Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A Review of Social Engineering Attack Detection Based on Machine Learning Techniques

Noor Sabah Asker, Essa Ibrahim Essa

Governments and institutions place the utmost importance on protecting sensitive intelligence information. Although the effectiveness of information security measures has improved, there is still a persistent human tendency to deceive, making them the weak link. Social engineering tricks involve cajoling and maneuvering individuals into divulging secret knowledge. These tricks trick others into performing or revealing tasks, collectively called social engineering. This scheme is known as a social engineering attack putting the assets of businesses organizations and government entities at risk. With progress making fraud more difficult it's crucial to discuss machine learning methods and tactics outlined in this paper to identify and prevent such risks. Attackers frequently use phishing as its easier to deceive individuals into clicking on yet harmful links, than bypassing computer security measures.

Keywords: Social engineering, phishing attacks, random forest.

1. Introduction

The occurrence and speedy dissemination of social engineering assaults in contemporary networks have decreased cybersecurity [1]. These assaults manipulate establishments, corporations, and individuals to extract valuable information for cybercriminals [2]. Despite the use of security, machine learning, and antivirus software, social engineering still poses a significant challenge because it relies on the weakness of the human psyche [3]. It is regarded as the most potent menace due to the nonexistence of detectable vulnerabilities within systems, as emphasized by the U.S. Department of Justice [4].

1.1 Social Engineering Attack:-

Social engineering attacks have emerged as one of the most perilous and significant menaces and apprehensions confronting cyber security [5]. Through the artistry of social manipulation, one can acquire classified and delicate knowledge, subsequently harnessing it for targeted ambitions such as extracting ransom from the vulnerable or trading it for unlawful intentions in the concealed realm [6]. Social engineering attacks exhibit variations in their goals, targets, and motivations, although they share a common approach with organized or endorsed steps for wrongdoers, encompassing four consecutive stages. Phase one entails gathering intelligence on the target; the second stage entails developing and maintaining a connection with the goal; and phase three entails using all the data gathered in steps one and two. Consequently, the actual attack starts in the last step, when the assailant disappears completely [7]. The four ever-present stages of an effort to manipulate society are graphically shown in Figure 1 [8]. The perpetrator makes an effort and gathers knowledge about the goal according to specified requirements for a particular goal in the first field, which is called inquiry and aggregation [9]. Step two involves deceit and strategy, and it centers on how to establish a connection with the goal and build trust via either immediate or indirect means to get what he wants. Step three involves capitalizing on the goal via various channels, whether it be emotionally or via security vulnerabilities, to obtain sensitive intelligence and commence the onslaught upon it. The ultimate stage is the culminating stage, wherein the perpetrator departs without leaving any trace or proof [10].

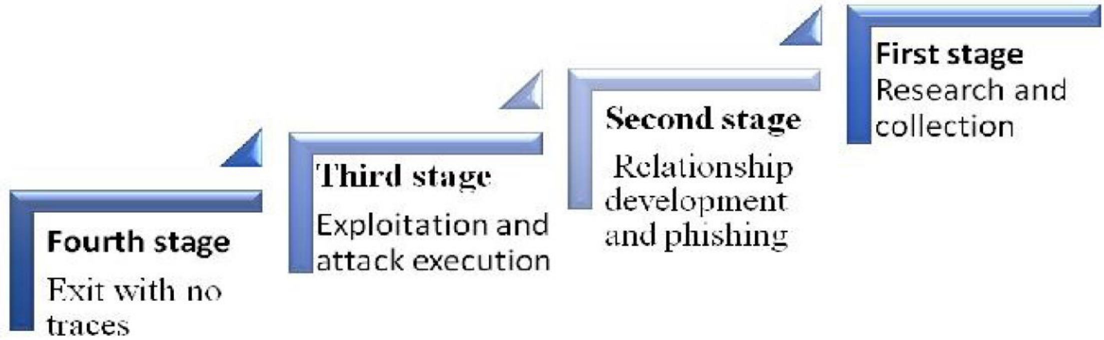
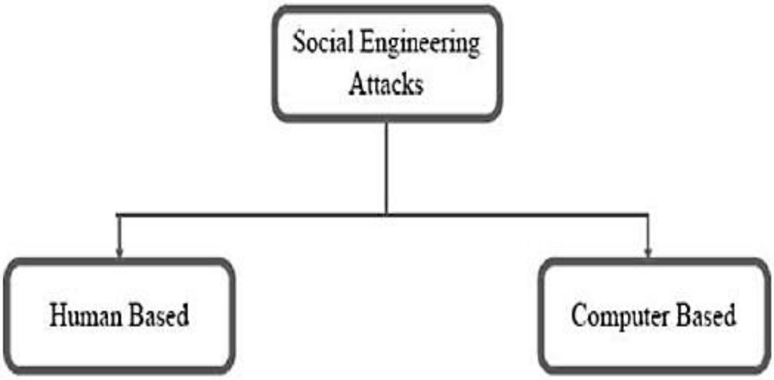


Figure 1:- Stages of Social Engineering Attacks [11].

1.1.1 Social Engineering Attack Classification:-

Social engineering attacks can be categorized in various manners to enhance comprehension and discover more effective resolutions for reducing and identifying them. Salahdine et al. [2] introduce many classification techniques illustrated in Figures 2, 3, and 4. In Figure 2, a clear distinction is made between two classifications that categorize cybersecurity attacks. The foremost categorization, acknowledged as human-centered onslaughts, encompasses the offender engaging in straightforward communication with the intended recipient to procure the coveted knowledge. This approach to assault includes a personalized and interactive tactic wherein the assailant strives to forge a direct connection with the target, thus eluding any technological barriers that may exist.

Conversely, the second categorization of onslaughts, mechanized assaults, entails a disparate modus operandi. In this instance, the offender relies heavily on computerized tools and software applications to amass the requisite data. By taking advantage of the potency and capabilities of these technological assets, the assailant aspires to derive an upper hand from susceptibilities within the digital framework of the target, thereby gaining unauthorized entry to confidential information. Consequently, these two classifications epitomize distinctive and divergent methodologies aggressors employ to procure invaluable records.



.

Figure 2:- Social engineering attacks, adapted from Salahdine et al. [2].

Figure 3 categorizes it into three categories: technological attacks, when the assailant relies on social networks and online platforms to amass information; societal attacks, when the assailant directly engages with a target to procure data; and human attacks, which are predicated on the perpetrator taking the initiative, such as secretly observing the victim to obtain information. Figure 4 amalgamates the two classifications above.

