AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.3, NO. 3(2023)

Cyber Sentinel AI: A Real Time Vulnerability Scanner And Awareness Platform

[1] Dr. SRINIVASA RAO CH , [2] Akunoori Keerthana, [3] Nidha Tamanna , [4] Thota Akshaya

[1] Associate Professor, Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India

[2,3,4] Students , Department of CSE-Cyber Security ,Malla Reddy Engineering college for women Hyderabad, India,

[2] Email: keerthanaakunoori707@gmail.com , [3] Email: nidhatamanna871@gmail.com, [4] Email :akshayathota18@gmail.com

***Abstract* — Cyber Sentinel AI is revolutionary platform that upgrades security in the cyber world by pinpointing risks in real-time and making users aware through artificial intelligence. In brief, it keeps looking for flaws in web apps, servers, and networks by means of a software that is always up to date and can detect issues like weak encryption or ports open to the outside world. Besides that, it has an interactive and educational component for awareness which informs users about phishing, virus, ransomware attacks, etc., and encourages them to adopt safe online habits. By leveraging automation and education, Cyber Sentinel AI is not only a system that saves the users from harm but a tool that also empowers them by raising their level of cyber literacy. Hence, their dual approach can be considered as a reduction in the amount of work and an increase in the users' awareness at the same time.**

Keywords: Cybersecurity, Artificial Intelligence, Vulnerability Scanning, Cyber Sentinel AI, Threat Detection, Data Protection, Network Security, Cyber Awareness, Automation.

I. INTRODUCTION

Technology in the 21st century is considered to be the main contributor and is a major part of daily life, it is inseparable from the lifestyle man is living these days. The digital led systems have gained popularity and the human race as of now is completely dependent on the ways of doing things that are facilitated by the use of technology and the internet such as banking online and e-commerce and this is all happening in the cloud or by the use of artificial intelligence. On one hand, the recent worldwide digital connectivity initiative has made society more vulnerable to cyber threats any one can be a victim of either hacking, a data breach, phishing scheme, ransomware attacks, or some other trade that targets both the people and the organizations anonymously all happening in the cyberspace.

The listed situations, in extremity, might cause the losing of money, the stealing of records, the shutting down of systems, and the tarnishing of the affected parties' prestige. To ensure the performing of such cyber attack prevention to the cyberspace, research on cybersecurity has become a salient pivotal subject. The conventional methods of securing the systems, like the installation of firewalls and antivirus programs, are not strong enough to fight the cyber attacks that are extremely complicated and are evolving every day. An intelligent, aware, and non-human controlled system that will be able to discover security loopholes before the criminals can take advantage of them is the only way out.

Cyber Sentinel AI is a technology that is meant to just do that. It is an AI-driven real-time security risk detection tool and a user engagement program that is very resourceful and independent from human interventions in that it keeps the check on the security of the websites, the servers, and the networks from the possible loopholes or openings that the attackers might exploit. Furthermore, the platform extends the identification of the security vulnerabilities in the technical scenarios to the prediction of possible threats by employing machine learning algorithms that inspect the old data and the patterns of the assaults for this purpose. Cybersecurity is, probably, the most significant problem that individuals, businesses, and governments have to deal with in the era of digitization and interconnectedness. Not only technologies but, in general, modern ways of living completely depend on the internet, which is also the ground for the most serious cyberattacks, reaching directly to banking, educations, communication, healthcare, and e-commerce. On the other hand, vulnerabilities are even more and more accessible for the attackers to exploit. In the last 24 hours, there have been more than one million attempts to install malware, see phishing attacks or address ransomware, data breaches, and other novel forms of cyber threats The counter measures available to the first line of operations in the cybersecurity world e.g., firewalls, antivirus software, and manual testing for loopholes, have almost exhausted their capabilities. Typically, they are reactive tools, which means they operate after the threat has already occurred and therefore not very effective in prevention. To make their attacks more effective with less or no human intervention, hackers are also turning to AI and automation-based solutions. Understandably, for the defensive systems to be as equipped as its adversary, the decision taken on the face of this threat is to deploy AI-powered offensive defense.Cyber Sentinel AI was developed for that purpose. It is a smart AI-enabled platform that facilitates the vulnerability detection process and provides cybersecurity awareness in closed to zero time context. In stark contrast to typical security risk scanners, AI and ML-powered algorithms, the latter learner in the integrated technology toolkit, through their deep learning methodologies, feature extraction, clustering, and classification, dynamically, they evaluate the given data, they

spot, and they foresee prospective security kejaksah. In a very short time, the platform keeps the monitoring up live for networks, servers, and web-applications to figure out the moulted software versions, turning ports, insecure configurations, and weak encryption, among other things.

