis et al. (2023)	Evaluation	CTI taxonomies	STIX, ATT&CK, CVE	N/A	Lack of standardization; poor inter-Operability
Lawall et al. (2024)	Threat-led CTI	Ransomware TTPs	OSINT, SOCMINT	N/A	Missing severity and impact met-Rics
Trivedi et al. (2024)	Theoretical framework	CTI concepts	Conceptual	N/A	High cost; privacy and skill chal-Lenges
Rosa et al.(2025)	Framework (ML + experts)	IoCs, infrastruc-ture	Telegram dataset	N/A	Scalability across regions and lan-Gauges

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

Table 2: Summary of ML-Based Cyber Threat Detection Papers

Author (Year)	Method	Feature	Dataset	Accuracy	Limitations
Naik et al.(2022)	XGBoost	Queries	30,926 queries	99.58%	Limited to SQL injection; lacks modern attack coverage
Apruzzese et al.(2022)	Review & Meta-analysis	Threat detection, IDS	Literature + case studies	N/A	IID assumption unsuitable for dynamic cyber threats
Dunsina et al.(2025)	Q-learning	Forensic evidence	Virtual malware environments	N/A	Uses basic RL; no LLM integration
Alshaikh et al.(2025)	Framework (qualitative)	ML communication	Focus groups	N/A	Needs real-world validation; external bias in ML adoption
Qiqieh et al.(2025)	HHO-SVM (Harris Hawks Optimization + SVM)	Feature weighting, parameter tuning, multi-threat features (fake news, IoT, URLs, spam)	FakeNews-1, FakeNews-2, FakeNews-3, IoT-ID, URL, SpamEmail-2, SpamWebsites	Up to 100%	Performance varies across datasets and high model complexity
Sadegh-Zadeh et al. (2025)	K-means clustering with geographic profiling (unsupervised ML)	Geolocation features, DNS query patterns, entropy-based anomalies	Passive DNS dataset (geospatial + DNS data)	92.3%	Geolocation inaccuracies and proxy/IP spoofing affect reliability
Sagar et al. (2025)	Random Forest, KNN, MLP, Inception (DL)	Network traffic features, statistical features	UNSW-NB15	98.4%	Struggles with high-dimensional data and evolving threats
Nnaka et al. (2025)	AI/ML-based approaches (SIEM, SOAR, XDR systems)	Real-time data analysis, anomaly detection, predictive modeling	Not specified	Not specified	Black-box models, adversarial attacks, and data quality issues

Table 3: Summary of CTI and ML Combined Research Papers

Author (Year)	Method	Feature	Dataset	Accuracy	Limitations
Dincy et al. (2025)	Swarm Learning + Blockchain	CTI sharing	CIC-Darknet, KronoDroid	F1 = 0.928	High computation cost; scalability issues
Fieblinger et al.(2024)	KG + LLMs (Llama2, Zephyr)	IoCs, CVEs, CWEs	CVE, CWE, CAPEC	Hits@10 = 0.606	Scalability issues; sensitive to noisy data
Rahman et al. [19] (2025)	LLM + Classifiers (XGB, RF)	MITRE ATT&CK TTPs	94 + 713 CTI reports	91% AUC	Limited coverage; low recall in temporal tasks
Arazzi et al.(2025)	BERT, DistilBERT, GCN	CVEs, IoCs, CTI feeds	NVD, CVE, blogs	~80%	Unstructured data issues; no quality standard

Table 4: Summary of CTI And ML Combined Research Papers

Author (Year)	Method	Feature	Dataset	Accuracy	Limitations
Ghaleb et al.(2022)	CTI + Ensemble Learning (RF + MLP)	URL + Whois + CTI	Malicious/Benign URLs	Improved (+7.8)	Manipulable URL features; dataset dependency
Iqra Naseer [22] (2023)	Literature Review	CTI, anomaly detection	Literature datasets	N/A	Data scarcity; poor zero-day detection
Aslam et al. (2023)	LSTM + XGBoost	URL, TF-IDF	PhishTank, Alexa	96.04%	High training time; not real-time optimized
van Geest et al.(2024)	Stacking models	URL, HTML	Zenodo dataset	97.44%	Limited real-world testing; no bypass analysis

