FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 3 No. 3, September, 2019, pp 202- 209

AN ENHANCED INTRUSION DETECTION SYSTEM USING HONEYPOT AND CAPTCHA TECHNIQUES

Abdullahi, M., Aliyu, S. and Junaidu, S. B.

Department of Computer Science, Ahmadu Bello University, Zaria- Nigeria

Corresponding author email: abnaum03@gmail.com

ABSTRACT

Internet is no doubt inevitable as it has a tremendous impact in our lives. Despite its importance, internet comes with many challenges, among which is security. From the literature, several attempts have been made to develop secure and user-friendly spam detection technique. But these attempts linger between these two fundamental issues: the robustness and the usability in CAPTCHA system, passiveness of Intrusion Detection System (IDS), which failed to detect some forms of novel attacks, flexibility to attacks and not efficient to users. In this work, honey CAPTCHA, an enhanced intrusion detection framework is designed to solve the above problems as it is capable of detecting crawlers' attacks, resilient and efficient to users. The system is mainly considered as an option to a CAPTCHA-BASED IDS model, which suffers the above problems. The system outperforms the existing system considering its performance measure based on the proposed metrics that includes detection rate (DR) of 76%, 1.7 times the detection rate of the existing system with false positive rate (FPR) of 10% against the existing system that have 36% FPR, which proved that the system is more robust compared to the existing system. The usability of the system measured using BDR and BNR is 1.5 times that of the existing system, which shows how efficient the system is to users when compared to the existing system. Both systems were compared based on standard IDS evaluation metrics CID which proves that the system is 2.26 times better than the existing system.

KEYWORDS: Intrusion Detection System, Intrusion Prevention System, CAPTCHA, Honeypot, Intrusion Detection Capability (CID)

INTRODUCTION

Computer security is a field in Information Technology (IT) that focuses on the protection of both computer hardware and software resources. The Internet as a major tool in IT needs to be secure as its usage is inevitable. Hence, security on the internet is becoming an appealing area of research. No doubt, Artificial Intelligence comes with a huge progress in the strive for technological advancement, though with the abuse of Artificial Intelligence technology it is now a threat to the development of technology. Cyber-attacks in the past were of concern to office holders and government, but today cyber-attack is a general concern to all as it can trigger war and political instability [1]. There is no defined feature that qualifies anyone that can fall a victim of cyber-crime, apart from being on the internet. Legitimate users of the internet can be attacked by web-bots in many ways, some of which include: social engineering, malvertising, ransomware, phishing and spy phishing, malware, sql injection etc. While attacking users, bots cause a severe harm to the victims ranging from file lost, computer malfunctioning, hardware destruction, and possibly the victim's life. About 4.5 million identities were stolen in 2017 approximately more than the internet users. Hence Cyber-criminals will continuously target identities and steal credential of users [1].

Some of the known threats are DDoS, Pharming, Hacking, Malware, Ransomware, Phishing, Trojan horse, Virus etc.

Measures or techniques used to protect computer and internet resources against those attacks consist of: Authentication, which ensures users is who they claim to be, by establishing proof of identity. Encryption, a process of encoding a message in a way that only authorizes person can access it. Firewall, a network security system that monitors the outgoing and incoming network traffic based on advance and defines set of rules. Intrusion Detection System (IDS), a process use to identify intrusions. Intrusion Prevention System (IPS), a pessimistic techniques use to prevent known intrusion. CAPTCHA are preventive technique that distinguished between computer and human apart. Response time are administrative technique that is use to compliment known techniques to prevent intrusion using timer in a page. Negative Selection Algorithm is bio-inspired techniques that imitate mammalian immune system use to detect anomalies in network traffic.

RELATED LITERATURE

According to the universal usability concept, information and communication systems should be designed in a way that could be used by a broad range of users including those with some disabilities [2].Usability incorporates measurements of efficiency, learnability, memorability, tolerance for error and users satisfaction into the inclusive nature of accessibility testing, ensuring that a product is usable and accessible to a wide range of individuals as possible [3].

Generally, traditional IDS are passive in such a way that they detect and report attacks based on predefined rules. Traditional IDS focus on how to detect attacks base on a given rule, i.e. either assigned or abnormality [4]. That means a new attack that is not defined in the system will not be detected, also some interactions with genuine human may ambiguously be considered as a threat.