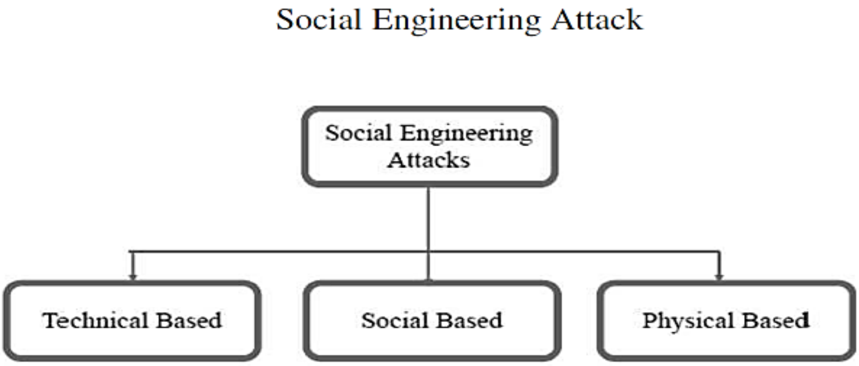


Figure 3:- Social engineering attacks, adapted from Salahdine et al. [2].

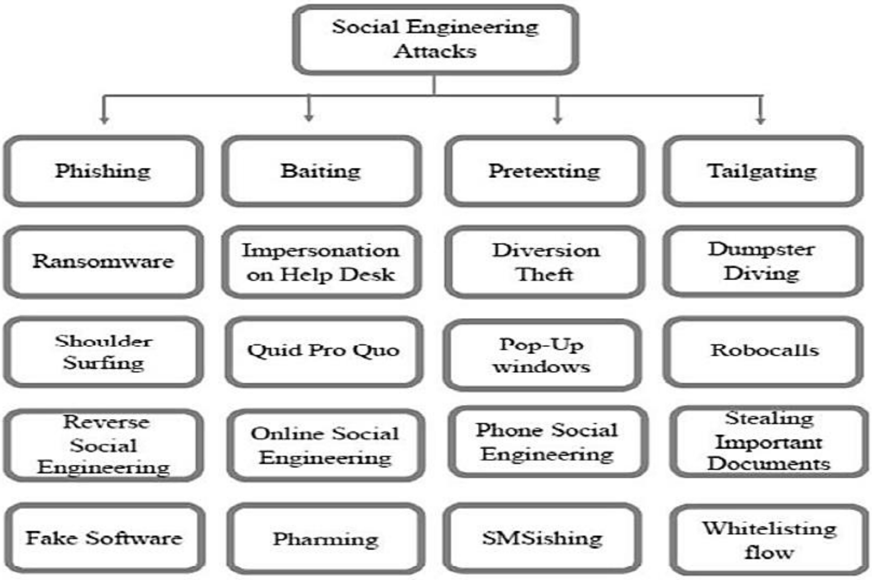


Figure 4:- Social engineering attacks, adapted from Salahdine et al. [2].

Following the illustration depicted in Figure 5, Ivaturi et al. [10]. It categorized social engineering assaults into two distinct classifications predicated on the manner of communication established between an assailant and a victim. The initial classification encompasses attacks directly exchanging information between the perpetrator and the target. Conversely, the second classification comprises assaults that materialize via an intermediary medium, such as telephone conversations or electronic mail correspondences.

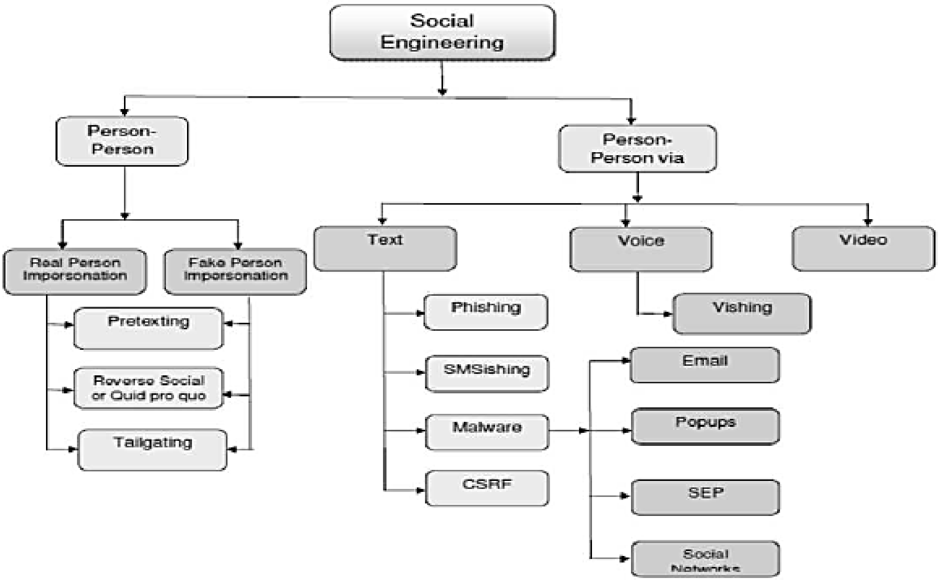


Figure 5:- Social engineering attacks, adapted from Ivaturi et al. [10].

1.1.2 Social Engineering Attack Strategies:-

A boundless array of social manipulation ploys thrive in their quest to obtain valuable data or infiltrate intricate systems by cunningly taking advantage of unwitting staff members. Despite their diverse methods, these attacks adhere to an archetypical pattern. These are [12]:-

(1) amassing pertinent intelligence.

(2) cultivating a profound bond.

(3) Capitalizing on this connection.

(4) carrying out actions with the ultimate goal of accomplishment.

The knowledge-gathering procedure can be acquired from societal origins like internet pages, communal media messages, phone directories, and employment gateways, among others, or from a preceding societal manipulation assault. The information from this stage is exploited to establish a joint connection with targeted individuals. In stage 2, connection evolution is directed towards forging a bond to recognize the inclinations and attributes of humans. Of being cooperative and confiding. When stage 2 triumphs, the assailant uses the objective to unveil vital information like passkeys, bank card digits, log-in specifics, and covert knowledge. This information procured can either be the supreme aspiration of the assault or the initiation of the subsequent phase. In the ultimate stage, the assailant endeavors to accomplish the foremost aim, which might encompass a repetition of the former stages.