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

Malarvizhi et al. (2024)	SVM platform	URL patterns	URL datasets	N/A	Limited model comparison
Ganesh Nayak et al. (2025)	FS + DNN, Wide&Deep, TabNet	111 URL features	PhishTank	94.46%	High feature extraction cost
Rahman et al.(2025)	AI integration (ML/DL/NLP/RL)	Behavioral, logs	150 studies	+17–35%	Adversarial risk; low explainability
An et al.(2025)	DT, RF, SVM, XGB	Email + OSINT	Kaggle	97.37%	Small dataset; limited generalization
Lim et al.(2025)	LogReg + TF-IDF + LIME + LLM	Email, URL	Benchmark datasets	98.4%	Some false positives/negatives remain
Jabbar et al. (2025)	RL (DQN)	Email + metadata	5K emails	95%	No adversarial training; limited scope
Li et al.(2025)	RBPD system	URL mismatch	Enterprise system	High precision	High inference cost; scalability issues
Saxena et al.(2026)	ML classifiers	URL structure	URL datasets	N/A	Dataset imbalance; real-time issues

Dunsina et al.,[15] evaluated the experimental framework within diverse virtual environment, incorporating a range of malware variants. This research presents a post-framework, constructed using a Markov Decision Process(MDP) model, which utilizes sophisticated reinforcement learning (RL) techniques. It uses the Q-learning technique and uses Virtual malware environments as datasets. Hence, it primarily uses Q-learning, which is a foundational reinforcement learning algorithm. The model did not initially include large language models.

Alshaikh et al.,[16] proposes a framework that addresses the need to standardize the communication of MLCS capabilities. It has been identified as necessary prior and related work. It was achieved in two parts – first is an analytical model that is verified by expert consultations, and second is a prototype standard that is developed focusing on key indicators.

Qiqieh et al.,[17] suggests a hybrid model that combines Harris Hawks Optimization (HHO) with Support Vector Machine (SVM) to make it easier to find a wider range of cyber threats. The model is able to deal with a wide range of threats, including fake news, IoT intrusions, and malicious URLs, because it focuses on feature weighting and parameter optimization. The experimental results show that the accuracy is very high, with some datasets reaching 100\%. The study, on the other hand, shows that performance changes based on the characteristics of the dataset. This shows that dataset dependency and increased model complexity are two major problems.

Sadegh-Zadeh et al.,[18] also talk about an unsupervised machine learning method that uses K-means clustering, geographic profiling, and DNS data analysis. This method uses geolocation and DNS query patterns to find unusual activity and spots where cyber threats are most likely to happen. The model gets about 92.3\% of the answers right, which shows that unsupervised methods work well with data that isn't labeled. The study recognizes limitations, including geolocation inaccuracies, proxy usage, and IP spoofing, which may compromise the reliability of threat attribution.

Sagar et al.,[19] present a deep learning framework that integrates an Inception model with conventional classifiers, including Random Forest, KNN, and MLP, for the detection of cyber threats in critical infrastructure. The model gets 98.4\% accuracy when using the UNSW-NB15 dataset, which shows how well deep learning can pick up on complicated network traffic patterns. The dataset has a lot of different types of attacks and a lot of features, which makes it a good choice for testing intrusion detection systems. The study shows that even though the system works well, there are still problems with dealing with high-dimensional data and keeping up with changing cyber threats, which are still big problems in real-world use.

Nnaka et al.,[20] also give a full review of AI-powered electronic danger detection systems, such as SIEM, SOAR, and XDR platforms. The study underscores the significance of AI in facilitating real-time analysis, predictive modeling, and the minimization of false positives. But it also points out some problems, such as the fact that the model acts like a black box, is open to attacks from enemies, and needs high-quality data. These problems show how important it is to have AI models in cybersecurity that can be explained and are strong. This is in line with other studies that show AI-based systems often have trouble being understood and need a lot of computing power.

C. Integration of CTI and ML Model Based Study

Dincy et al.,[21] propose a framework for Secure Cyber threat intelligence sharing. This framework integrates swarm learning and blockchain technologies to enable business to collaborate, preserving the privacy of their CTI data. This framework performs a collaborative training of ML models between different organizations through swarm learning approach. After that it assesses models and data quality through the use of validator nodes and zero-knowledge proof.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

It uses CIC-Darknetand KronoDroid datasets. Results in accuracy of F1= 0.928.