[5] Reviewed most of the soft computing techniques used in IDS development. They comprise the biologically-inspired techniques like the genetic algorithm and some major machine learning tools like Fuzzy logic, support vector, artificial neural network. On their conclusion, they emphasized that soft techniques application in IDS and IPS will optimally improve system security.

[6] Developed 'DeCAPTCHA' software which enables the computer to render the CAPTCHA code legible by cleaning up the text. The software was successful in cleaning up 66% of Visa's Authorize.net CAPTCHAs, 70% of Blizzard's Entertainment and 73% of CAPTCHA.com's captcha. [7] Designed a generic method to break all text based CAPTCHAs, which is considered the best in generic attack, with the success rate of 5% to 77%, which can solve a puzzle in less than 15 seconds average speed in a standard desktop. Text-based CAPTCHAs are more of human friendly but vulnerable to attack. [9] Classified methods used to exploit CAPTCHA into three: the Optical Character Recognition (OCR), Learning which used machine learning techniques to break CAPTCHAs and farming that exploit CAPTCHA by exposing it to humans to solve based on a certain reward, known or unknown to the solver.

[2] Reviewed different CAPTCHAs and categorized them into three i.e. the visual, non-visual and hybrid. They evaluate them and suggest some alternatives base on the given criteria that will be considered when prioritizing the selection and implementation of the CAPTCHAs. The criteria consist of the cost, efficiency and robustness on usability. They identified security and usability as the major barrier in CAPTCHA deployment. They suggested some alternatives to CAPTCHA which were categorized into three that includes; Administrative, Interactive and cheating bots and tested by the same CAPCTHA criteria, with great improvement in both the usability and security in their deployment.

[8] Designed fCAPTCHA, which consists of multiple image of human faces and non-face image with varying degree of distortion. Users get access by matching faces belonging to a single individual.

After a comparative analysis of different CAPTCHAs and their alternative, [10] arrived at a conclusion with a suggestion, that honeypots and CAPTCHA have their respective weaknesses and drawbacks that makes them independently less effective, but by integrating and removing the weaknesses will form a viable defense for online system.

[11] Designed a novel image-based CAPTCHA that uses object recognition inspired by negative selection algorithm of the biological immune system. It also has a two-phase filtering algorithm which ensures that the CAPTCHA is resilient to automated attack while remaining easy for human users to solve. The image CAPTCHA is not convenient for users, hence the need to completely eliminate CAPTCHA's should be considered [12].

To eliminate traditional CAPTCHA, Google introduced reCAPTCHA that makes verification simple for users by only clicking on a checkbox while making it harder for bots. The reCAPTCHA works using an advanced risk analysis that comprises of browsing history of the genuine user already tracked by google cookie just to determine the difficulty of challenge that is presented to the user, explores how aspect of the browser environment affects the risk analysis, canvasses rendering techniques to fingerprint users across machines and browsers, identifies how user-agent influence the user's reputation and the timing of movement and movement pattern of mouse to decide what type of challenges will be presented to the user [13].

An advanced no CAPTCHA reCAPTCHA, which is invisible to human, was introduced in 2017 by Google due to the trouble with reCaptcha that drives users to the extreme edge of sanity. The invisible CAPTCHA shows no challenge to user, instead it returns probability scores between 0.0 (100% bots) and 1.0 (100% human) [14].

The limitation of the Google reCAPTCHA in general is that a user looks suspicious with reason not directly connected or even clear to him, for example, having an outdated version of browser. With this, users are presented with a dreaded CAPTCHA for advanced verification and also machine can solve up to 70.78% of image reCAPTCHA [13].

Also, the latest no CAPTCHA reCAPTCHA users have no false positive fallback and opportunity for actual humans to prove wrong the decision of the system in case you receive a low score [14]. Google reCAPTCHA used their long-acquired database for the analysis which restricts the technology only to them.

The approach to this problem looks similar to the invisible Google reCAPTCHA system with no challenges for users and a decoy field that detect only bots to pass it to the honeyCAPTCHA.

Some IDPs that employ negative selection algorithm include the work of [15], which focuses on the improvements in detection accuracy and algorithm efficiency through covering a non-self-space with fewer detectors and cover the holes by using detectors with a smaller radius.

[16] Proposed a self-adaptive NSA that uses a novel technique to adjust adaptively the self-radius and evolve non self-covering detectors, to build an appropriate profile of the system only by using a subset of self-samples aimed at reducing the number of self-elements and resolve the problem of adaptability in classical NSA. The results on Iris showed that the system is an efficient solution to anomaly detection with high detection rate, low false alarm rate, self-learning and adaptation.

