Hindawi
Scientific Programming
Volume 2021, Article ID 9957323, 9 pages
https://doi.org/10.1155/2021/9957323

*Research Article*

# Cluster-Based Antiphishing (CAP) Model for Smart Phones

**Mohammad Faisal** [1] **and Sa'ed Abed** [2]

[1]*Department of Computer Science and IT, University of Malakand, KPK, Pakistan*
[2]*Computer Engineering Department, College of Engineering and Petroleum, Kuwait University, Kuwait City, Kuwait*

Correspondence should be addressed to Sa'ed Abed; s.abed@ku.edu.kw

Received 30 March 2021; Accepted 24 June 2021; Published 8 July 2021

Academic Editor: Shah Nazir



Different types of connectivity are available on smartphones such as WiFi, infrared, Bluetooth, GPRS, GPS, and GSM. The ubiquitous computing features of smartphones make them a vital part of our lives. The boom in smartphone technology has unfortunately attracted hackers and crackers as well. Smartphones have become the ideal hub for malware, gray ware, and spyware writers to exploit smartphone vulnerabilities and insecure communication channels. For every security service introduced, there is simultaneously a counterattack to breach the security and vice versa. Until a new mechanism is discovered, the diverse classifications of technology mean that one security contrivance cannot be a remedy for phishing attacks in all circumstances. Therefore, a novel architecture for antiphishing is mandatory that can compensate web page protection and authentication from falsified web pages on smartphones. In this paper, we developed a cluster-based antiphishing (CAP) model, which is a lightweight scheme specifically for smartphones to save energy in portable devices. The model is significant in identifying, clustering, and preventing phishing attacks on smartphone platforms. Our CAP model detects and prevents illegal access to smartphones based on clustering data to legitimate/normal and illegitimate/abnormal. First, we evaluated our scheme with mathematical and algorithmic methods. Next, we conducted a real test bed to identify and counter phishing attacks on smartphones which provided 90% accuracy in the detection system as true positives and less than 9% of the results as true negative.

## 1. Introduction

A phishing attack is used to obstruct and limit legitimate user access to resources of service providers on global networks. A phish exploits the victim's systems resources to acquire confidential and nonconfidential data. The phishing attack can be single and standalone on the system resources or can be distributed, known as a phishing Distributed Denial of Services (DDOS) attack. Phishing attack focuses on a single system by using different launching pads [1]. Although it is not mandatory for both standalone and distributed phishing attacks to harm the data permanently and directly, it is certain that they deliberately compromise all the resource availability for cornerstone security services. Phishing attacks craft congestion in networks by spawning tremendous data traffic in the vicinity of the victim's system, which is adequate to thwart a legitimate packet from reaching its destination. In phishing attacks, the attacking traffic not only contaminates legitimate users but also attacks the target system, either to downgrade the system performance or, in some cases, to stop the service availability. Compared to other cyberattacks, phishing attacks are harder and more complex to circumvent [2]. Most often, phishing attacks exploit network bandwidth and connectivity, downgrading performance in systems they are compromising, whether during network-based attacks or host-based attacks, as shown in Figure 1. Consequently, phishing attacks are successful at halting, interrupting, and demoting the real-time performance of the system by draining all its resources [3].

Figure 1 shows multiple-incident level attacks that can occur on smartphones. Among these attacks, a phishing attack is the worst as its damages smartphones compared to other attacks such as ransomware, backdoors, Denial of Service (DOS)/(DDOS), bot activity, and worm propagation. A phishing attack harms smartphones in both active and