Fieblinger et al.,[22] conduct a research article on the effectiveness of using Large Language Models (LLMs) and Knowledge Graphs (KGs), which demonstrates automating the extraction of actionable Cyber Threat Intelligence from unstructured data. Primarily, it highlights IOCs, CVEs, etc., resulting in an accuracy of Hits@10=0.606. To achieve this, it uses CVE, CWE and CAPEC datasets. This study highlights some issues also which include Scalability challenges for large-scale data, Difficulty with complex syntactical structures, and struggle with irrelevant data.

Rahman et al.,[23] presents a study on mining Temporal Attack patterns. This study utilises LLM and classifiers such as XGB and RF techniques. This approach focuses on features like MITRE ATTACK and TTPs. It uses CTI reports as datasets and resulting in 91\% accuracy. Hence it has limitations such as limited ATTACK techniques Scope.

Arazzi et al.,[24] Examines a research studyon NLP-based techniques for cyber threat intelligence. This study first describes the foundational definitions and principle of cyber threat intelligence. After that examination of NLP based techniques for CTI data analysis and relation extraction from cybersecurity data. It describe features like IOCs and CTI feeds. It uses NVD and CVE blogs as datasets. In result, it shows 80\% accuracy. Limitations include Unstructured and Irrelevant data challenges, lack of standardized quality assessment.

D. Specific Threat Bases Study

Author in [25] study proposes a malicious URL detection model based on Cyber Threat Intelligence (CTI) and ensemble learning techniques. The methodology integrates Random Forest (RF) classifiers with a Multilayer Perceptron (MLP) in a two-stage classification framework to improve detection performance. The main features used in the model include URL-based attributes, who is information, and CTI features extracted from web searches and online intelligence sources. The study utilized a dataset containing benign and malicious URLs collected from multiple web sources. Experimental results demonstrated improved detection performance with approximately 7.8\% improvement in accuracy and a 6.7\% reduction in false positive rates compared to traditional URL-based models. However, the study highlights that URL features can still be manipulated by attackers and may limit the robustness of the model in highly dynamic threat environments.

Author in study [26] presents a comprehensive review of machine learning applications in Cyber Threat Intelligence (CTI) for improving cybersecurity defense mechanisms. The study analyzes various machine learning approaches including supervised learning, unsupervised learning, and reinforcement learning used for anomaly detection, malware classification, and threat prediction. The framework mainly focuses on threat intelligence data, network behavior patterns, and anomaly detection features extracted from cybersecurity datasets and literature sources. Instead of using a single dataset, the study reviews multiple research works across several domains including retail, finance, healthcare, and cybersecurity environments. The findings highlight that machine learning can significantly enhance proactive threat detection and automated analysis. However, the research identifies major challenges including data scarcity, poor data quality, and difficulties in detecting emerging cyber threats, which may affect the practical deployment of machine learning-based CTI systems.

[27] represent a model which is based on generalization model for optimization phishing URL detection. It uses LSTM and XGBoost method with PhishTank and Alexa datasets. This study mainly covered features like URL and TF-IDF. It shows results in 96.04 accuracy. Conclude with its limitations which include Lack of Average performance metric, model training time is high for both datasets, and real time detection.

Author in study [28] offers hybrid framework for automated phishing detection. This framework evaluate its effectiveness, robustness, and detection speed. Furthermore it introduces an innovative methodology for simulating bypass attacks on single-analysis base models. It uses Stacking models to gain results and used Zenodo datasets. It shows 97.88 accuracy. This framework has limitations also which covers limited scope of applicability factors tested.

Author in study [29] proposes a machine learning-based cyber threat detection system for identifying malicious URLs. The proposed system utilizes a Support Vector Machine (SVM) classifier trained on datasets containing malicious and benign URLs. The model analyzes lexical URL patterns and structural characteristics to determine whether a given URL is safe or malicious. The dataset used for training contains a large number of URLs collected from publicly available sources. The experimental implementation is integrated into a web-based platform where users can input URLs to check their security status. The results demonstrate the feasibility of machine learning techniques for detecting malicious web links and improving cybersecurity awareness. However, the study is limited by the use of a single machine learning algorithm and lack of comparative evaluation with other advanced models, which may restrict its effectiveness in complex threat scenarios.