[17] Proposed a new NSA, named boundary-fixed NSA with online adaptive learning under small samples (OALFB-NSA). In their work, detectors are generated into two steps: Firstly, the Boundary-fixed NSA (FB-NSA) generates a layer of detectors, which are around the self-space. These detectors are only related to the training samples and have nothing to do with the training times. Secondly, OALFB-NSA detectors can adapt themselves to real-time variety of self-space during the testing stage. Experimental comparison among proposed algorithms, V-detector and other anomaly detection algorithms on Iris datasets and biomedical dataset shows that the FB-NSA and OALFB-NSA can obtain the higher detection rate and lower false alarm rate in most cases.[18] Proposed email detection based on the modified classical NSA. The model improves the random generation of a detector in NSA with the use of both the spam and non-spam spaces. Two set of detectors are generated one for spam and the other for non-spam detectors. The experimental result in spam base dataset shows that the detection performance of the model is higher than the conventional NSA.

Response time is another trick that is use to control spam invasion into our information content. The idea behind this tricky approach is to calculate the time during which forms are filled and submitted. Although it takes little time for users to complete forms, bots are almost instantaneous. System could determine bots if the form is filled out in a predefine amount of time [2]. Real users take a few moments to read all the information and fill in the blanks; however, robots can fill it all at instant. By setting a low minimum time limit for webpages, submission sites can catch bots without any impact on genuine users. Unfortunately, some spammers will be wise to this trick and find a way around it, but it will at least catch out some unwanted visitors [19]. By estimating the average time spent on a comment, one could define certain rules. For example, if a submission takes less than five seconds, which is virtually impossible for a human but just enough time for a bot to do its job, you could ask the user to try again [20].

IDPs that employ honeypot to strengthen security and improve user efficiency of information systems include the work of [21], who designed an intrusion detection system that depends on honey pot. They built the model of normal behavior for multitier web applications considering both front-end requests and backend database queries. It provides a container-based IDS with multiple input streams to produce the alerts and can identify a large number of attacks with the minimal false positive rate. But the system limitation is that it works on the assumption of an abnormal behavior. The IDS did not indicate the mechanism it will employ for detecting whether it is malicious user or not. [22] Used two honeypot systems to setup a malware catcher on one hand and a malicious connection logger on the other hand. Using only honeypot, makes the system to be weak and only activities of intruders are logged.

[30] Proposed a system that handles multiple clients using the concept of honeypot, Intrusion detection system (IDS) monitor whole network and looks for intrusion, when detected, honeypot will be activated and divert the traffic to dummy/virtual servers & backtrack the source (IP address). The system putsIDS in front of the honeypot, which means the passiveness of an IDS still exist in the system. [23] combined the features of IDS, IPS and Honeypot. Their system analyzes and tracks the behavior of the attacker by monitoring the network and capturing the log. The propose system has the sophisticated framework for investigating intruders as well as intrusion events.The entire incoming packets are logged by the honeypot and the gateway contains added verification on username/password thereby increasing the users verification process.[24] used an adaptive approach based on genetic algorithm to select features for profiling and parameters for anomaly-based intrusion detection. Their system was evaluated using FPR, Detection Rate, with the limitation of dependent on the anomaly of an existing IDS.[25] designed a portable Java-based real time packet capturing with intrusion detection and prevention honeypot for windows based operating system. The limitation of their system is that the attack must be on the system. Rule-based IDS and the default Firewall of the operating system were used. Their system also requires a lot of computation because it implements a real time IDP, so its performance depends on the processing power of the CPU.

Based on the suggestion of [10] on combining CAPTCHA and honeypot, [26] developed a CAPTCHA-BASED IDS, which on their view CAPTCHA becomes IDS instead of an IPS. The system work in a way that an active CAPTCHA is presented in the gateway with a placeholder tag “DO NOT TYPE ANYTHING IN THIS TEXTBOX”. Human users were tasked to read, comprehend and abide by the instruction. While an intelligent bots which targets the system will solve the CAPTCHA and pass in with the zeal of bypassing the security, but unfortunately will be redirected to a dummy page where his information will be tracked and blocked instantly. Their aim also includes identifying those intelligent bots that attack our systems, study their behaviors for further research and production.