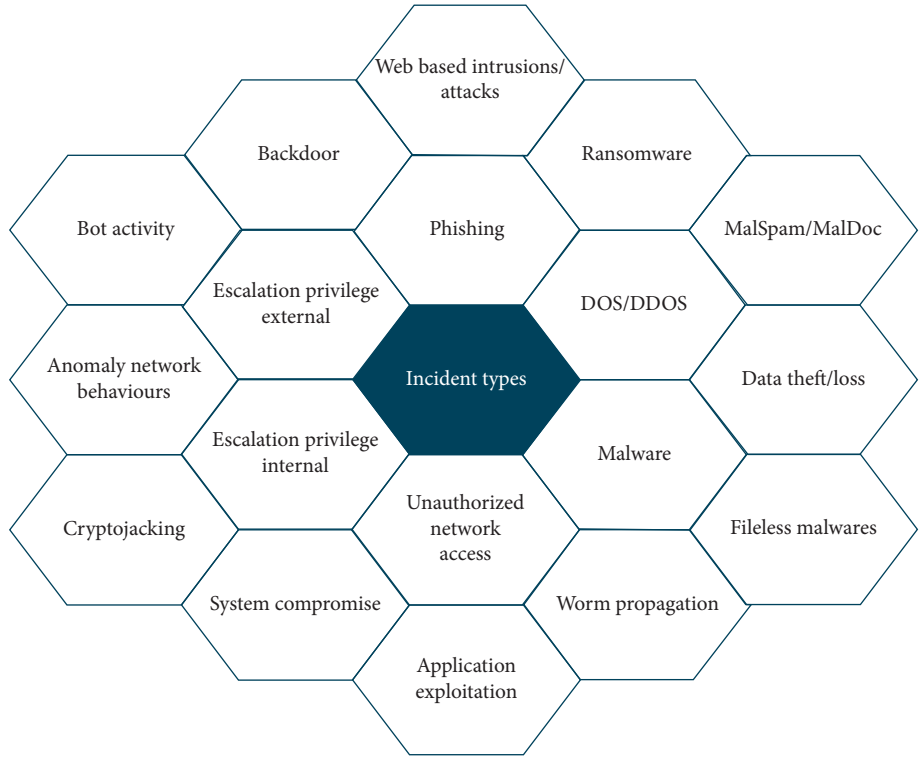


Figure 1: Smartphones incident types.

passive attack scenarios. In active attack scenarios, a phishing attack damages all the data content of the smartphones, while in passive attack scenarios, a phishing attack uses the smartphone as a launching pad against other systems after compromising the system. The additional attacks mentioned in Figure 1 target the system in either active or passive mode. For example, other attacks in Layer 1 are DOS/DDOS, escalation privileges (internal/external), unauthorized access, and malware, which are active attacks only. Similarly, if we examine Layer 2 of Figure 1, different attacks are seen, which can be easily classified as active or passive. In this work, the challenge in all the various incident types is the phishing attack, where an intruder can harm the victim in both an active and passive manner.

Confidentiality, integrity, and availability (CIA) are the main trivet underlying security services. Avoiding any one of these tenets deliberately or inadvertently might lead to open security breaches and unresolved vulnerabilities, consequently leading to a loss of credentials, reputations, and financial gains. Hence, the focus on web security against phishing attacks is necessary and must counter the latest exploitation techniques [3]. Among all cyberattacks, phishing attacks appear friendly but target financial transactions and highly confidential data. Their exploitation might result in the disappearance of financial gains and critical losses. Phishing attacks employ spam emails that attack online banking and money transfer accounts, all of which contain secret pins and passwords for user authentication, which is why hackers focus on banking and money transfer websites [4].

Cluster-based searching is vital, particularly in cybersecurity, because the algorithms use Markov chains to rank the data into clusters. Also, cluster-based searches work on probability, in which clustering is more appropriate for the query in process. Cluster-based searches also save battery life and execution time for smartphones.

The following are the objectives of this work:

(1) To counter the phishing attacks on smartphones.

(2) To falsify the fake websites containing phishing scams into a cluster form.

(3) To report the true positives and true negatives.

(4) To gray list and then blacklist the phishing attack links

The paper is organized as follows: Section 2 elaborates the literature review with critical analysis along with the security trial parameters. Section 3 explains the proposed scheme. Experimental results are evaluated with the help of detailed algorithms and mathematical and statistical methods. With assistance from the Weka tool and JavaScript language, a real test bed experiment was conducted using datasets from UCI and Mendeley, which are discussed in Section 4. Finally, Section 5 summarizes the key findings and presents our future trends.

## 2. Literature Review

Tools such as the Global System for Mobile (GSM), General Packet Radio Services (GPRS), enhanced data rates for GSM evolution (EDGE), Universal Mobile Telecommunication

System (UMTS), Bluetooth, and infrared make smartphones as a device of connectivity. However, this connectivity also serves as a gateway for malware, gray ware, and spyware. The GSM global communications expertise of another generation-2G enables the messaging among smartphones and sorted locations by exchanging the subsystem's replaced first-generation (1G) analog-centered facilities for a numerical, complete duplex and circuit substituted network for voice telephony [4].

GPRS 2.5-generation technology developed to improve the data rates and decrease the connection access time for 2G. Implementing the packet switching mechanism and introducing the Wireless Access Protocol (WAP) and Multimedia Messaging Services (MMS). EDGE improved GPRS features with an enhancement of its data rates and service reliability [5].

The UTMS, developed in 2002 attained a data rate perimeter of 2 Mbps together for packet and circuit-switching networks sustained concurrently. Several facilities can be entered instantaneously by the consumer such as streaming, discussions, and collaborations with colleagues. Bluetooth was industrialized in 1999, grounded on radio-broadcast small wavelengths customary for data communication as well as private area networks. Bluetooth provided an optimal level of security and a small array of communications up to 100 meters with negligible charge and ingestion [6, 7].

Based on the legality, delivery methods, and user authentication, mobile threats are classified into three main categories: malware, gray ware, and spyware, with regard to assorted attack vectors, motivations, and defense mechanisms [8].