Author in study [30] proposes a machine learning and deep learning-based phishing detection framework with feature selection techniques. The research evaluates multiple models including Feedforward Neural Networks, Deep Neural Networks (DNN), Wide and Deep models, and TabNet architectures. The system analyzes 111 features extracted from phishing URLs and website characteristics to distinguish malicious websites from legitimate ones. The dataset used in the experiments consists of 58,645 URLs collected from phishing datasets such as PhishTank and other sources. Through feature optimization and hyperparameter tuning, the proposed feedforward model achieved an accuracy of 94.46\% in phishing detection tasks. Despite the promising results, the study reports that extracting and processing a large number of features can increase computational cost and reduce efficiency in real-time applications.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

Author in study [31] investigates the integration of artificial intelligence and machine learning techniques in cybersecurity threat detection and response systems through a systematic meta-analysis. The study evaluates various AI approaches including machine learning, deep learning, natural language processing (NLP), and reinforcement learning (RL) used for intrusion detection, malware analysis, anomaly detection, and phishing prevention. The research analyzes 150 high-quality studies selected from an initial pool of 400 papers retrieved from major academic databases. The findings show that AI-driven cybersecurity systems can improve detection accuracy by 17–35\% and reduce response time by up to 45\% compared to traditional approaches. However, the study identifies several challenges including data imbalance, lack of model explainability, vulnerability to adversarial attacks, and high computational requirements, which may hinder widespread adoption of AI-based cybersecurity solutions.

Author in study [32] proposes a method based on email phishing attacks detection using OSINT and machine learning. It uses methodology such as SVM and XGB. Main features highlighted in this framework is SINT and email text. It used Kaggle datasets resulting 97.37 accuracy. The experiments were conducted in a smaller sample datasets which affected the generalizability of the findings.

[33] represents a concept of Enhancing phishing 77 detection through explainable AI and LLM-powered Interpretability. It uses methods like LIME and LLM. Main features this solution include is Email and URL features. This solution utilizes 98.4 accuracy. It shows Drawbacks such as Residual False Negatives and false positives.

Authors in [34] develop a model for Ai-driven phishing detection which enhancing cybersecurity reinforcement learning. It use RL deep Q network methodology and real emails as datasets. Its core features is focuses on Email content and metadata . it shows high accuracy about 95 . The proposed RL-based model was not explicitly trained against adversarial examples.

Authors in [35] proposed a framework practical deployment of reference-based phishing detection. This system determine if a URL can be processed immediately or not. It uses RBPD- fast slow task system and Enterprise system as datasets. Core feature include phishing detection for Webpage and URL mismatch.

Author in study [36] explores the application of machine learning techniques for phishing URL detection to improve online security systems. The proposed approach analyzes URL structural characteristics, lexical patterns, and statistical features to distinguish datasets containing phishing and benign URLs collected phishing websites from legitimate ones. The study evaluates different machine learning classifiers trained on from publicly available repositories. The experiments demonstrate that machine learning models can effectively identify phishing patterns and provide automated detection capabilities for browsers and email security systems. However, the research highlights several limitations including dataset imbalance, feature dependency, and challenges in deploying models for real-time detection environments, which may impact the overall reliability of the proposed system.

V. RESEARCH GAPS

The existing literature of research on Cyber Threat Intelligence (CTI) shows that several limitations that regulate the effectiveness and scalability of current approaches. A major gap depends on the lack of structured and interoperable ontologies with CTI systems. Most of the articles depend on isolated standards such as STIX, CVE, etc., which lack semantic depth, reasoning capabilities, and interoperability across platforms. Furthermore, most of the CTI data is unstructured, inconsistent, and collection from diverse sources such as threat reports, malware analysis and dark web listings. This unstructured behaviour creates difficulties in automated feature extraction, actor profiling, and identification of TTPs. Also CTI frameworks depens on manual or semi-automated annotation, limiting threat detection and large-scale implementation. Theoritically CTI frameworks also highlight organizational challenges, such as lack of skilled professionals, ethical and privacy concerns, and high cost of CTI program deployment.

Machine Learning (ML)-based cybersecurity models often do well on static datasets but fail to adapt to evolving or adversarial threats. Many studies lack real-world validation and rely on limited data. In addition, the importance of interpretability and explainability is often overlooked, which affects how reliable the results are and how easily they can be used in practice.