Naïve Bayes Classification techniques will be used in this work to develop a model that will be used to classify our collected dataset, due to its implementation in the existing work of [26] and other several works related to spam classification, like the work of [27] Used Entropy and Bayesian Classifiers to classify Chat bots on one of the most popular and large commercial chat networks Yahoo! Chat, The entropy classifier is to identify new chat bots and add to the Chat bot corpus based on a certain metrics (message sizes and inter message delay) while the Bayesian used the bots and human corpora to learn text pattern of bots and humans and then quickly classify bots based on the pattern**.** Also [28] used Naïve Bayes to classify email spam tested on a different data set, which they conclude that the algorithm's quality performance is based on the dataset used. Dataset with few instances of email and attributes gives good performance for Naïve bayes Classifiers. The performance of the datasets is evaluated based on their accuracy, recall, precision and F-measure, which they concluded that the Naive Bayes classifier also can get highest precision that will give highest percentage spam message manage to block, if the dataset is collected from single e-mail accounts. Hence Naïve Bayes is considered for the training of the proposed system model to predict accurate classification

Proposed System Framework

The systems' framework is a modification of the CAPTCHA-Based IDS model. The framework forms a modified version of the existing system with a focus on security and usability. Figure 1 is the architecture of the proposed system.

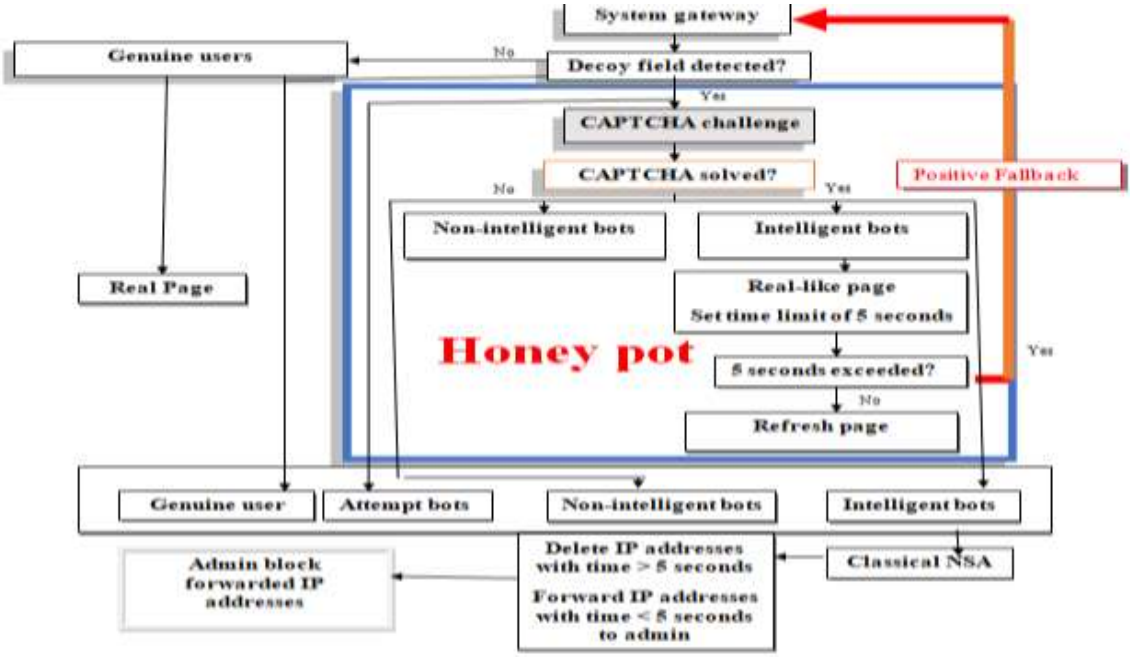

Fig. 1: The Proposed System Framework

The system was designed to ease user access to the verifiable resources in the internet at the same time increase the security robustness of the system by making it harder for bots. In that regard the proposed system comes with a unique feature of allowing a genuine user to have access to the resources by only supplying his username and password without any further verification, while on the other hand obscuring access to a detected attacker. This was achieved by removing the CAPTCHA test entirely from the users view while a hidden detector will redirect the attacker to a fruitless cognitive honeyCAPTCHA that lures the attacker away from the actual system resources. A positive fall back opportunity that does not exist in the existing system will be an added advantage to misclassified humans. This allows for an opportunity to fall back to the gateway. The Negative Selection Algorithm is also use in our system to enable proper selection of the real bots identified by their timestamp. This helps genuine user not to be block permanently from accessing the system. The system was hosted to attract visitors, from all over the world, to justify the datasets collection. Although, the existing system only considers collecting the intelligent bots capable of breaking the CAPTCHA test, the system in addition considers both the intelligent and non-intelligent bots. Robustness of our system as against the existing system was computed by considering the percentage of the bots' penetration of our system to that of the existing system.

