WEBSITE DEFACEMENT DETECTION AI

Mrs. K. SANGEETHA, M.E, (Ph. D)
ASSISTANT HOD(SRG) (CSE-IOT AND CYBER SECURITY INCLUDING BLOCKCHAIN TECHNOLOGY)
SNS COLLEGE OF ENGINEERING
COIMBATORE, INDIA
sangeetha.k.iot@snsce.ac.in

E. SARATHY
B.E- CSE (IOT AND CYBER SECURITY INCLUDING BCT)
SNS COLLEGE OF ENGINEERING
COIMBATORE, INDIA
sarathy.e.iot.2022@snsce.ac.in

R. SHARMILA
B.E-CSE (IOT AND CYBER SECURITY INCLUDING BCT)
SNS COLLEGE OF ENGINEERING
COIMBATORE, INDIA
sharmila.r.iot.2022@snsce.ac.in

S. SHREENTH
B.E-CSE(IOT AND CYBER SECURITY INCLUDING BCT)
SNS COLLEGE OF ENGINEERING
COIMBATORE, INDIA
shreenth.s.iot.2022@snsce.ac.in

R.GUNA
B.E-CSE(IOT AND CYBER SECURITY INCLUDING BCT)
SNS COLLEGE OF ENGINEERING
COIMBATORE, INDIA
guna.r.iot.2022@snsce.ac.in

ABSTRACT

The Defacement presents significant threats to security in that it involves an unauthorized individual making changes to web content intended to harm the reputation of a site or spreading misinformation. Thus, this project would aim to develop an AI-driven solution that would be applicable for detecting and preventing website defacement through the continuous monitoring of web pages for unauthorized changes.

We use Python as the programming language and tools such as Selenium for web scraping, Tesseract for OCR, Pillow for image manipulation, and urllib for HTTP requests. It operates by taking periodic screenshots of the website and comparing them with a set of base images of the original web pages using several image comparison techniques. In addition, it checks for unauthorized changes made to the source code.

Keywords— Website Defacement Detection, Cybersecurity Solution, Real-Time Monitoring, Image Processing, Optical Character Recognition (OCR), HTML Code Comparison, Anomaly Detection, Machine Learning, Web Scraping, Security Alerts, Visual Content Analysis, Textual Defacement Detection, Website Integrity Monitoring, Hybrid Detection System, Automated Website Protection

1. INTRODUCTION

Presently, web-sites play a crucial role in the operation of modern digital communications and organizations. Websites are vulnerable to attacks from undesired people through various types of attacks including website defacements, literally the unauthorized changes made to the content of a website toward degrading the reputation of an organization or otherwise spreading malicious information or/and messages. These could impact the reputation and service delivery of an organization, cause financial losses.

The conventional methods for the detection of website defacement rely upon the manual monitoring of or simple alerting mechanisms, which are likely to alert the change in the content of the website. But, the methods are slow and prone to inefficiencies and false alarms. The proposed project aims to suggest an AI-driven system to automate the process of website defacement detection and prevention.

The system utilizes sophisticated tools and techniques for continuous monitoring of websites. The core programming language applied in this solution was Python. Selenium was applied for automated web scraping; Tesseract for Optical Character Recognition was used to recognize the text extracted from images; and Pillow for further manipulation of the images. The urllib library was used to send HTTP requests and retrieve the website content. The system periodically takes screenshots and analyzes the source code of the website, comparing its present state with its baseline

version. Any unauthorized changes are detected at a very early stage, hence increasing the safety of the website.

This is a two-tiered approach involving visual as well as code-based analysis, thus providing a holistic solution to overcome website defacement. The system features a highly reliable and automatic means of detecting attempts at web page defacement and reacting to such attempts, thus strengthening website security and reducing the impact of successful attacks.

EXISTING SYSTEM

EXISTING SYSTEM NO 1:

Authors: Zhang L & Liu W

Title: An Effective Approach for Website Defacement Detection Using Content Hashing

This system used hashing algorithms, such as MD5 and SHA-1, to produce fingerprints of the website's content. When the content of the webpage is modified, it fails to match the reference hash stored, indicating potential defacement. Although it had merit for static websites, it had a lot of trouble with modern dynamic web pages, making false alarms in many cases due to the presence of advertisements, reloaded banners or news on the site pages.

EXISTING SYSTEM NO 2:

Authors: Nguyen T & Hwang D

Title: Visual-Based Website Defacement Detection Using Structural Similarity Index

This approach worked on the simple idea of taking screenshots of web pages and comparing them with base-line images through the use of the Structural Similarity Index (SSIM). The system performed exceptionally well for visual defacements such as changes to logos, banners, or other background images. However, rotating banners, user generated content, or advertisements tended to introduce noise in the process of comparison thereby sometimes producing false positives. It was of great utility for static sites or sites with minimal dynamic content.