Research based on integration of CTI and ML indicates assurance, but it is still in its early phase. Integrated frameworks using LLMS, knowledge graphs, or blockchain suffer from scalability issues, inconsistent CTI sources, and limited attack coverage. Existing models faces struggle to process complex and large-scale data efficiently, and few address temporal or contextual relationships among cyber events.

In specific studies about phishing, high accuracy has been using ML and deep learning models; however these models lack real time detection, robustness against adversarial examples, and adaptability to evolving phishing strategies. Dependence on benchmark datasets, limited language coverage, and residual false detections indicate the need for more adaptive, explainable, and scalable phishing detection framework.

VI. FUTURE WORK

The future directions of the research in Cyber Threat Intelligence (CTI) and Machine Learning (ML)-based Cyber Security would be to create semantically enriched and interoperable models of intelligence. Although various Cyber Threat Intelligence standards, such as MITRE ATT&CK and STIX, have been developed to provide a structured representation of the various types of threats, these standards have yet to be enriched with complex reasoning capabilities to integrate diverse platforms semantically. The future directions of the research would be to explore ontology-based architecture

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

as well as knowledge graph-based models, which can be used to effectively integrate various types of vulnerabilities, threats, TTPs—Tactics, Techniques, and Procedures, etc., into a unified machine-readable format, which would be a form of semantic enrichment of the existing CTI standards to facilitate the inference of various types of cyber threats and features using ML models.

Another important area of research involves the utilization of Large Language Models (LLMs) for enabling the automatic processing of unstructured CTI sources such as threat reports, malware reports, vulnerability reports, and dark web reports. However, it is also important for such research in this direction to consider issues such as domain adaptation, hallucination, and computational cost in the context of secure deployment in SOC environments. Fine-tuning strategies could be crucial for solving these problems.

From a machine learning perspective, systems should be able to use "adaptive," "continuous," and "adversarial" learning methods to deal with the constantly changing nature of threats. The existing models have also been based on static data, which have not been robust enough for addressing "adversarial" attacks. The effectiveness of "online" learning paradigms, "incremental" model updates, and "adversarial" training should also be considered for improving the robustness of the model. In addition to this, it is also required that the effectiveness of the model should be validated using live traffic data for ensuring the overall "generalizability" of the model.The incorporation of "Explainable Artificial Intelligence" would also be crucial for improving the overall "trust" and "compliance" of the model in the "cybersecurity" space.

Scalability, as well as the ability to work in real-time, are areas that need more research and development, such as the ability to work with high-velocity CTI as well as network information using distributed processing models. Additionally, the use of edge detection has the potential to assist in the reduction of the time taken to detect phishing as well as malware attacks. Further more, the rise of decentralized intelligence-sharing tools offers a chance to build a trust and integrity among colaborating groups while also following privacy regulations.

Regarding the detection of phishing attacks, future research should concentrate on proposing multilingual, multimodal, and context-aware frameworks, incorporating URL features, domain intelligence, behavioral patterns, and temporal patterns. Graph-based and sequence-based learning models can be employed to identify dynamic phishing attack patterns and the intricate relationships inherent in diverse cyber attack types.

In the end, a systematic approach is necessary, considering both organizational and ethical aspects. Further research is crucial to find effective ways to use and apply Cyber Threat Intelligence (CTI), automated analyst assistance tools, and privacy-preserving intelligence models. Creating benchmark dataset and standardized protocols will improve the reproducibility and comparability of results in machine learning that use cyber threat intelligence.

VII. CONCLUSION

Cyber Threat Intelligence (CTI) is also an important part of the cyber security infrastructure because it helps find and stop cyber threats before they happen. Cyber threats are very dynamic by nature. The present literature review aims to ascertain the current state of existing Cyber Threat Intelligence systems, Machine Learning (ML) security models, and their integration for the purpose of intelligent threat detection. There are formalized threat intelligence systems like the MITRE ATT\&CK framework and STIX, but the current Cyber Threat Intelligence systems don't have semantic interoperability, reasoning, or scalability.

The analysis also pointed this out, showing that ML-based cybersecurity models work well with benchmark data but are limited because the data they use is static and not very strong. But there is also the problem of explainability and interpretability, which is still a big problem that makes it hard to use and deploy ML-based cybersecurity models.