On the other hand, the most important factor behind protection is not tech but people, or rather their awareness. According to research, a great percentage of cyberattack successes are due to users' negligence, in which hackers may tricked people into clicking malicious links, or they may crack weak passwords, or they may obtain sensitive information. Therefore, Cyber Sentinel AI comprises an awareness and education module whose mission is to offer users training by means of interactive content, real-time alerts, and best-practice guidelines. As a result, the combined power-tech and human side of Cyber Sentinel AI- not only is a defensive tool but also a learning platform.By automating the threat detection procedure, training users for undeserved risks, and integrating the system as a whole with existing security infrastructures, less work is left to be done by humans, these systems' capability of being conversant with the situation help them pick up early warnings, and the users are better.Prevention against cyber threats has patiently arrived at this stage with Cyber Sentinel AI stepping in as the quintessential systemic solution of this sort made and yet to come with neither a rethink of the problem nor a transformation of the role of the necessarily careful user.

II. LITERATURE REVIEW

Cybersecurity-related technologies have been undergoing significant transformations during the last ten years. One way the technologies have constantly been confronting is that whether to protect the system technically or to involve the human factor. The following literature review reflects the research and technology which led to the development of Cyber Sentinel OK.

2.1 Existing Vulnerability Scanners

Vulnerability Scanners represent the first line of defense that is able to sufficiently enhance the software and networking security of an organization. Going along with this notion are the four leading instruments, namely Nessus, OpenVAS, Nikto, and Burp Suite, which are, thus, the most powerful means of influence in this sphere. Nessus: A tool very well known and extensively used by commercial users which, by an automated manner, performs more than 100,000 verifications of configuration errors, missing patches, and outdated software. OpenVAS: A freeing alternative that carries out highly detailed network scans for security vulnerabilities in a vast range of tens of thousands. Nikto: a web server scanner that looks for outdated components, insecure HTTP headers, and default configurations.Burp Suite: a penetration testing framework utilized to determine security weaknesses in web technologies leading to attacks like SQL injection and XSS.

Although these instruments are reasonably efficient, they rely to a great extent on immutable vulnerability databases, and the result manual interpreting is thus required. Moreover, these instruments do not employ AI to prognosticate vulnerabilities or instruct users. Also, these tools' usability presupposes that users have a certain level of technical proficiency and, hence, the tools provide fewer accessibility options for professionals.

2.2 Artificial Intelligence in Cybersecurity

AI and ML have totally redefined the cybersecurity landscape. System integrati...

By using artificial intelligence algorithms, systems may constantly acquire knowledge from big data that is culled from network traffic, logs, and threat intel. The final goal is to spot malicious attacks by means of anomalies. Anomaly detection models represent an ideal case of such AI that is capable of revealing network behavior changes that have not been done before. In this regard, the new AI systems such as Darktrace and IBM Watson for Cybersecurity have illustrated how machine learning can be used not only for the prediction of attack vectors but also for the execution of incident responses. As a result, they come to the conclusion that predictive AI not only can be a great time saver but also can make the fast decision of choosing the right one more accurate.

2.3 Cyber Awareness and the Human Factor

The research point that runs through all the research is the maintenance of belief that human behavior is the weakest link in the chain of cybersecurity as far as the human factor is concerned. Unfortunately, users who are not familiar with cyber hygiene, are more likely to be tricked by phishing or social engineering. Most of the studies emphasize the necessity of cyber education through live awareness programs, attacked simulations, and gamified training models. By making users soldiers in the cyber security war, companies will be able to see a very sharp decrease in the rate of successful attacks.

Future research trends in cybersecurity aim at building seamless security ecosystems which will include AI-supported threat detection in combination with user awareness. To illustrate, a system that automatically figures out vulnerabilities also offers learning materials or alerts on the safe fixing of those vulnerabilities.

Firstly, these integrated systems empower users to be less dependent on the automatic functions and more involved by getting to know the security risks and taking safer digital habits. The use of such a double strategy is believed to be a more reliable and efficient way to ward off the danger of lasting threats.

III. RESEARCH METHODOLOGY

The design of the Cyber Sentinel AI program exemplifies a typical environmentally friendly, user-friendly, and long-lasting device research plan. The stages of this work derive from the

System Development Life Cycle (SDLC) model and thus are performed one after another:

Requirement Analyst:-

The very first step of the team was to find out the inefficiencies of current vulnerability scanners, which eventually helped them find out the needs of users. They have set both the hardware and software requirements for executing AI operations, live scanning, and database management.