EXISTING SYSTEM NO 3:

Authors: Smith R & Ahmed M

Title: Detection of Malicious Web Defacements Using OCR Techniques

This system was based on the OCR-based textual analysis. It captured text from screenshots of web pages and compared it with the baseline database to determine if changes were unauthorized. The system was very efficient in catching textual types of defacements, for example, changing slogans or inserting malicious messages. However, the system's dependence on OCR created several impediments, such as poor image quality, variation in fonts, or complex layout causing a mistake in text extraction.

EXISTING SYSTEM NO 4:

Authors: Shukla S & Singh R

Title: A Machine Learning-Based Framework for Defacement Detection

This model employed supervised machine learning algorithms to detect between defaced and legitimate web pages. The model was trained on a labeled dataset comprising of defaced and clean web pages so that it can recognize tiny alterations in visual as well as textual content. Even though highly accurate for dynamic websites, this approach demanded significant amounts of labeled datasets for training, and its performance degraded with outdated or diverse data.

PROBLEM STATEMENT

Website defacement is the biggest threat against the integrity of an online platform and its reputation. The weakness of a website attracts bad elements, thereby changing its content-carrying context to spread misinformation or to vandalize visual elements or place malicious links. Purely manual inspections and simple checksum verification fail in the modern dynamic web environments as such methods do not scale, result in high false positives, and are not flexible with changes in legitimate content.

There is a critical need for a comprehensive, automated system in order to detect and prevent defacement in real time with advanced tools like image processing, OCRs, and machine learning. Accuracy, scalability, and adaptability characterize any solution that would overcome the challenging nature of website security.

EXISTING SYSTEM

Existing website defacement detection systems have used various techniques such as checksum-based

monitoring, visual comparison, HTML code analysis, text extraction with OCR, and predictive model-based anomaly detection. Although checksum methods are rudimentary, they fail in handling dynamic content and high false positives. Even visual comparison techniques such as SSIM identify graphical changes but have limitations with dynamic content like advertisements. HTML code analysis will detect structural changes but fails to identify the changes visually. OCR-based systems try to read the text from images. However, these are suffering from the problems of having poor image quality and complex layouts. Hybrid systems put together these methods with improved accuracy but require significant computational resources and are less scalable for handling large, dynamic websites. In general, these systems lack adaptability, efficiency, and robustness to handle modern web environments that are highly dynamic, making it necessary to design more robust and holistic solutions.

The existing systems may have limitations but have still paved the way for more advanced approaches by highlighting the importance of multi-technique integration. They show that defacement can be dealt with completely with visual textual, and structural analysis combination. Modern web environments, however, necessitate solutions that are based on real-time processing, adaptive machine learning-based detection, and scalability in regard to monitoring large networks. These gaps in current methodologies underscore the need for innovative, hybrid systems capable of reducing false positives while maintaining high detection accuracy, paving the way for the proposed solution.

PROPOSED WORK

The proposed system is designed to offer an advanced, automated, and scalable real-time detection solution for website defacement. It applies a hybrid approach through image processing, text extraction, HTML code analysis, and machine learning in order to guarantee all-around monitoring and detection. Key technologies integrated into the system include Pillow for image comparison, Tesseract OCR for extracting text, Selenium for web scraping and HTML code comparison, and machine learning algorithms for anomaly detection.

The workflow starts with capturing website data in the form of screenshots, HTML source code, and URL responses. Screenshots are analyzed using image processing techniques by identifying visual changes, whilst OCR extracts textual content for identifying unauthorized modifications. The HTML source code is compared to detect structural changes. The anomalies detected across these layers are then analyzed using machine learning models to differentiate legitimate updates from malicious defacements. This system then alerts administrators to defacements in real-time, so they can act to mitigate the effect as much as possible.

This approach supersedes the current trends of systems as it combines multi-layered detection techniques, ensuring adaptability to dynamic web environments and lowering the false positives. It's also scalable to monitor multiple websites in parallel and resource-efficient for actual practical use within any type of organizational setting.

IMPLEMENTATION

The proposed website defacement detection system provides a proper implementation while integrating multiple technologies for a complete monitoring process with accurate detection. To begin with, the system collects data from the targeted website using web scraping tools like Selenium and URL requests using Urllib. Additionally, to visually analyze images, automated screenshots are taken. Captured images are now processed using Pillow to detect visual changes, and text extracted from images in Tesseract OCR is then compared against predefined baselines. The source HTML code is compared to the stored reference versions to search for structural anomalies such as injected scripts or unauthorized modifications. Together, these methods build a strong, multi-layered detection framework.