For launching cyberattacks, all illegitimate activities such as spam emails and messages and twitter messages are exploited for smartphones. These cyberattacks either damage all the data contacted in the smartphones or compromise the smartphone to use it as a launching pad against other platforms. In [9–11], all schemes used data-mining techniques in different ways to counter cyberattacks on smartphones.

In [12, 13], the authors highlighted phishing attacks targeting smart grids to launch a phishing attack and compromise the system data to roll back the system. The authors proposed a data-mining technique to identify and counter phishing attacks and falsify fake pages and messages.

Table 1 shows the critical evaluation of the literature review with respect to the classifications. The table consists of six columns, in which the first column states the approach of the scheme with its reference, while the second column explains the classification of the category where the scheme is occurring.

In the third column, the mechanism of the antiphishing scheme and how the scheme is working are briefly stated. In the fourth column, the contribution or the strength of the scheme is highlighted with its achievements. In the fifth column, the weaknesses or the limitations of the scheme are mentioned with its possible vulnerabilities. In the sixth column, we mentioned the implementation scenario that in which scenario the scheme is implemented. In the last column, there is the tool/technology used by the scheme mentioned in the literature.

The main emphasis of malware is to annoy the genuine consumers, damaging the platform, cutting the reserved data, or misusing the scheme or policy susceptibilities irrespective of any notice to the victim users. Malware includes viruses, worms, Trojans, rootkits, and botnets. A computer virus is defined as a self-replicating piece of code, and a worm is a self-copying program [19], Trojans impersonate software that appears to provide services but in reality is a malicious program. A rootkit installs Trojans after which it then disables firewalls and antiviruses. Finally, botnets are a complete set of device viruses that infect victims for organized crime, consisting of a group of "zombies"; each is an infected computer or device [20].

Malware is prohibited in numerous countries, such as the United States, and in some cases of malware sharing, jail sentences have been administered [21].

Determining the position of a node and retrieving its history for a specific span of time is the main objective of the spyware. Depending on the practical circumstances, spyware may be genuine or illicit. For example, if a person is going to install personal spyware on his children or spouse's smartphone, the spyware is not going to cheat the victim. However, if the spyware is installed without the user's consent and successfully gains access to the device, sending confidential information to the intruder rather than the real author, then it is illegitimate [22].

Accumulating consumer evidence for the sole tenacity of summarizing and then advertising are the main intentions of gray ware, as indicated in Table 2. The gray ware distributor's corporate objectives are not to harm the user but rather to provide some sort of functionality and importance to the host user. If a user finds that the data collection process of gray ware is questionable, the user can complain and block the services of the gray ware. In contrast to malware and spyware, the illegal use of gray ware is punished by fines rather than any personal statements in countries where there is a rule of law. Therefore, gray ware is sometimes identified as laying at the boundary of legitimacy and illegitimacy. Based on the dogma of confidentiality and the consumer's rights of grievances, gray ware companies must disclose their compilation practices [23–26].

Another novelty of this research is that we classify schemes in a unique way that can be easily detected. We organized phishing attacks into multiple classes so that each category was tested against our proposed scheme of the CAP model. Based on the literature review, we classified the phishing attacks as shown in Figure 2. The main categories include Internet Protocol (IP), Uniform Resource Locator (URL), Domain Name System (DNS), certificate-based, social engineering, and technical maneuver [27–29].

In the first category, IP-based phishing attacks are classified. In the second category, URL-based phishing techniques are classified, which are subclassified into abnormal URL, URL of anchor, URL of long address, and repeating the same characters of the URLs. In the third category, we classified all phishing attacks based on social engineering. In the fourth category, we classified all phishing attacks that can be caused by technical maneuvers. In the fifth category, we classified phishing attacks that can occur from DNS poisoning. In the last category, we classified

Table 1: Critical review of the literature schemes.

| Approach | Classification diagram | Mechanism | Contribution | Limitations | Implementation scenario | Technology/ algorithms used/tools |
|---|---|---|---|---|---|---|
| Network-level protection [14] | IP | Internet service providers database is used | Attack detection good, offender address list is up to date | Rule tuning, message content not verified | DNS | Snort |
| Authentication [15] | Certificates | User, domain, e-mail, and transaction based authentication based on digital signatures and hashing | Less complexity, no need of inter e-mail domains cooperation, enhance security | Vulnerable to man-in-the-middle attacks, technology constraints | Hotmail, Yahoo, Gmail | PGP, S/MIME |
| Client-side tools [16] | URL | Whitelisting and blacklisting | Legitimate e-mail will be acceptable only, best for already known phishing websites | High false positive and false negative rate for white- and blacklisting respectively | Mozilla, Firefox, and Internet Explorer browsers | Net craft, eBay toolbar, IE phishing filter |
| User education [17] | Social engineering | Online material, online test, and contextual training | Authority, attractive and impressive | False negative | All scenarios | Smart OS |
| Server-side filters and classifiers [18] | Technical maneuvers | Compare multiple classifiers and clustering techniques | Discover phishing attacks with narrow earlier knowledge | Time and space tradeoff | Internet browsers | Support vector machines |