Evaluation

The performance of this system and that of [26] were evaluated using Detection Rate and False Positive Rate metrics that were used in [26] and a single unified, intuitive and appealing metric, grounded by information theory from the work of [7]. Both robustness and efficiency of both systems were evaluated. Table 1 shows the result of a five-month IP addresses of all one hundred and ninety-two (192) visitors from December, 2018 to April, 2019 which were categorized as either humans, attempted bots, intelligent and non-intelligent. Figure 2 shows the graphical representation of the visitors according to its representation on Table 1.

Table 1 shows the entire visitors of the proposed system categorized in month

Month	**Total visitors**	Human	Attempts bots	Intelligent	Non-intelligent
Dec 2018	**34**	17	17	4	13
Jan 2019	**39**	18	21	1	20
Feb 2019	**40**	16	24	5	19
Mar 2019	**38**	9	29	3	26
April 2019	**41**	16	25	6	19
	192	**76**	**116**	**19**	**97**

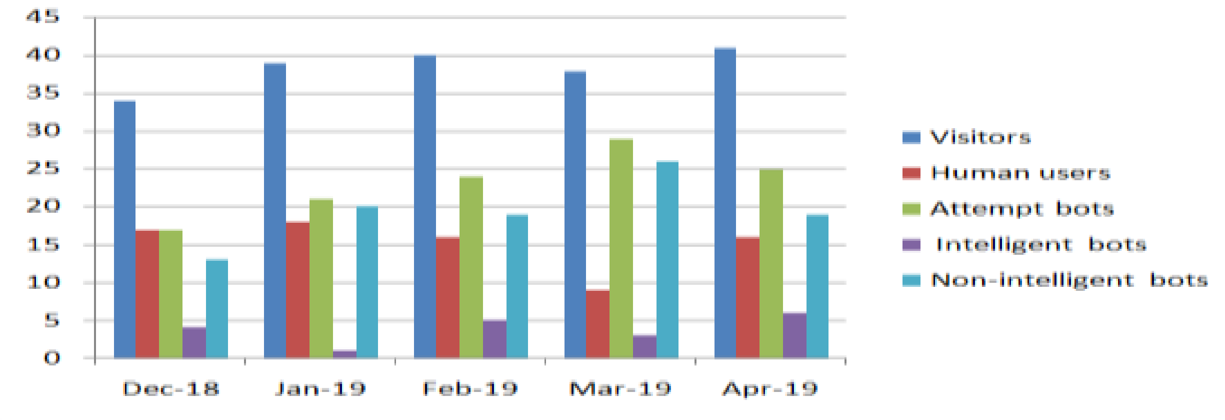

Fig. 2: Graphical representation of 192 visitors of the proposed system.

Analysis of the two systems were conducted in R using the caret and e1071 packages as discussed earlier. Generally, we considered using R due to the availability and richness of it classification and evaluation metrics [29].

The proposed system and that of [26] robustness based on the Detection Rate, False positive Rate and True Positive Rate were computed and compared in Table 2.

Table 2: Evaluating of robustness of the proposed system and that of [26]

SN	Evaluation Metrics	Existing System	Proposed System	Performance Differences
1.	Number of dataset	98	192	-
2.	Detection Rate	0.45	0.76	0.31
3.	False Positive Rate	0.36	0.10	0.26
4.	True Positive Rate	0.75	1.00	0.25

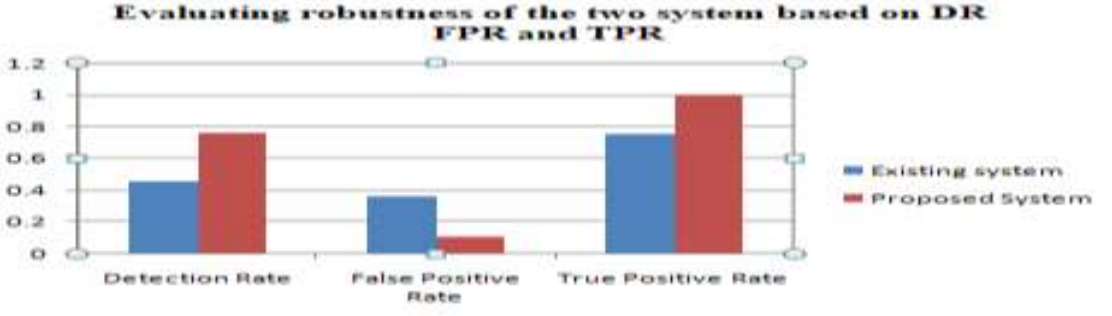

Fig. 3: Graphical representation of the system performance

Also, a standard metric that uniquely measures the capability of any IDS was used in Table 3 to compare the proposed system and that of [26].