Machine learning models are incorporated, which measure visual, textual, and structural anomalies, thus enabling the system to adjust classification of legitimate updates vs. defacements. Historically accumulated data is used to improve detection accuracy through training. Upon detection of anomalies, real-time alerts with detailed reports are sent to administrators for immediate action. The entire implementation is designed for scalability, with regard to monitoring many websites while maintaining resource efficiency. The main technologies used include Python, Scikit-learn, and MySQL, which give it flexibility to be deployed on local or cloud platforms. This complete implementation brings in the missing links of traditional systems and produces high accuracy and usability for defacement detection.

RESULT

The proposed defacement detection website system was tested using various static and dynamic websites in order to evaluate its effectiveness and accuracy. It was able to successfully detect visual, textual, and other changes regarding logos, banners, as well as embedded text modification while keeping the rate of false positives low. Changes about visual changes were done by comparing baseline screenshots with current ones, while Tesseract OCR successfully and accurately identified unauthorized textual modifications even in very complex layouts. HTML code analysis efficiently raised alarms for structural changes, including the injection of malicious scripts or changing metadata.

Incorporation of the machine learning models made the detection result exponentially better in time as it learned new patterns of legitimate changes. Thus, the system could distinguish harmless updates such as refreshing content or tweaking a design versus attempts to deface, providing low false alarm rates. Real-time alerts were issued in timely succession, detailing reports that clearly pointed out the exact nature of change, thus enabling administrators to respond promptly through corrections. The system also exhibited scalability by handling multiple websites successfully, which confirmed its suitability in large-scale deployment. Thus, the system was proved to be highly accurate, adaptive, and efficient in offering a comprehensive solution for real-time website defacement detection.

CONCLUSION

Defacement of websites is a critical cybersecurity challenge due to the threat it poses to an organization's integrity and reputation worldwide. Common detection methods that work in specific scenarios fail when it comes to dealing with the complexity of the modern web environment. Bringing AI tools into the game brings a great level of advancement in the detection and prevention of defacement attacks.

This project integrates image-based analysis and source code verification to ensure an accurate, automated process. Utilizing tools such as Selenium for web scraping, Tesseract for text recognition, Pillow for image processing, and urllib for HTTP requests will assure that all elements of the website are monitored. The dual-layered approach—visual and code-based—ensures a reliable mechanism for detecting unauthorized changes with a low probability of false positives and false negatives.

It is improved in detection capabilities along with instant responses to any attempt at defacement, thereby reducing downtime and further minimizing potential damage. This system presents itself as being very critical in protecting web assets against changing cyber threats and molds a safer digital ecosystem.

REFERENCES

[1] Al-Mohannadi, H., Marrington, A., & Emam, A. (2016). Website Defacement Detection and Prevention: A Review. International Journal of Cyber-Security and Digital Forensics, 5(2), 55-63.

[2] Sharma, K., & Kaur, G. (2021). AI-Driven Cybersecurity Solutions for Web Applications. Journal of Cybersecurity and Privacy, 1(2), 150-169.

[3] Mitra, S., & Bhattacharya, P. (2019). Secure Web Scraping for Real-Time Defacement Monitoring. Proceedings of the International Conference on Web Intelligence, 349-356.

[4] Li, H., & Zhang, Y. (2020). Adaptive Content Integrity Verification Using Machine Learning. IEEE Access, 8, 35645-35655.

[5] Amini, S., & Jalali, M. (2017). Using Support Vector Machines for Web Defacement Detection. Journal of Information Security and Applications, 34, 98-105.

[6] Kamal, N., & Abdullah, M. (2019). Using Deep Convolutional Networks for Automated Defacement Detection. Journal of Artificial Intelligence Research, 65, 1-19.

[7] Baeza-Yates, R., & Ribeiro-Neto, B. (2016). Modern Information Retrieval: The Concepts and Technology Behind Search. Addison-Wesley.

[8] Venkatesh, R., & Singh, P. (2017). An Enhanced Framework for Website Defacement Detection Using Hybrid Methods. International Journal of Advanced Research in Computer Science, 8(7), 201-208.

[9] Jiang, Y., & Chen, S. (2016). Real-Time Monitoring of Website Integrity Using Image and Text Comparison Techniques. Journal of Information Assurance and Security, 11(4), 189-195.

[10] Rahman, A., & Habib, M. (2018). Web Anomaly Detection Using Historical Analysis and Predictive Modeling. Proceedings of the IEEE International Conference on Cybersecurity, 320-328.