Table 2: Security trials of smartphones platforms (OS).

| Security trials | Android | Nokia-Ovi | Apple iOS (iPhone OS) |
|---|---|---|---|
| Software installation markets | Allowed from both official Android market and unofficial sites | Allowed from both official Symbian market and unofficial sites | Allowed only from official sites Apple App Store |
| Grant permissions | Installation time-extensive fully | Only for unsigned Symbian | Runtime user permission only |
| Spyware and gray ware permissions | Allow and available at Android market | Allow | Disallow both |
| Premium SMS | Did not require user confirmation | Did not require user confirmation | Require user confirmation |
| SMS spam | Possible | Possible | Not easily allowed |

attacks that can occur via digital certificates. This category is subclassified into Secure Socket Layer (SSL) and centralized authority certificates.

## 3. Proposed Schemes

A novel cluster-based antiphishing (CAP) mechanism, which addresses the following concerns, is necessary to secure users from cybersecurity attacks. For example, to thwart admittance of phishing websites/phishing attacks, to shield vital e-mail communication from phishes, to perceive deceptive website via (a) Appropriate Domain Name System and IP/MAC addresses toning and (b) authentication followed by authorization of website, data trickle consequential from device damage or robbery, inadvertent confession of data from smartphones, assault on decommissioned smartphones, mitigate spyware attacks, supervise network spoofing attacks, and financial malware attacks.

Our scheme operates in three main phases. In the first phase, the classification of incoming data is observed on the basis of a map provided in the second phase. In the second phase, packets are being clustered into their classified groups. In the third phase, digital forensics of the malicious packets are investigated, tracking back the culprits for future blacklists or recovery that can be used as a honey pot. As our scheme focuses on smartphones, which are capable of using only lightweight software, we designed our novel solution for implementations on base stations (centralized) rather than smartphones (distributed). This focus allows for placing all of the mechanisms in one package because the smartphone market is full of variants with different architectures of software and hardware. For smartphones, not only the attack (phishing) is distributed but also the tools and techniques are multiple and distributed in nature, such as social engineering and website spoofing techniques.

## 4. Results and Discussion

The CAP mechanism is elaborated in the following three evaluation methods: (1) algorithms, (2) mathematical and statistical formulae and tools (e.g., SPSS), and (3) test bed