Research integrating CTI and ML has yielded encouraging outcomes regarding their capacity to enhance contextual awareness and precision in the detection process, particularly concerning phishing attacks. The integrated framework is still in its early stages of development, though. There are still problems with unstructured sources of intelligence, data reliability, scalability, and the fact that it doesn't cover all the complex temporal relationships that come with the threat.

For phishing detection, advanced machine learning and deep learning techniques may excel in classification performance but may lack real-time adaptability, multilingual capabilities, and resilience against adversarial evasion in phishing detection contexts. The models' ability to be used is also limited by their reliance on benchmark data sets.

In general, this review shows how important it is to create cybersecurity strategies that are effective, easy to understand, and based on intelligence, and that use structured CTI and adaptive ML methods in the right way. It is crucial to connect the theoretical and practical parts of cybersecurity in order to make good defensive systems that can deal with the constantly changing cyber threat landscape.

REFERENCES

[1]. A. Trivedi, R. Gupta, and K. Jangal, "Cyber Threat Intelligence Research Paper," Arabian Agricultural Services Company (ARASCO), Tech. Rep., Aug. 2024.
[2]. A. Aljuhami, “Cyber Threat Intelligence in Risk Management: A Comprehensive Survey,” Computers & Security, vol. 105, pp. 1–12, 2021
[3]. R. Samtani, R. Chinn, and H. Chen, “AZSecure Hacker Assets Portal: A Cyber Threat Intelligence and Malware Analysis Platform,” IEEE Intelligence and Security Informatics (ISI), pp. 1–6, 2016.
[4]. R. Rastogi and R. Dutta, “MALOnt: An Ontology for Malware Threat Intelligence Representation,” Journal of Information Warfare, vol. 19, no. 4, pp. 45–58, 2020.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