Table 3: Comparative Evaluation of the proposed system with that of the existing system based on the standard Intrusion Detection Capability (CID)

SN	Evaluation metrics	Existing System	Proposed System	Performance Difference
1.	CID	0.42	0.95	0.53

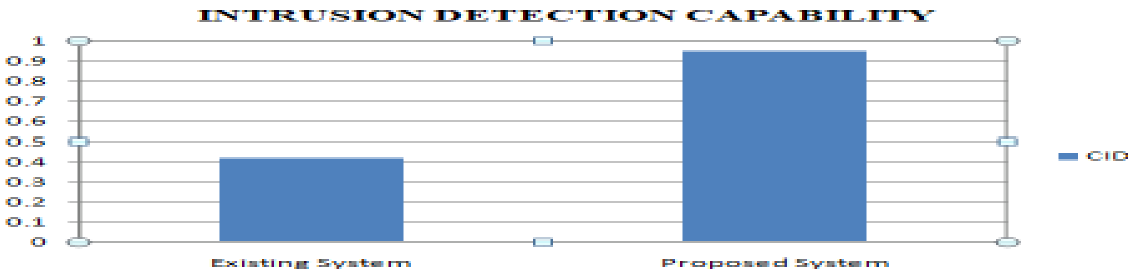

Fig. 4: Graphical representation of CID differences of the two systems.

Generally the two systems were analyzed based on Intrusion Detection Capability (CID), the proposed system performed better than [26] system 2.26 times with the CID of 0.95 or 95% and that of [29] was 0.42 or 42%.

The System usability was also measured using the Bayesian Detection rate and Bayesian Negative rate, which were stated to be the most recommended metrics in the usability point of view in [29]. Table 4 shows the Usability of the proposed system as against that of [26].

Table 4: The usability comparative analysis of the two systems

SN	Metrics	Existing System	Proposed System	Performance Difference
1	Bayesian Detection Rate (PPV)	0.76	0.97	0.21
2.	Bayesian Negative Rate (NPV)	0.63	1.00	0.37

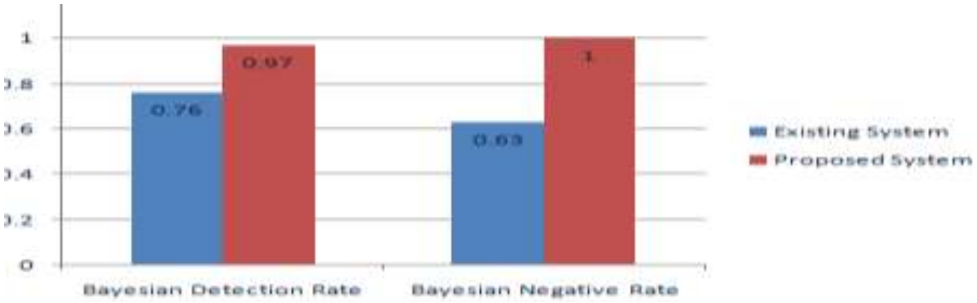

Fig. 4: Graphical representations of the BDR and BNR of the two systems

The proposed system has a Detection rate of 0.76 or 76% while that of existing system had Detection rate of 0.45 or 45%, false positive rate of 0.10 or 10% against 0.36 or 36% of the existing system and True positive rate of 1.00 or 100% against 0.75 or 75% of the existing system. This means our system is 1.7 times better than that of [26] in detecting bots and has 10% less problems than the existing system with 36% issues in misclassifying human as bots. This is due to the possible JavaScript disability, though tackled by the sample respond time detection used to create a possible fallback for normal visitors when they were classified as intruders. High scores for precision and recall showed that the classifier is returning accurate results. The Usability of the system is treating based on the Bayesian Detection rate and Bayesian Negative rate, which are considered most sufficient in measuring IDS usability. The proposed system has 0.97 or 97% BDR and that of the existing system had 0.76 or 76% and the BNR of the proposed system 1.00 or 100% against existing system with 0.63 or 63%. It also means that the efficiency of the proposed system is 1.5 times that of existing system. This will also not be unconnected with the free verification of the proposed system to users and ultimately IDS alarm is useful only if the IDS have high PPV and NPV [26]. With this record our proposed system out-performs that of [26], this is because the system eliminates any security verification in the gateway while employing the used of decoy fields inscribed by JavaScript, a recent feature in honeypot technology.