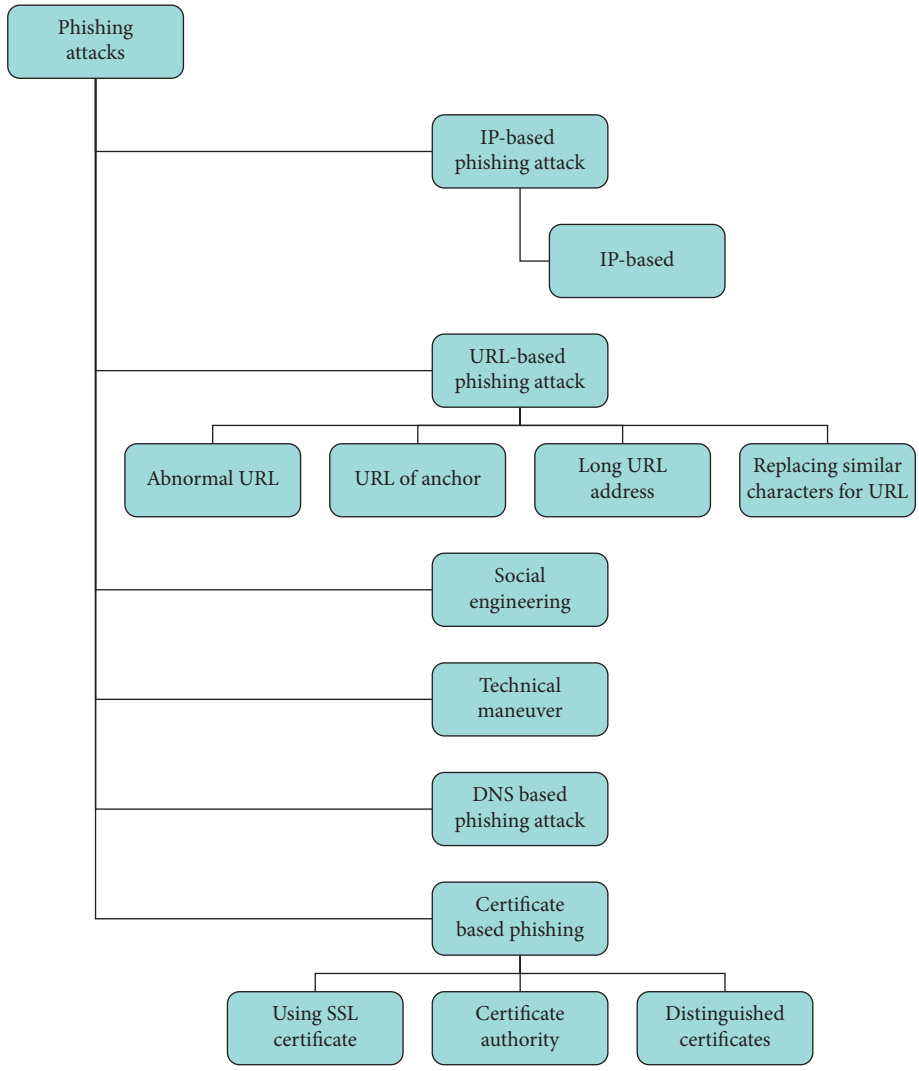


Figure 2: Classification of phishing attacks.

implementation via the Wireshark tool. The evaluation matrix consists of the following four main components: "true positive" measures the rate of correctly detected phishing attacks relative to overall prevailing phishing attacks; "true negative" measures the proportion of appropriately noticed genuine occurrences in relation to completely prevailing genuine occurrences; "false positive" measures the proportion of genuine occurrences that are inaccurately identified as phishing attacks relative to completely prevailing genuine occurrences; and finally, "false negative" measures the rate of phishing attacks that are inaccurately noticed as genuine relative to entirely prevailing phishing attacks.

*4.1. Algorithm.* In this section, the pseudocode of the CAP mechanism algorithm exploiting the IRC messenger of a smartphone is shown in Algorithm 1. In Step 1, we defined all the parameters involved in the execution of our scheme: PS, $N$, $S$, $E$, C, $M$, and $P$, all of which are labelled as described. In Step 2, the values received by the scheme as inputs will be validated, and each entry is executed as with FOUR subsequent IF and ELSE conditions. For example, if the argument $E$ is received, then it means end times of communication or NULL value; if the argument $C$ is received, then the channel name is identified through which the communication is required; if argument $M$ is received, then the Internet Relay Chat (IRC) messenger will be communicated; and if argument $P$ is received, then the port number is received through which the communication will be considered. In Step 3, once the communication is initiated with the IRC messenger, then a connection object is created in Step 4. Subsequently, a channel is created for communication between the nodes. In Step 5, an event handler is activated that is already defined in JavaScript to monitor malicious activities. The communication is countered if it is malicious; otherwise, it will proceed as normal.

*4.2. Mathematical and Statistical Model.* In our mathematical and statistical model, we attempted to best generalize the CAP model to all possible incoming phishing attacks.

//PS: packet size defined in RFC, $N$: number of packets (date rate) defined in RFC, $S$: start time of the data communication, $E$: end time of data communication, $C$ for channel name, $M$ for IRC messenger/IRC name, $P$ for port number.

(1) Assignment and validating entries/values of the parameters defined
$\sum(S, E, C, M, P)$ IF $S \geq 0$ THEN $\int T = 0$ IF $E = 1$ THEN ends time of communication ELSE 0, IF $C = 1$ THEN channel name ELSE 0, IF $M = 1$ THEN IRC messenger name ELSE0, IF $P = 1$ THEN port number ELSE 0.
(2) $\int \text{IRC} \sum \text{IRC} \geq 0$
(3) $\int C = 1\, E \leq D$
(4) $€E \int DP$
(5) $\int E = M$ then $\sum M = 0$

Algorithm 1: Phishing attack detection using the CAP algorithm.

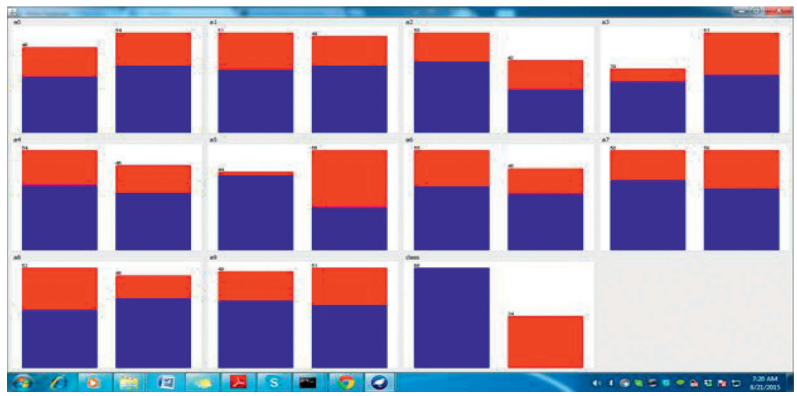


Figure 3: Weka tool results after a phishing attack on a smartphone.

We checked the maximum size and threshold value of the packets as well as their starting and ending limits. Furthermore, we tested combinations of various types of attacks from multiple resources and finally, the probability of the attack to occur:

For all $\sum$ of all bits = packet maximum size (defined in RFC).