[5]. M. Peng Gao, “Enabling Efficient Threat Hunting with CTI (THREATRAPTOR) Using NLP and TBQL Queries,” IEEE Access, vol. 9, pp. 108732–108745, 2021.
[6]. D. Ejaz, S. Siddiqui, and F. Irshad, “Visualizing Interesting Patterns in Cyber Threat Intelligence Reports Using Machine Learning,” Procedia Computer Science, vol. 207, pp. 121–130, 2022.
[7]. H. Li, T. Zhang, and X. Liu, “Automatic Construction of Technique Knowledge Graphs from Cyber Threat Intelligence Reports,” Expert Systems with Applications, vol. 204, 2022.
[8]. N. Irshad and S. Siddiqui, “Attack2Vec: Threat Actor Profiling through NLP-Based CTI Analysis,” Future Generation Computer Systems, vol. 142, pp. 213–224, 2023.
[9]. I. Connolly, “Dark Web Malware Marketplaces: A CTI-Based Web Scraping Study,” Journal of Digital Forensics, Security and Law, vol. 18, no. 4, pp. 45–60, 2023.
[10]. M. Mavroeidis and S. Bromander, “Cyber Threat Intelligence Ontologies and Interoperability Standards: A Critical Evaluation,” Computers \& Security, vol. 132, 2023.
[11]. M. Lawall and A. Beenken, “Threat-Led Approach to Mitigating Ransomware Using OSINT and SOCMINT,” Journal of Cybersecurity and Digital Trust, vol. 11, no. 1, pp. 23–36, 2024.
[12]. H. Rosa, “An Integrated Framework for Monitoring Phishing Campaigns Using CTI and Machine Learning,” Computers \& Security, vol. 143, 2025.
[13]. M. Naik and P. Deshpande, “Machine Learning-Based SQL Injection Detection Using XGBoost,” Journal of Information Security and Applications, vol. 71, 2022.
[14]. A. Apruzzese, M. Andreolini, L. Ferretti, and M. Marchetti, “Machine Learning for Cybersecurity: A Review and Meta-Analysis,” Computers \& Security, vol. 121, 2022.
[15]. E. Dunsina, J. Obafemi, and P. Ezimadu, “Reinforcement Learning for Post-Incident Malware Investigation,” Forensic Science International: Digital Investigation, vol. 48, pp. 1–10, 2025.
[16]. S. Alshaikh, L. Alqahtani, and A. Watson, “Understanding the Communication and Adoption of Machine Learning in Cybersecurity,” Computers & Security, vol. 139, 2025.
[17]. I. Qiqieh, “An intelligent cyber threat detection: A swarm-optimized machine learning approach,” Alexandria Engineering Journal, 2025.
[18]. S.-A. Sadegh-Zadeh, “An unsupervised machine learning approach for cyber threat detection using geographic profiling and Domain Name System data,” Decision Analytics Journal, 2025.
[19]. S. B. Shah, “Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure,” Journal of Global Research in Electronics and Communication, 2025.
[20]. K. I. Nnaka, “AI-powered threat detection: Opportunities and limitations in modern cyber defense,” World Journal of Advanced Research and Reviews, 2025.
[21]. A. Dincy R. Arikkat and N. Joseph, “SECTIS: Secure Cyber Threat Intelligence Sharing Using Swarm Learning and Blockchain,” IEEE Transactions on Network and Service Management, vol. 19, no. 5, pp. 5232–5245, 2025.
[22]. F. Fieblinger, M. Reichenbach, and A. R. Sadiq, “Integrating Knowledge Graphs and Large Language Models for Cyber Threat Intelligence Automation,” Applied Intelligence, vol. 54, no. 2, pp. 1120–1135, 2024.
[23]. R. Rahman, T. Nasir, and H. Chowdhury, “Temporal Attack Pattern Mining Using LLMs and ML Classifiers,” IEEE Access, vol. 13, pp. 20125–20138, 2025.
[24]. M. Arazzi, F. Moretti, and C. Piras, “NLP-Based Cyber Threat Intelligence and Relation Extraction Using BERT and GCN,” IEEE Access, vol. 13, pp. 47210–47225, 2025.
[25]. M. Alsaedi, F. A. Ghaleb, F. Saeed, J. Ahmad, and M. Alasli, "Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning," Sensors, vol. 22, no. 9, p. 3373, Apr. 2022, doi: 10.3390/s22093373.
[26]. I. Naseer, "Machine Learning Applications in Cyber Threat Intelligence: A Comprehensive Review," Asian Bulletin of Big Data Management, vol. 3, no. 2, pp. 190–200, Jan. 2024, doi: 10.62019/abbdm.v3i2.85.
[27]. A. Aslam, M. Khan, and N. Hussain, “AntiPhishStack: Phishing URL Detection Using LSTM and XGBoost,” International Journal of Information Security Science, vol. 12, no. 3, pp. 145–158, 2023.
[28]. V. van Geest, T. de Koning, and M. van Vliet, “Hybrid Framework for Automated Phishing Detection Using Stacking Models,” Expert Systems with Applications, vol. 237, 2024.
[29]. N. Malarvizhi, C. S. Krishna, J. K. Kumar, and P. V. S. Kumar, "Cyber Threat Detection in URLs using Machine Learning," Grenze International Journal of Engineering and Technology, June Issue.
[30]. G. S. Nayak, B. Muniyal, and M. C. Belavagi, "Enhancing Phishing Detection: A Machine Learning Approach With Feature Selection and Deep Learning Models," IEEE Access, vol. 13, 2025, doi: 10.1109/ACCESS.2025.3543738.
[31]. M. M. Rahman, K. Dhakal, N. Gony, M. K. Shuvra, and M. Rahman, "AI integration in cybersecurity software: Threat detection and response," International Journal of Innovative Research and Scientific Studies, vol. 8, no. 3, pp. 3907–3921, 2025.
[32]. A. An, S. Alghamdi, and R. Aljohani, “Multilingual Email Phishing Detection Using Ensemble Machine.
[33]. A. An, S. Alghamdi, and R. Aljohani, “Multilingual Email Phishing Detection Using Ensemble Machine Learning,” IEEE Access, vol. 13, pp. 67230–67242, 2025.
[34]. K. Lim, A. Rajendran, and L. Tan, “EXPLICATE: Explainable AI for Phishing Detection Using TF-IDF, LIME, and LLM,” Information Sciences, vol. 657, pp. 212–224, 2025.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26may787

[35]. P. Li, X. Zhang, and Y. Chen, “Reference-Based Phishing Detection for Enterprise Web Systems,” IEEE Transactions on Dependable and Secure Computing, vol. 22, 2025.
[36]. D. Saxena, S. Degadwala, and M. Joshi, "Phishing URL Detection Using Machine Learning," International Journal of Scientific Research in Science and Technology, vol. 13, no. 1, pp. 19–25, Jan. 2026, doi: 10.32628/IJSRST2613101.