CONCLUSION AND FUTURE WORK

Sequel to the lingering tradeoff between usability and the robustness of security techniques, in IDPs state of the art, an enhanced Intrusion Detection Framework named honeyCAPTCHA as a means of tricking intruders of web-based applications was designed. The system was designed purposely as an alternative to CAPTCHA-BASED IDS that was designed by [26] to solve the perpetuated problem of web-based security. honeyCAPTCHA forms a gateway that seems easy for users to login while bots find it complicated due to the travail it undergoes in accessing the system. Detected intrusions were lured to a CAPTCHA challenge, which stands as a scapegoat for their possible attack. The decoy field obscured by JavaScript is the Detector, while the CAPTCHA challenge is the IPS that will separate the intelligent bots (i.e., intruders capable of breaking CAPTCHAs) and those that cannot. Response time and classical negative selection algorithm were used to safe the victimized humans from bot's treatment by providing an opportunity for them to retry their login. This entirely is used purposely to strengthen the security of web-based application gateway and to enable an efficient interaction with genuine users in a honeypot way, i.e. by deceiving the intruders to collect their information, which will be useful in upgrading our security techniques. The system combines IDS, IPS, response time, classical negative selection algorithm and honeypot technology to form a formidable framework for online applications. It serve as an alternative solution to those popular security gateways like CAPTCHA, IDS and other restricted honeypot skills used in protecting online applications.

The outcomes of this research have led to the following recommendations for future work:

i. Further categorization of the intruders based on their activities on the dummy page will also improved the security check and boost the activities of the honeypots techniques.
ii. The system makes emphasis on the bots detection just the honeypots side with less consideration in the aspect of real systems, probably to detect the possibility of a bots among the genuine users
iii. Using direct survey to enable users interaction with the system will also measure some of the usability part like the learnability and memorability straight away.

REFERENCES

1. Joseph, C. (2018, April, 17). Symantec Internet Security Threat Report 2018: TheTop Takeaways.[Blog post]. Retrieved from:https://thycotic.com/company//blog/2018/04/17/symantec-internet-security-threat-report-2018/. It is a snapshot of the page as it appeared on 26 Aug 2018 06:22:50 GMT.
2. Mohammad, M., &MohammadReza, K. (2014). CAPTCHA and its Alternatives: A Review. *SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks*, 8: 2135–2156.
3. Foley, A. (2012). Biometric Alternatives to CAPTCHA: Exploring Accessible Interface Options. *Dublin Institute of Technology.*
4. Mohammad A. F. & Syed S. H.(2010). Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems, *International Journal of Computer Science and Network Security* (IJCSNS), 10(7).
5. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of network and computer applications, 36*(1), 42-57.
6. Steven G., Mengjun X., Zhenyu Wu., &Haining W. (2011). Humans and Bots in Internet Chat:Measurement, Analysis, and Automated Classification. *, ieee/acm transactions on networking*, 19(5).
7. Gu, G., Fogla, P., Dagon, D., Lee, W., Skori, C. (2006) Measuring intrusion detection capability: An information-theoretic approach. In: Proc. of the 2006 *ACM Symposium on Information, computer and communications security*, pp. 90–101.
8. Powell, B. M., Kalsy, E., Goswami, G., Vatsa, M., Singh, R., & Noore, A. (2017). *Attack-resistant aiCAPTCHA using a negative selection artificial immune system.* Paper presented at the 2017 IEEE Security and Privacy Workshops (SPW).
9. Andrew, D. (2014). ESCAPT: Easy Strategies for Computers to Avoid the Public Turing Test. *Mentor: Ming Chow Fall*.
10. Parita, C., Chintan, T., & Manish, S. (2016). A Review Paper on Analysis of Decisive and Non-Intrusive Technique to Combat Form Spam, *International Journal of Innovative Research in Computer and Communication Engineering*, 4(3).
11. Powell, B. M., Kalsy, E., Goswami, G., Vatsa, M., Singh, R., & Noore, A. (2017). *Attack-resistant aiCAPTCHA using a negative selection artificial immune system.* Paper presented at the 2017 IEEE Security and Privacy Workshops (SPW).