$\int$ starting and ending of packets ratio = threshold (defined $n$ RFC).

"Starting" indicates the lower limit and "ending" means the upper limit.

$n$Cr combination of different packets from various resources.

$n\text{Cr} = n!/r!\ (n - \text{r})!$

Where $n$ = for all incoming packets and $r$ = malicious packets.

$n$Pr permutation of different malign and nonmalign packets.

$n\text{Pk} = n!/(n - k)!$

Hence, the probability of launching a successful attack.

*4.3. Implementation via Weka Tool with Results.* Figure 3 shows the results taken by the Weka tool after the successful launching of a phishing attack on a smartphone. To validate our scheme, we considered the following system setup. The principal server where the DNS is laid on is considered as the main target of a phishing attack. The clients are exhausting a JavaScript code to implement bots on the server, while keeping the JavaScript code in an indefinite loop within the malicious code. A Wireshark instrument mounted on the server notices the scheme's position and deployment before and after the attack. Results are displayed in both scenarios in the real test bed implementation phase.

Table 3: Techniques' descriptions.

| A1DE | Average one dependency estimator |
|---|---|
| NB | Naïve Bayes |
| MLP | Multilayer perceptron |
| QDA | Qualitative Descriptive Analysis |
| SVM | Support Vector Machine |
| WiSARD | WiSARD |
| CHIRP | COMPOSITE HYPERCUBE ON ITERATED RANDOM PROJECTION |
| DecisionTable | DecisionTable |
| DTNB | DecisionTable\Naïve Bayes |
| Ridor | Ridor |
| J48 | Decision Tree |

JavaScript code used for phishing attack: the malicious code below was used against our CAP model to test its capability for countering a phishing attack.

```
<html> <head>
hello me PHISHING attack.
</head> <SCRIPT language = JavaScript>
var name = prompt ("R u ready", "Name");
</SCRIPT> <BODY> </BODY> </html>
```

The results are shown in Figure 3, in which the blue shows the true positive data while the red shows the false positive data successfully encountered by our CAP model.

Table 4: Statistical data from UCI datasets.

| Serial number | Technique | Instances | | | Precision | Accuracy (%) |
|---|---|---|---|---|---|---|
| | | Correctly classified | Incorrectly classified | Total | | |
| 1 | A1DE | 1140 | 213 | 1353 | 0.81 | 84.2572 |
| 2 | NB | 1107 | 246 | 1353 | 0.792 | 81.8182 |
| 3 | MLP | 1153 | 200 | 1353 | 0.847 | 85.218 |
| 4 | QDA | 1130 | 223 | 1353 | 0.828 | 83.5181 |
| 5 | SVM | 1131 | 222 | 1353 | 0.83 | 83.592 |
| 6 | WiSARD | 1197 | 156 | 1353 | 0.886 | 88.4701 |
| 7 | CHIRP | 1171 | 182 | 1353 | 0.862 | 86.5484 |
| 8 | DecisionTable | 1133 | 220 | 1353 | 0.816 | 83.7398 |
| 9 | DTNB | 1172 | 181 | 1353 | 0.867 | 86.6223 |
| 10 | Ridor | 1204 | 149 | 1353 | 0.893 | 88.9874 |
| 11 | J48 | 1215 | 138 | 1353 | 0.899 | 89.8004 |

Table 5: Statistical data from Mendeley datasets.

| Serial number | Technique | Instances | | | Precision | Accuracy (%) |
|---|---|---|---|---|---|---|
| | | Correctly classified | Incorrectly classified | Total | | |
| 1 | A1DE | 8724 | 276 | 10000 | 0.872 | 87.24 |
| 2 | NB | 8515 | 1485 | 10000 | 0.864 | 85.15 |
| 3 | MLP | 8694 | 306 | 10000 | 0.869 | 86.94 |
| 4 | QDA | 8657 | 1343 | 10000 | 0.881 | 86.57 |
| 5 | SVM | 8388 | 612 | 10000 | 0.839 | 83.88 |
| 6 | WiSARD | 8733 | 1267 | 10000 | 0.893 | 87.03 |
| 7 | CHIRP | 8633 | 367 | 10000 | 0.863 | 86.33 |
| 8 | DecisionTable | 8526 | 474 | 10000 | 0.853 | 85.26 |
| 9 | DTNB | 8641 | 359 | 10000 | 0.864 | 86.41 |
| 10 | Ridor | 8644 | 356 | 10000 | 0.864 | 86.44 |
| 11 | J48 | 8731 | 269 | 10000 | 0.873 | 87.31 |

The CAP model produces more than 90% accuracy in its detection system, which has been classified as true positive (blue packets). Similarly, the CAP model also reduces the percentage of false negatives (red packets) to a single digit, that is, less than 9%.