1.1.3 Social Engineering Attacks Types:-

(1)Phishing Attack:-

The utmost prevalent social engineering assault is the Phishing assault [13]. It was previously employed to procure sensitive information from the targets utilizing various methods. Transmitting deceitful electronic messages is the customary phishing assault methodology. Telephonic conversations, internet pages, SMS messages, and social networks are alternative platforms for this endeavor. The assailant impersonates a reputable individual or assumes the guise of a lawful entity to gain a targeted individual's confidence. Delineated by the mode of communication between the assailant and the target, as well as the type of target, there exist a multitude of manifestations of phishing assaults [14]:

(A)Vishing assaults:- include talking on the phone, often when a criminal pretends to be a colleague and asks an IT staffer for help in resetting a password.

(B)Smuggling Attacks:- represent malicious attacks carried out via contact.

(C)In whale attacks:- attackers focus on essential or well-known people, greatly benefiting them.

(D)Spear Phishing Attacks:- An attacker targets a specific victim; this is more effective than the traditional phishing attack focusing on groups of people [15].

(2)Baiting Attack:-

The criminal entices victims with curious or greedy items to manipulate them. They use malware or flash memory to pique curiosity. Information about the target's interests is crucial for baiting [15].

(3)Reverse Social Engineering Attack:-

This offensive maneuver commences in a manner distinct from all other offensives. The intended recipients are under the impression that they have instigated a rapport with the assailant, utterly oblivious to the true identity of this assailant. This, in turn, renders them more inclined to disclose their information and seek assistance freely. Meanwhile, the assailant, having enticed the victim into initiating this connection and fostering trust, proceeds to exploit said victim. The assailant may set their sights on an individual user or a collective of users and may execute the assault either directly or indirectly [16].

(4)Watering Hole Attack:-

The attacker cunningly observes the target's online activities, identifying their most frequented webpage, and exploits a weakness in that page to gather valuable information, necessitating the expertise of a skilled assailant [17].

(5)Pretexting Attacks:-

The deceiver cunningly disguises themselves as a genuine individual, fabricating a pretext to engage with their target and pilfer confidential data, such as masquerading as a worker in a lawful financial institution and contacting victims to request updates on their particulars [18].

(6)Quid Pro Quo Attacks:-

In the art of quid pro quo, the assailant assumes the identity of an authorized individual and seeks information from the target in order to assist; for instance, the assailant may pose as a technical support staff and request the user to divulge confidential data or turn off the antivirus software under the guise of resolving a particular issue [19].

(7)Physical Attacks:-

(A)Creative Summary:- Trash treasures were stolen in dumpster diving attacks; valuable data was snatched for identity theft crimes [18].

(B)A shoulder surfing attack:- involves observing the targets to collect information about them, such as peering over the shoulder to steal the password or using a camera to obtain sensitive information while users enter it on their devices [19].

1.1.4 Defense Approaches Against Social Engineering Attacks:-

One distinguishing factor between social engineering and technical assaults is the level of expertise of the individuals involved. Technical attacks typically involve the staff employed in the Department of Information Security, or I.T., who possess technical knowledge. In contrast, social engineering attacks target individuals across all levels of the organization who may lack technical expertise and awareness of security concerns. Reducing social engineering breaches completely may be challenging, but implementing a multilayered defense strategy can aid in mitigating risks and minimizing harm to systems and data. This strategy includes developing a security policy, providing resistance training, ongoing reminders, responding to incidents, and implementing social engineering land mines [20].

(A) Enhanced protection for the body [21].

(B) A more stringent security policy is required (The Level of Foundation) [22].

(C) Response to Security Infringements [23].

(D) Incidence Handling Procedures [24].

1.2 Phishing Attacks:-

Phishing attacks are a common and widely used tactic among hackers. Phishing attacks include tricking a victim into revealing sensitive information by pretending to be a trustworthy source. The target attempts to communicate via several methods, such as email or phone calls, encompassing malevolent sites, fraudulent declarations of prizes, counterfeit proposals, deceitful internet shopping sites, and an abundance of methods and strategies employed by the assailant to trap the prey. To exemplify transmitting a deceptive electronic mail to the prey, you have achieved an accolade with us; to acquire the accolade, click on the hyperlink and finalize your particulars and credit card digits in conjunction with clandestine digits or input any information that is sensitive or classified knowledge. The attackers reap the rewards and cater to their needs online [26].

1.2.1 Phishing Attack Types:-

(1)Phishing that utilizes algorithms:- Attackers use various algorithms to obtain sensitive data from a website's database. V,Shreeram, M,Suban, P,Shanthi, and K,Manjula suggested a method to detect phishing links using a rule-based system created from a evolutionary model. A link is considered phishing if it complies with the guideline stored in a database created by the genetic algorithm [27].

(2)Phishing with a deceptive approach:- The approach at hand encompasses the provision of malicious links to clients through emails, subsequently guiding them towards websites of a negative nature wherein the likelihood of divulging sensitive information is high. A comprehensive analysis is presented by Huajun Huang, Junshan Tan, and Lingxi Liu regarding a deceitful phishing attack and the array of antiphishing techniques employed. The authors duly outline the phishers' various methods and discuss the various remedies' benefits and drawbacks [28].

(3)URL Phishing:- Even in a seemingly innocuous part of an universal resource locator (URL), attackers may hide links that take users to malicious websites. An strategy to recognizing URL phishing by URL ranking is shown in the work of M.N. Feroz and S. Mengel. They sort and rank the URLs using the internet popularity solutions provided by URL systems after classifying them according to linguistic and host-related features [29].

(4)Hosts File Poisoning:- By transforming the names of hosts within host records, the typical method used by DNS servers retrieving I.P. addresses can be overridden, leading to the potential for valid URLs to direct to malicious pages instead of secure sites due to the server's I.P. associations having been compromised. S.Abu-Nimeh and S.Nair propose a novel assault that utilizes DNS poisoning to bypass security and phishing filters, successfully attacking multiple security toolbars and browser filters undetected [30].

(5)Injection of Content Phishing:- Gathering information is accomplished in this methodology by consolidating malevolent segments within an authentic website. J.P. Erkkil expounds on the diverse techniques by which phishing methodologies can deceive an individual. A catalog of numerous approaches that possess the capability to identify instances of phishing is enumerated. The scholarly article posits that organizations should embrace efficacious protocols to ensure the contemporaneity of their security features [31].