12. Josh, D. (2019). Why CAPTCHAs have gotten so difficult.Demonstrating you're not a robot is getting harder and harder. [Blog Post]. Retrieved from https://www.theverge.com/2019/2/1/18205610/google-captcha-ai-robot-human-difficult-artificial-intelligence. Josh Dzieza@joshdzieza Feb 1, 2019, 11:00am EST.
13. Suphannee, S., Jason, P., & Resendes, D.(2019) I'm not a human: Breaking the Google reCAPTCHA. University, New York NY, USA
14. Google no Captcha + INVISIBLE reCaptcha – First Experience Results Review (2019, Mar 10). Retrieved from https://tehnoblog.org/google-no-captcha-invisible-recaptcha-first-experience-results-review/.
15. Ramdane, C., & Chikhi, S. (2017). Negative selection algorithm: recent improvements and its application in intrusion detection system. *Int. J. Comput. Acad. Res.(IJCAR), 6*(2), 20-30.
16. Jinquan, Z., Xiaojie, L., Tao, L., Caiming, L., Lingxi, P., & Feixian, S. (2009). A self-adaptive negative selection algorithm used for anomaly detection. *Progress in natural Science, 19*(2), 261-266.
17. Li, D., Liu, S., & Zhang, H. (2016). A boundary-fixed negative selection algorithm with online adaptive learning under small samples for anomaly detection. *Engineering Applications of Artificial Intelligence, 50*, 93-105.
18. Abdolahnezhad, M., R. &Banirosta,T. (2016) Improved Negative Selection Algorithm for Email Spam Detection Application, *International Journal of Advanced Research in Electronics and Communication Engineering* (IJARECE), 5(4).
19. Moth, D. (2013, July 29). Six alternatives to using the dreaded Captcha images. [Blog Post]. Retrieved from https://econsultancy.com/six-alternatives-to-using-the-dreaded-captcha-images/.
20. Bushell, D. (2011, March 4). In search of the best CAPTCHA. Retrieved August, 20, 2019, from https://www.smashingmagazine.com/2011/03/in-search-of-the-perfect-captcha/.
21. Linora, J. A., &Barathy, M. N. (2014). Intrusion detection and prevention by using light weight virtualization in web applications. *International Journal of Computer Science and Mobile Computing*;3(3), 392-396.
22. Koniaris, I., Papadimitriou, G., Nicopolitidis, P., & Obaidat, M. (2014). *Honeypots deployment for the analysis and visualization of malware activity and malicious connections.* Paper presented at the 2014 IEEE international conference on communications (ICC).
23. Yesugade, K. D., Sanika, M. A., Sanika N. S., Charmi S. S., Malav, S. (2016). Infrastructure Security Using IDS, IPS and Honeypot. *International Engineering Research Journal* (IERJ), 2(3) Page 851-855.
24. Resende PAA, Drummond AC.(2018) Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling. *Security and Privacy*; 1:4. Doi: https://doi.org/10.1002/spy2.36
25. Vivekan & Rajbhar. (2018). Intrusion detection & prevention using honeypot. *International Journal of Advanced Research in Computer Science*, 9(4),
26. Boukare, S.,& Abubakar,H. (2018). Acaptcha – based intrusion detection model. *International Journal of Software Engineering & Applications* (IJSEA), 9(1).
27. Stevens, I., D. (2016) Using machine learning to detect bots in World of Warcraft. *Transactions on networking*19 (5).
28. Rusland, N., F., Norfaradilla Wahid, N., Kasim, S. &Hafit, H. (2017). Analysis of Naive Bayes Algorithm for Email Spam. *International Research and Innovation Summit*.
29. Zhuoheng, X., Zhenghao, Y., Simon, J., Michael, R.,, Chris, R., Theerakorn, P., Matthew A.(2018), Caret Versus Scikit-learn A Comparison of Data Science Tools Lanham Purdue University Krannert School of Management, Retrieved From: http://matthewalanham.com/Students/2018_PURC_caretvsscikit.pdf
30. Malav, S., Avinash, M. S., Satish, N. S., & Sandeep, S. C. (2015). Network security using IDS, IPS & honeypot. *Int. J. Recent Res. Math. Comput. Sci. Inf. Technol, 2*(2), 27-30.