*4.4. Real Test Bed Experiment Conducted Using Datasets from UCI and Mendeley.* As per the standard for assessment when evaluating the performance, a 10-time validation is completed for each classifier. A standard methodology examines a dataset by dividing data into 10 equal sizes, in which one set is used for testing and the other is used to train the data until each subset has been used for testing [30]. Investigating antiphishing revealed the following techniques for analysis, evaluation, and experimentations, as provided in Table 3. The 10 different techniques were then used for testing the UCI and Mendeley datasets.

*4.4.1. Dataset Taken from UCI.* Source Neda Abdelhamid, Auckland Institute of Studies, nedah '@' ais.ac.nz.

*(1) Dataset Information*. In online communications such as e-banking and e-commerce, phishing attacks are considered a threat. From 1353 websites, we have collected different issues related to legal and phishing websites (http://www.phishtank.com), where anyone can collect information about phishing attacks. The website used is Yahoo, in which 548 websites out of 1353 found were legitimate using a web script developed in PHP, 702 phishing URLs and 103 suspicious URLs. The results are shown in Table 4.

In the second column of Table 4, different techniques are considered for testing on the UCI datasets. As shown in the third column, the highest correctly classified technique used is J48, with the lowest incorrectly classification specified. However, regarding percentages, J48 is still less effective than our CAP model, which produces 90% true positive and 9% false negative results. As shown in the sixth column, the precision value of the J48 is 0.899, while the accuracy level in the last column is 89.8%. Similarly, if we consider any other technique applied to the UCI datasets shown in Table 4, none can reach the value of 90% accuracy. Therefore, we can deduce that the accuracy of our CAP model is much superior to any other of the latest techniques tested on UCI datasets.

*4.4.2. Dataset Taken from Mendeley.* Source Phishing web page: Phish Tank, Legitimate web page source: Alexa, Common Crawl.

*(1) Dataset Information*. In this scenario, the dataset under consideration is extracted from 10,000 websites; 48 features were extracted from 5000 phishing and legitimate websites. The results are shown in Table 5.

As a second test case, different techniques were considered for Mendeley datasets. As seen in the third column of

Table 5, J48 shows the highest precision (0.873) and accuracy at 87.31%, yet it is still less than our CAP model. We can conclude that by either changing the datasets or the technique, no method can achieve better than our proposed CAP model.

## 5. Conclusion

Fake commercial advertisements can play the role of honey pots for phishing attacks, as they behave like original finance and business sector advertisements. As the users follow, the fake websites and log on once, it is enough for the phishing hackers to steal the passwords and transact according to their own wishes and possibly changing login details. Currently, all phishing hackers must pass through some sort of Internet service providers (ISP), for which the administrator is responsible for countermeasures. Techniques such as content filtering, heuristics engines, IP blacklisting, and fingerprinting are currently employed; however, the problem of spamming followed by phishing is not yet contained. Neither of the schemes in the broad classification above focus on smartphone platforms. All the schemes in this work are silent about the digital forensics of the phishing attack. Our scheme successfully identified and maligned all the phishing attack packets in one single solution. The test bed results showed that the CAP model successfully identified and countered phishing attacks on smartphones. The CAP model produces more than 90% accuracy in its detection system, which has been classified as true positive. Similarly, the CAP model also reduces the percentage of the true negative to a single digit, namely, less than 9%. As a future trend, our model can be extended for Edge, FOG, and cloud computing environments as the CAP model is a lightweight scheme that can easily be integrated into such energy deficient computing zones.

## Data Availability

The data used to support the findings of this study are included within the article.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References


[1] S. Afzal, M. Asim, A. R. Javed, M. O. Beg, and T. Baker, "URLdeepDetect: a deep learning approach for detecting malicious URLs using semantic vector models," *Journal of Network and Systems Management*, vol. 29, no. 3, pp. 1–27, 2021.

[2] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, pp. 1–39, 2021.

[3] A. G. Martín, A. Fernández-Isabel, I. M. de Diego, and M. Beltrán, "A survey for user behavior analysis based on machine learning techniques: current models and applications," *Applied Intelligence*, 2021.

[4] M. H. Siddiqi Abdullah, Y. S. Alhwaiti, I. Alrashdi, A. Ali, and M. Faisal, "Segmentation and classification of heart angiographic images using machine learning techniques," *Journal of Healthcare Engineering*, vol. 2021, Article ID 6666458, 9 pages, 2021.

[5] X. Liao, M. Faisal, Q. Chang, and A. Ali, "Evaluating the role of big data in IIOT-industrial Internet of things for executing ranks using the analytic network process approach," *Scientific Programming*, vol. 2020, Article ID 8859454, 7 pages, 2020.

[6] A. Das, S. Baki, A. El Aassal, R. Verma, and A. Dunbar, "SOK: a comprehensive reexamination of phishing research from the security perspective," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 671–708, 2019.