(6)Clone Phishing:- The act of replicating previously dispatched electronic mails and appending a harmful hyperlink to them has the potential to facilitate the accomplishment of an assault on an unsuspecting individual. Ahmad Alamgir Khan put forward a novel approach wherein internet sites employ a creative system for time passwords and machine-user authentication to counteract assaults from spam. Web servers will transmit a unique password to a user through a short message service or electronic mail and generate a secret code for the gadget once the user inputs the aforementioned private key [32].

1.2.2 Description of Existing Phishing Attack Detection:-

Social engineering attacks use many Internet networks and threaten people's privacy, businesses, and essential information. The following table highlights some studies and research [33].

Reference No.	Description	Advantage	Disadvantage
[34]	Conducts a comprehensive assessment of squatting phishing, wherein the phishing pages assume the identities of target brands in terms of their domain and content.	*The utilization of characteristics derived from visual analysis and optical character recognition is observed in this study. * Furthermore, the tool employed in this research is an open-sourced one. * In addition, the development of classifiers is facilitated by integrating evasive behaviors exhibited by phishing pages.	*The identification of phishing pages that employ cloaking remains elusive. *Solely concentrates on widely recognized and renowned brands. * No hacking tool, including CANTINA and CANTINA+, can match the classifier.
[35]	ML aggregate analysis is suggested for pattern discovery. of page layouts. This mechanism is employed to identify phishing pages.	*A set of classifiers is trained automatically to assess the similarity of web pages based on CSS layout features, thereby eliminating the need for human expertise.	*The method is lightweight, as it exclusively relies on a singular class of features, namely the CSS structure. * The power of its performance is limited by the size and distribution of the data it works with.
[36]	A comment spam detection mechanism should be implemented to function as a browser plugin, thereby facilitating the elimination of spam comments.	*The dataset is balanced using WEKA filters to obtain the most appropriate features. *The classifier for spam detection can incorporate novel features and identify novel types of spam content.	*Cannot be proficient in handling a random dataset in the absence of implementing a supervised resample filter.
[37]	This manuscript posits a state-of-the-art antiphishing framework that employs seven classification methodologies and features rooted in natural language processing (NLP).	*Autonomy from linguistic and external service providers. *Vast collection of valid and deceptive information. *Instantaneous implementation	*Machine learning systems cannot effectively leverage a dataset of such magnitude.

		*Possesses the capability to identify novel websites due to the incorporation of natural language processing characteristics.	
[38]	An investigation utilizes a novel characteristic referred to as the "similarity of the top page within the domain" to enhance the efficacy of a model for detecting phishing attacks based on machine learning.	*Enhances the f-measure and diminishes the rate of error. *Demonstrates that the detection rate is significantly elevated by employing superior characteristics and can be executed in forthcoming endeavors.	*The paradigm is exceedingly reliant on the precision of the characteristics.
[39]	Constructing a classifier to identify malicious web pages and threats is achieved by incorporating elements derived from JavaScript code, HTML contents, and URLs.	*A variety of characteristics are present. *A considerable level of precision is achieved. *Emphasizes the attributes that are essential for extraction.	*The dataset is limited, consisting of 2500 URLs. *The classifier's performance may be compromised when dealing with extensive datasets.
[40]	A machine learning-based approach is presented to identify whether a web page demonstrates indications of phishing attacks.	*The method under consideration is founded upon a feature vector that is readily obtainable and does not necessitate supplementary computation.	*The detection process solely employs a mere ten features. *The dataset employed for analysis is confined to a modest number of 1353 instances.
[41]	A system is constructed employing the principles of machine learning to enable the classification of websites through the utilization of URLs.	*Can be utilized to construct a normative framework with associative principles to categorize Uniform Resource Locators (URLs).	*nine characteristics for every Uniform Resource Locator (URL). *Every characteristic is distinct. *Restricted dataset (1353 URLs).
[42]	Identifies instances of phishing attacks through the utilization of an allowlist screening mechanism.	*Pages that circumvent the safelist filter undergo another round of filtration through Support Vector Machines.	*A small dataset of 850 pages was found. * Identifying DNS mimics and real websites was almost impossible.
[43]	Employs the feature selection mechanism to discern salient attributes that classify websites into the categories of phishing and legitimate.	* feature selection dramatically enhances the precision score after implementation. *The employment of feature selection diminishes the computational time.	*14 characteristics identified. *Dataset limited, consisting of 200 legitimate and 1400 phishing URLs. *Possible issues when applied to datasets with equal numbers of legitimate and phishing web pages.

2. Literature Review:-

Phishing is the most effortless approach to amassing sensitive data from unsuspecting individuals. Phishers pursue confidential information encompassing passphrases, log-in details, and bank account particulars. Cybersecurity specialists are actively investigating dependable and efficacious procedures to discern phishing sites. Subsequently, the ensuing paragraphs divulge the most up-to-date investigations and inquiries pertinent to this domain [44].

2.1 Social Engineering Attack Detection Based on Machine Learning:-

In this manuscript, Assefa & Katarya [45] proposed an ingenious neural network, Autoencoder, that utilizes anomaly scrutiny to differentiate and categorize web portals as authentic or deceptive websites. The algorithm scrutinizes numerous fictitious and bona fide Uniform Resource Locators. It employs this methodology to investigate their attributes and accurately recognize the shady sites, encompassing those constructed spontaneously, commonly called zero-hour misleading websites.

Veach & Bualkibash [46] This document endeavors to comprehend the exploration carried out in the domain and scrutinize the subsequent strides ahead. Concentrating on selecting suitable attributes, including genetic algorithms like AdaBoost and MultiBoost, leads to accomplishment. Classifiers like neural networks, ensemble algorithms, and innovative approaches are examined. The data is processed into a system for detecting phishing websites on the cloud and client sides. Advice for upcoming inquiries and assessments is offered to help advance in this sector.

A.Abu Zuraiq & M.Al-Kasassbeh [47] This paper has eloquently addressed the previously mentioned subject matter through the clever implementation of advanced machine learning algorithms and the ingenious utilization of a unique dataset to identify deceptive online practices. This remarkable dataset encompasses 5,000 authentic web pages and several insidious phishing pages. To achieve the most impeccable and optimal results, a comprehensive examination of various machine learning algorithms was conducted with the utmost diligence. The algorithms handpicked for this study include the esteemed J48, the enigmatic random forest, and the formidable multilayer perceptron. In addition, a diverse array of tools for characteristic selection were deftly employed to augment the efficacy of the models. The culmination of this experiment yielded a truly extraordinary outcome, as it was revealed that the most favorable precision was attained when a selection of 20 distinguishing characteristics out of the available 48 was adroitly applied in conjunction with the esteemed Random Forest algorithm. The resulting level of precision reached an astounding 98.11%, a testament to the sheer brilliance of this research endeavor.

Alsufyani and Alzahrani [48] In this manuscript, we shall exhibit specific endeavors that rely on the marvels of automated cognition methods and demonstrate the information harnessed in these methodologies. Furthermore, we shall allude to societal manipulation and its perils.

Lopez & Camargo [49] This document introduces a framework for identifying instances of social manipulation using written discourse as an input. This framework can be employed within various contexts where textual inputs, such as SMS, chats, emails, and so forth, are the primary medium. By leveraging the power of natural language processing, this framework's methodology entails the extraction of distinctive attributes from the conversational text, such as the tally and appraisal of URLs, spell-checking, and enumeration of blacklisted terms, alongside other relevant factors. The attributes above are then employed to educate machine learning algorithms, namely neural networks, random forests, and support vector machines, to classify social engineering attacks. The outcomes of these classification algorithms have demonstrated an accuracy exceeding 80% in detecting instances of this nature.

Abdulmunem et al. [50] This exploration employed various contrivance learning procedures to avert these onslaughts and safeguard the contraptions via the acquisition of MTM and DDoS attack-related datasets obtained from the Kaggle website. This investigation used preprocessing after acquiring the dataset methodologies such as filling the absent values, as this dataset encompasses copious void values. Afterward, we utilized four ingenious learning techniques to perceive these attacks: chance-filled woodland (R.F.), utmost gradient boosting (XGBoost), gradient boosting (G.B.), and verdict tree (D.T.). Many classification metrics are utilized to evaluate the efficacy of the methods: precision, exactness, remembrance, and harmony of f1. The investigation achieved the ensuing outcomes in both kinds of data: i) all techniques can ascertain the MTM strike with indistinguishable effectiveness, which exceeds 99% in all measures; and ii) all techniques can ascertain the DoS strike with indistinguishable effectiveness, which exceeds 97% in all measures. Outcomes demonstrated that these techniques can perceive MTM and DoS onslaughts remarkably well, which inspires us to harness their power in safeguarding devices from these strike.

U.A.Butt et al. [51] This manuscript uses unique lawful and fraudulent data aspects, discovers new emails and applies diverse characteristics and algorithms for classification. A new dataset is generated by analyzing the current methods. A CSV file and a document with titles are created. The inquiry utilizes SVM, NB, and LSTM algorithms. The primary objective is to identify fake emails. SVM, NB, and LSTM have excellent performance in detecting fraudulent emails. Naive Bayes, Support Vector Machines, and Long Short-Term Memory classifiers exhibit precision rates of 97%, 98%, and 99.62%, respectively.

d.v.grbic&i.dujlovic [52] In this paper, we present the potential utilization of ChatGPT in preparing environments for carrying out social engineering-based assaults. Shortly after its public release, ChatGPT has demonstrated remarkable efficacy across various subjects, encompassing the provision of responses to broad and specific inquiries, code generation, and creating text templates about particular subjects. By merging these capabilities with the system's adeptness in readiness, it becomes feasible to obtain all the necessary elements for phishing or similar attacks with minimal effort and in a matter of minutes. This paper comprehensively explores the scenario of orchestrating a phishing attack through the employment of ChatGPT, accompanied by an overview of social engineering assaults and their general preventive measures.

C.K. Jia et al. [53] The current framework incorporates two distinct modules, self-enhancement and interactive enhancement, which gradually augment characteristics to capture intricate morphing patterns. The proposed methodology was compared against nine traditional technologies through experimentation conducted on a widely recognized database, ultimately exhibiting outstanding performance.

Hussain et al. [54] This article introduces the concept of social manipulation. The internet has revolutionized contemporary systems. Billions of internet users exist and are increasing daily and making sure that security is a primary concern for cyber-physical systems. The article focuses on social manipulation as a crucial aspect of cyber security. It involves manipulating human emotions. Organizations use advanced systems to protect data in their data centers. However, individuals must also secure their personal information from social manipulators. The article discusses issues related to data privacy and social manipulation methodologies. It provides a concise summary of these methodologies, concluding the article.

2.2 Phishing Attack Detection in Social Engineering:-

Lansley et al. [55] The innovative minds behind this study have devised an ingenious technique to identify social engineering attacks. This groundbreaking method relies on utilizing the potential of natural language processing and artificial neural networks. It seamlessly finds application in online and offline situations, promptly identifying any conversation indicating a social engineering assault. In the initial stages, the text of the conversation undergoes meticulous parsing and thorough examination to detect any grammatical errors, employing the exceptional capabilities of natural language processing methods. Following that, an artificial neural network steps in and adeptly classifies potential attacks. To validate the effectiveness of this approach extensive evaluations have been conducted using both partially artificial data sets resulting in highly impressive accuracy outcomes.

Yichiet Aun et al. [56] a cutting edge security engineering framework has been developed utilizing a neural network for long and short term memory functions. The primary goal is to uncover security engineering threats lurking within social media posts. A unique dataset meticulously gathered from corporate and personal Facebook posts serves as the foundation for this research. Initially a designed tool called Social Engineering Attack Detection (SEAD) is deployed to analyze posts and filter out those, with intentions using domain specific rules. Subsequently each social media post is broken down into sentences followed by a detailed sentiment analysis that leads to the labeling of content. Finally an RNN LSTM model is meticulously trained to identify five categories of social engineering attacks that may show signs of information gathering attempts.Experimental findings unequivocally demonstrate that the Social Engineering Attack (SEA) model attains a remarkable classification precision of 0.84 and a commendable recall rate of 0.81 compared to the ground truth, expertly identified by network specialists.

Fatima Salahdine et al. [57] In this manuscript, the authors have used an ingenious technique for identifying fraudulent phishing attempts by applying machine learning. We have diligently gathered and meticulously examined over 4000 deceitful emails aimed explicitly at compromising the esteemed University of North Dakota's electronic mail system. We have meticulously selected ten salient distinguishing characteristics to emulate these insidious attacks and constructed an extensive data repository. This comprehensive collection has been employed to proficiently train, validate, and assess the efficacy of the machine learning algorithms. To accurately gauge the performance, we have judiciously used four key metrics: probability of detection, probability of miss-detection, probability of false alarm, and accuracy. It has been unequivocally demonstrated through empirical exploration that employing an artificial neural network leads to heightened detection capabilities.