[7] A. Rana, "Phishing attacks survey: types, vectors, and technical approaches," *Future Internet*, vol. 12, no. 10, p. 168, 2020.

[8] S. Jindal and M. Misra, "Multi-factor authentication scheme using mobile app and camera," *Advances in Communication and Computational Technology*, Springer, New York, NY, USA, 2021.

[9] R. Zhang, X. Wang, X. Yang, and X. Jiang, "Billing attacks on SIP based VoIP systems," in *Proceedings of the 1st USENIX Workshop on Offensive Technologies (WOOT)*, pp. 1–8, Berkeley, CA, USA, August 2007.

[10] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A social network based patching scheme for worm containment in cellular networks," in *Proceedings of the 28th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2009)*, pp. 1476–1484, Rio de Janeiro, Brazil, April 2009.

[11] K. A. Otunaiya and G. Muhammad, "Performance of data-mining techniques in the prediction of chronic kidney disease," *Computer Science and Information Technology*, vol. 7, no. 2, pp. 48–53, 2019.

[12] E. U. Soykan, M. Bagriyanik, and G. Soykan, "Disrupting the power grid via EV charging: the impact of the SMS Phishing attacks," *Sustainable Energy, Grids and Networks*, vol. 26, Article ID 100477, 2021.

[13] A. K. Ghazi-Tehrani and H. N. Pontell, "Phishing evolves: analyzing the enduring cybercrime," *Victims & Offenders*, vol. 16, no. 3, pp. 316–342, 2021.

[14] H. Shahriar and L. Etienne, "Presentation attack detection framework," *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*, Springer, New York, NY, USA, pp. 297–311, 2021.

[15] A. Saxena, N. Sharma, P. Agarwal, and R. Barotia, "Phishing website prediction by using cuckoo search as a feature selection and random forest and BF-tree classifier as a classification method," *Rising Threats in Expert Applications and Solutions*, Springer, New York, NY, USA, 2021.

[16] G. K. Bhageria, V. Ekambaram, and S. K. Rakshit, *Protecting against Notification Based Phishing Attacks*, 2021.

[17] G. Shrivastava, K. Sharma, and S. Rai, "The detection & defense of DoS & DDoS attack: a technical overview," in *Proceedings of the ICC*, pp. 274–282, Kampala, Uganda, 2010.

[18] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the Phishing and Phishing problems," *ACM Computing Surveys*, vol. 39, p. 3, 2007.

[19] D. C. W. M. Wozniak, N. C. N. Meghanathan, and D. Nagamalai, *Advances in Network Security and Applications, Springer, Chennai, India*, 2011.

[20] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, ""Andromaly": a behavioral malware detection framework for android devices," *Journal of Intelligent Information Systems*, vol. 38, no. 1, pp. 161–190, 2012.

[21] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pp. 3–14, Chicaga, IL, USA, October 2011.

[22] P. Porras, H. Saïdi, and V. Yegneswaran, "An Analysis of the iKee.B iPhone Botnet," in *Security and Privacy in Mobile Information and Communication Systems*, pp. 141–152, Springer, New York, NY, USA, 2010.

[23] A. Apvrille, "Symbian worm Yxes: towards mobile botnets?" *Journal in Computer Virology*, vol. 8, no. 4, pp. 117–131, 2012.

[24] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 446–471, 2013.

[25] G. Kambourakis, C. Kolias, S. Gritzalis, and J. H. Park, "DoS attacks exploiting signaling in UMTS and IMS," *Computer Communications*, vol. 34, no. 3, pp. 226–235, 2011.

[26] A. Bose and K. G. Shin, "Proactive security for mobile messaging networks," in *Proceedings of the 5th ACM Workshop on Wireless Security (WiSe'06)*, pp. 95–104, ACM, New York, NY, USA, September 2006.

[27] A. Bose and K. G. Shin, "On mobile viruses exploiting messaging and Bluetooth services," in *Proceedings of the Securecomm and Workshops*, pp. 1–10, Baltimore, MD, USA, 2006.

[28] A. Bremler-Barr, R. Halachmi-Bekel, and K. Kangasharju, "Unregister attacks in SIP," in *Proceedings of the 2nd IEEE Workshop on Secure Network Protocols*, pp. 32–37, Santa Barbara, CA, USA, November 2006.

[29] G. Zhang, S. Ehlert, T. Magedanz, and D. Sisalem, "Denial of service attack and prevention on SIP VoIP infrastructures using DNS flooding," in *Proceedings of the 1st International Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM)*, pp. 57–66, New York, NY, USA, July 2007.

[30] W. Conner and K. Nahrstedt, "Protecting SIP proxy servers from ringing-based denial-of-service attacks," in *Proceedings of the 10th IEEE International Symposium on Multimedia (ISM)*, pp. 340–347, Berkeley, CA, USA, December 2008.