Nikolaos et al. [58] In this manuscript, we unveil the present cutting-edge S.E. assault identification frameworks. We meticulously analyze an S.E. assault to perceive the diverse phases, structures, and qualities and segregate the pivotal catalysts that can sway an S.E. assault to operate. In conclusion, we present our innovative approach to a framework that automates the detection of chat-based S.E. attacks. This framework is built upon the foundations of personality recognition, influence recognition, deception recognition, speech act, and chat history.

Abeer & Emad [59] in this document, the survey encapsulates the notion of societal manipulation and how the assailant endeavors to attain it. For this purpose, it initiates with an assault, phishing. It constitutes a fusion of societal manipulation and technical approaches to entice the user into divulging their delicate and private information. In addition, it delves into the categorization of phishing through societal manipulation. Furthermore, this manuscript will delve into survey techniques to mitigate this onslaught and strive to enhance awareness of safeguarding while nurturing a more refined civilization of humanity to avoid falling victim to a fraudulent ploy. The goal of these well-planned assaults is to steal sensitive information or trick targets into doing what the attackers want them to do through email exchanges or malicious and counterfeit software posing as a legitimate platform and urging compliance. Instances encompass personal credit card particulars and passwords. The manipulation of society represents one of the most formidable obstacles to network security, as it capitalizes on the inherent human inclination to bestow trust. To conclude, I propose a few preventative measures and potential resolutions to the perils and vulnerabilities of societal manipulation.

Francois et al. [60] The SEADM's underlying limited state system is asserted in this study. The model's effectiveness in preventing social engineering attacks employing two-way, one-way, or indirect communication has been validated. A more accurate picture of the model's cognitive processes may be obtained by speculating about and investigating the model's basic finite-state machine. Limited-state machines provide a more conceptual and adaptable model that emphasizes the relationships between task types connected to various situations, in contrast to the current model that provides a detailed, step-by-step approach for creating detection systems for social engineering assaults. To facilitate the inclusion of organization-specific enhancements more rapidly, the limited state machine classifies related tasks into separate categories, which are further subdivided into several states.

Yuanyuan et al. [61] This paper presents a novel framework for identifying social engineering attacks employing a deep neural network. The current methodologies for social engineering detection, encompassing phishing, deception, and content-based detection, are critically examined. Furthermore, an in-depth analysis of deep learning algorithms with exceptional data performance is conducted. The attention-based Bi-LSTM is employed to capture and extract the semantic context from natural language in chat history. Additionally, ResNet integrates user and content characteristics for classification and judgment. By elucidating the characteristics of social engineering attacks and online conversations, the proposed model's viability and efficacy are substantiated through algorithm selection and applicability.

Kesari et al. [62] The task involves harmonizing diverse A.I. algorithms, namely Logistic Regression, Naive Bayes, Decision Trees, and Gradient Booster. This amalgamation forms a flawless framework, one that is astoundingly intelligent. Consequently, they have successfully implemented this exemplary model to forge a comprehensive email security system. This system effectively combats the prevailing threat of social engineering attacks. The authors have duly provided source validation, spam detection, extensive content scanning, and URL extraction.Additionally, they have meticulously analyzed the model, utilizing many performance metrics. These metrics encompass performance accuracy and execution time. Moreover, the creators have adeptly elucidated how this methodology can bolster the development of an intelligent and precise model. Such a model can be aptly tailored to meet the specific requirements of various organizations.

Noor Faisal et al. [63] This quest for knowledge embarks on a journey exploring three exquisite machine learning algorithms, all harmoniously working together to unravel the mysterious realm of predicting the enigmatic phishing status of any given website. Throughout the arduous path of experimentation, these unparalleled models were painstakingly trained, drawing inspiration from the very essence of the URLs themselves. Furthermore, a valiant effort was undertaken to thwart the treacherous Zero-Day attacks, where a visionary software proposal emerged capable of discerning between the virtuous sanctity of legitimate websites and the dangerous waters of phishing websites, all through an intricate URL analysis. This proposed model, magnificent in its design, showcases a graceful combination of swiftness and efficiency, as it elegantly relies solely on the URL for its profound analysis without the need for other extraneous resources, thus distinguishing itself from the previous studies in a most remarkable manner.

Ajeetha & Priya [64] A groundbreaking technique has been used to identify widespread refusal of service onslaughts via the imprints within the course of traffic. An enigma array has been created from these imprints. Two categorizers, Uninformed Bayes and Haphazard Woods, categorize the traffic as aberrant or typical, employing the characteristic and onslaught contours acquired from existing datasets. The uninformed Bayes formula yields superior outcomes compared to the Haphazard-Woods formula.

3. Conclusion:-

In finality, it is of utmost significance to acknowledge that identifying fraudulent activity is a pivotal realm of apprehension and presents a grave hazard to the safety and fortification of the online domain. So, we focused on the newest research and studies that showed promising results in the area of fraud using the power of automated learning systems and the quality of the haphazard woodland mechanism. This would lead to even better fraud detection by quickly giving all users access to the best attributes.

References

1. R,Kalniņš,J. Puriņš,G. Alksnis, "Security Evaluation of Wireless Network Access Points", Applied Computer Systems, 2017. 21(1): p. 38-45.
2. F,Salahdine , N. Kaabouch, "Social engineering attacks: A survey", Future Internet, 2019. 11(4): p. 89.
3. N .Pokrovskaia, N.S.O. Snisarenko," Social engineering and digital technologies for the security of the social capital'development. in 2017 International Conference", Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS). 2017. IEEE.
4. A.M .Aroyo,"Trust and social engineering in human robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations or gamble?", IEEE Robotics and Automation Letters, 2018. 3(4): p.3701-3708.
5. M.Arana,"How much does a cyberattack cost companies", Open Data Security, 2017: p. 1-4.
6. C. Atwell, T. Blasi, , T. Hayajneh.," Reverse TCP and social engineering attacks in the era of big data", in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart

Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS). 2016. IEEE.

7. F.Mouton, L. Leenen, H.S.Venter, "Social engineering attack examples, templates and scenarios",Computers & Security, 2016. 59: p. 186-209.
8. P.L.Gallegos-Segovia,"Social engineering as an attackvector for ransomware", in 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), 2017. IEEE.
9. E.O.Yeboah-Boateng,P.M. Amanor, "Phishing, SMiShing & Vishing: an assessment of threats against mobile devices", Journal of Emerging Trends in Computing and Information Sciences, 2014, 5(4): p. 297-307.
10. K. Ivaturi , L. Janczewski, "A Taxonomy for Social Engineering attacks", Int. Conf. Inf. Resour. Manage, pp. 1–12, 2011, [Online]. Available: https://pdfs.semanticscholar.org/9a86/754bf4481b06da7a90a62d3b9c0da9ffe72d.pdf.
11. P.L.Gallegos-Segovia, "Social engineering as an attack vector for ransomware", in 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), 2017. IEEE.
12. A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: Affect-based model," in Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for. IEEE, 2013, pp. 508–515.
13. L. Astakhova and I. Medvedev, "Scanning the Resilience of an Organization Employees to Social Engineering Attacks Using Machine Learning Technologies," 2020, doi: 10.1109/USBEREIT48449.2020.9117746.
14. J. R. C. Nurse and J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," Oxford Handb. Cyberpsychology, pp. 662–690, 2019, doi: 10.1093/oxfordhb/9780198812746.013.35.
15. K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," J. Inf. Secur. Appl., vol. 22, no. October 2017, pp. 113–122, 2015, doi: 10.1016/j.jisa.2014.09.005.
16. D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse social engineering attacks in online social networks," 2011, doi: 10.1007/978-3-642-22424-9_4.
17. S. Lohani, "Social Engineering: Hacking into Humans," Int. J. Adv. Stud. Sci. Res., vol. 4, no. 1, p. 10, 2019.
18. P. P. Parthy , G. Rajendran, "Identification and prevention of social engineering attacks on an enterprise," Proc. - Int. Carnahan Conf. Secur. Technol., vol. 2019-Octob, 2019, doi: 10.1109/CCST.2019.8888441.
19. D. van Liempd, A. Sjouw, M. Smakman, and K. Smit, "SOCIAL ENGINEERING AS AN APPROACH FOR PROBING ORGANIZATIONS TO IMPROVE IT SECURITY: A CASE STUDY AT A LARGE INTERNATIONAL FIRM IN THE TRANSPORT INDUSTRY," 2019, doi: 10.33965/es2019_201904l015.
20. M. I. Mann, Hacking the human: social engineering techniques and security countermeasures. Gower Publishing, Ltd., 2012.
21. I.Ghafir , V.Prenosil, a.Alhejailan,m.Hammoudeh," Socialmengineering attack strategies and defence approaches",IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloudm 2016),2016, DOI: https://doi.org/10.1109/FiCloud.2016.28
22. S. Satish, "Educating computer users concerning social engineering security threats," Feb. 10 2015, uS Patent 8,955,109.
23. X. R. Luo, R. Brody, A. Seazzu, and S. Burd, "Social engineering: The neglected human factor for," Managing Information Resources and Technology: Emerging Applications and Theories: Emerging Applications and Theories, p. 151, 2013.
24. K. Beckers, L. Krautsevich, A. Yautsiukhin, "Using attack graphs to analyze social engineering

threats," International Journal of Secure Software Engineering (IJSSE), vol. 6, no. 2, pp. 47–69, 2015.

25. P.Patil, P. Devale, "A literature survey of phishing attack technique", Int. J. Adv. Res. Comput. Commun. Eng, 2016. 5: p. 198-200.
26. L.Peotta, "A formal classification of internet banking attacks and vulnerabilities", International Journal of Computer Science & Information Technology, 2011. 3(1): p. 186-197.
27. V. Shreeram, M. Suban, P. Shanthi and K. Manjula, "Antiphishing detection of phishing attacks using genetic algorithm," 2010 International Conference on Communication Control and Computing Technologies, Ramanathapuram, 2010, pp. 447-450, doi:10.1109/ICCCCT.2010.5670593.
28. H. Huang, J. Tan and L. Liu, "Countermeasure Techniques for Deceptive Phishing Attack," 2009 International Conference on New Trends in Information and Service Science, Beijing, 2009, pp. 636-641, doi: 10.1109/NISS.2009.80.
29. M. N. Feroz and S. Mengel, "Phishing URL Detection Using URL Ranking," 2015 IEEE International Congress on Big Data, New York, NY, 2015, pp. 635-638, doi: 10.1109/BigDataCongress.2015.97.
30. S. Abu-Nimeh and S. Nair, "Bypassing Security Toolbars and Phishing Filters via DNS Poisoning," IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, New Orleans, LO, 2008, pp. 1- 6, doi: 10.1109/GLOCOM.2008.ECP.386.
31. J. Erkkila, "Why we fall for phishing", Proceedings of the SIGCHI conference on Human Factors in Computing Systems CHI 2011 ACM, 2011.
32. A. Alamgir. "Preventing phishing attacks using one time password and user machine identification." ,arXiv preprint arXiv:1305.2704 (2013).
33. s.hossain,d.sarma,r.j.chakma," Machine Learning-Based Phishing Attack Detection", (IJACSA) International Journal of Advanced Computer Science and Applications,2020,Vol. 11, No. 9.
34. A. Belabed, E. Aïmeur , A. Chikh, "A Personalized Whitelist Approach for Phishing Webpage Detection," 2012 Seventh International Conference on Availability, Reliability and Security, Prague, 2012, pp.249-254, doi: 10.1109/ARES.2012.54.
35. M.Alsaleh, A.Alarifi , F.Al-Quayed, A.Al-Salman," (2015) Combating Comment Spam with Machine Learning Approaches", 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), doi:10.1109/icmla.2015.192.
36. A.Cuzzocrea , F.Martinelli, F. Mercaldo, "(2018). Applying Machine Learning Techniques to Detect and Analyze Web Phishing Attacks", Proceedings of the 20th International Conference on Information Integration and Web-Based Applications & Services - iiWAS2018.doi:10.1145/3282373.3282422.
37. S. Carolin, E. B. Rajsingh, "Phishing URL detection-based feature selection to classifiers", International Journal of Electronic Security and Digital Forensics 9.2 (2017): 116-131.
38. D.Arun, L. Brown, "Phishing websites detection using machine learning" ,(2019).
39. Jian,"Phishing page detection via learning classifiers from page layout feature." EURASIP Journal on Wireless Communications and Networking 2019.1 (2019): 43.
40. N. Sanglerdsinlapachai , A. Rungsawang, "Using Domain Top-page Similarity Feature in Machine Learning-Based Web Phishing Detection" ,2010 Third International Conference on Knowledge Discovery and Data Mining, Phuket, 2010, pp. 187-190, doi:10.1109/WKDD.2010.108.
41. O. Koray, "Machine learning based phishing detection from URLs", Expert Systems with Applications 117 (2019):345-357.
42. K. Tian, T. K.Steve, H. Hu, D.Yao, G. Wang", 2018. Needle in a Haystack: Tracking Down Elite Phishing Domains in the Wild", In Proceedings of the Internet Measurement Conference 2018 (IMC '18). Association for Computing Machinery, New York, NY, USA, 429–442. DOI:

https://doi.org/10.1145/3278532.3278569.

43. T. Yue, J. Sun and H. Chen, "Fine-Grained Mining and Classification of Malicious Web Pages," 2013 Fourth International Conference on DigitalManufacturing & Automation, Qingdao, 2013, pp. 616-619, doi: 10.1109/ICDMA.2013.145.

44. S.Mhapankar, R.Bhddha, A.Kharuk, R.Patil," A Machine Learning Approach for Phishing Attack Detection", Journal of Artificial Intelligence and Technology,2023, DOI:https://doi.org/10.37965/jait.2023.0197.

45. A.Assefa , R.Katarya," Intelligent Phishing Website Detection Using Deep Learning", 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS),2022,DOI:10.1109/ICACCS54159.2022.9785003.

46. A.Veach , M. Abualkibash," Phishing Website Detection Using Several Machine Learning Algorithms: A Review Paper" ,international journal of informatics , information systems and computer engineering, https://doi.org/10.34010/injiiscom.v3i2.

47. Al.Abu Zuraiq,M.Al-kasassbeh, " Phishing Detection Based on Machine Learning and Feature Selection Methods",2019, https://doi.org/10.3991/ijim.v13i12.11411.

48. A. A. Alsufyani , 2 S. Alzahrani , " SOCIAL ENGINEERING ATTACK", International Journal of Advanced Res earch in Engineering and Technology (IJARET), DOI:10.34218/IJARET.11.11.2020.089

49. J. C. Lopez,J. E. Camargo, " Social Engineering Detection Using Natural Language Processing and Machine Learning" , 2022 5th International Conference on Information and Computer Technologies (ICICT) , DOI: 10.1109/ICICT55905.2022.00038.

50. S. Abdulmunem, M. Al-Juboori , F. Hazzaa , Z. S. Jabbar ,S. Salih , H. M. Gheni ," Man-in-the-middle and denial of serviceattacks detection using machine learning algorithms", Bulletin of Electrical Engineering and Informatics, DOI: 10.11591/eei.v12i1.4555.

51. u.a.buut,r.amin,h.aldabbas,s.mohan,b.alouffi,a.ahmadian," Cloud-based email phishing attack using machine and deep learning algorithm", Complex Intelligent Systems,2023,doi.org/10.1007/s40747-022-00760-3.

52. d.v.grbic,i.dujlovic," Social engineering with ChatGPT", 2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH),2023, DOI: 10.1109/INFOTEH57020.2023.10094141.

53. C.k. Jia, Y.c. Liu,Y.l. Chen," Face morphing attack detection based on high-frequency features and progressive enhancement learning", School of Electrical and Information Engineering, Hunan Institute of Traffic Engineering, Hengyang, China,2023, doi.org/10.3389/fnbot.2023.1182375

54. m.hussain,s.siddiqui,n.islam," Social Engineering and Data Privacy", Fraud Prevention, Confidentiality, and Data Security for Modern Businesses,2023, DOI: 10.4018/978-1-6684-6581-3.ch010.

55. M.Lansley,F.Mouton,S.Kapetanakis,N.Polatidis," SEADer++: social engineering attack detection in online environments using machine learning",JOURNAL OF INFORMATION AND TELECOMMUNICATION,2020, doi.org/10.1080/24751839.2020.1747001.

56. Y. Aun, M.L. Gan ,N. H. B. Abdul Wahab , G. H. Guan," Social Engineering Attack Classifications on Social Media Using Deep Learning",Computers, Materials & Continua Tech ,2023,DOI: 10.32604/cmc.2023.032373.

57. F. Salahdine, Z. El Mrabet, N. Kaabouch," Phishing Attacks Detection A Machine Learning-Based Approach",2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON),2021, DOI: 10.1109/UEMCON53757.2021.9666627.

58. N. Tsinganos, G. Sakellariou, P. Fouliras, I. Mavridis," Towards an Automated Recognition System for Chat-based Social Engineering Attacks in Enterprise Environments", ARES '18: Proceedings of the 13th International Conference on Availability, Reliability and Security,2018, https://doi.org/10.1145/3230833.3233277

59. F. AL-Otaibi , E. S. Alsuwat,"A STUDY ON SOCIAL ENGINEERING ATTACKS: PHISHING ATTACK",International Journal of Recent Advances in Multidisciplinary Research,2020, Vol. 07, Issue 11, pp. 6374-6380.
60. F. Mouton, A. Nottingham,L. Leenen,H.S.Venter,"Underlying finite state machine for the social engineering attack detection model", 2017 Information Security for South Africa (ISSA),2017,DOI: 10.1109/ISSA.2017.8251781.
61. Y. Lan, " Chat-Oriented Social Engineering Attack Detection Using Attention-based Bi-LSTM and CNN", 2021 2nd International Conference on Computing and Data Science (CDS),2021,DOI: 10.1109/CDS52072.2021.00089.
62. k. sathvik, P.Gupta ,S. S. Sitra, N. Subhashini , S. Muthulakshmi," Social Engineering Attack Detection Using Machine Learning",Advances in Distributed Computing and Machine Learning,2023, DOI https://doi.org/10.1007/978-981-99-1203-2_27.
63. N. F. Abedin, R. Bawm, T. Sarwar, M. Saifuddin, M. A. Rahman, S. Hossain," Phishing Attack Detection using Machine Learning Classification Techniques",2020 3rd International Conference on Intelligent Sustainable Systems (ICISS),2020,DOI: 10.1109/ICISS49785.2020.9315895.
64. G. Ajeetha ,G. M. Priya," Machine Learning Based DDoS Attack Detection", 2019 Innovations in Power and Advanced Computing Technologies (i-PACT),2019,DOI: 10.1109/i-PACT44901.2019.8959961.