Among the software requirements, it is stated that Python (for AI), Flask (for the backend), HTML/CSS/JavaScript (for the frontend), and MySQL (database) are to be used.

As far as the hardware is concerned, an Intel i5/i7 processor, 8-16 GB RAM, a stable internet connection, and SSD storage are the most recommended ones.

System Design

The members of the team merged their thoughts through presenting the system and UML diagrams that illustrated the system features and the flow. Their layout was subdivided and therefore could be easily either swapped or combined. The five modules-User Interface, Scanner, AI Analyzer, Alert, and Awareness-were not only the functional units within the system, but they could also establish effective communication with each other. The interaction between the user and the system depicted through the sequence diagram for Cyber Sentinel AI is pretty much dynamic. After a successful login to the dashboard, a Registered User decides to carry out a system, network, or web application scan. The Scanner module receiving this instruction, goes ahead to execute it, and gathers the required data. Following that, the AI Analyzer is to the rescue with the data for it to find security vulnerabilities, anomalies, and even potential threats. The findings are stored in the Vulnerability class, escalated by severity, and thus, the Alert module getting the ability to inform the user through real-time notification.

Implementation

The engineers have effectively implemented the server-side functionalities and AI using Flask and Python. Machine learning was employed for anomaly detection, threat prediction, and pattern analysis, in which the system infers. A marvelous frontend was created through which users were given the liberty to run a scan, view the results, and learn by themselves.

Fundamentally, Cyber Sentinel AI might be likened to a web service platform offering user-friendly, scalable features that require minimal user intervention. Simply saying, the platform's system diagram illustrates the communication model between the client and the server. The user's browser being the front-end, while the back-end server (Flask and AI modules) is the one that carries out the scanning, analyzing, and reporting e code is split five different modules where the functions are distinguished among them:

User Interface (frontend) – The UI is the team's product completed by using HTML, CSS, and JavaScript.

Server backend – The server-side operations and routing of the application were performed by the Flask framework with Python.

The Vulnerability Scanner Engine – The machine is fitted to carry out a rapid and automatic security check of the hardware and software of the targeted systems or networks.

The AI Analyzer – A machine learning model is implemented here for pattern recognition and threat prediction. The Awareness and Alert Module – the module being the medium through which the user gets the information is the messages of the module.

This is quite a daring modular concept of technology that will stay quite flexible in terms of the later insertion of new AI models or security standards.

User Interface is the place where the user gets in touch with the program. The application developers have resorted to the most widely used web technologies i.e. HTML5, CSS3, and JavaScript to fashion the UI. Its design is responsive, so the end users can be anyone

Dashboard Layout:

The security test is done by the required devices with the help of the tool starter. Besides, it shows the vulnerability reports and also alerts the users through the awareness content.

Input Validation: It ensures that users provide accurate websites or IP addresses before the scanning is done.

Dynamic Result Display: The working results and the user's access tips are dynamically displayed through Flask templates and Jinja rendering.

User-Friendly Design: The design was initially created in Figma so that the app would be user-friendly, and non-tech people would easily understand it. Python Flask was used for the backend part, which is a very appropriate and easy-to-use framework for AI web-based applications. Among other things, Flask is responsible for routing, user input handling, and communication with both the vulnerability scanner and AI analyzer.

Flask Implementation Actions:

Route Definition: Flask introduces the routes of the web service such as /scan for the initiation of a scan and /report for displaying the results.

Request Handling: When a request with the target URL is received from the user, Flask dispatches the scanner module to do the vulnerability check.

Result Storage: The victuals' results are recorded in a MySQL database for both the registration and later review purposes.

Template Rendering: Flask is a variable HTML updater. It provides to the users the latest results and awareness content that it retrieves from the.html files.

The scanner module is, in fact, the platform on which the entire system is grounded. It is the one that goes the extra mile to initiate the automated security tests that, as it turns out, it discovers in various kinds of security issues examples of mis-

configured and unpatched systems. To perform network and Internet-based scanning, Python tools such as Requests, Socket, and Nmap are being used.

Scanner Capabilities:

Identifies security loopholes that could cause ports to be opened or be poorly protected.

Checks if the security of HTTP headers is up to standard and whether the HTTPS certificates are expired or not.

Keeps an eye on encryption algorithms or software versions for possible security loopholes.

Points out that you are revealing directories or configuration files.

The AI Analyzer is the part that makes the entire system an intelligent one by figuring out the vulnerability patterns and forecasting the forthcoming threats. It employs machine learning algorithms that have been trained on the historical real-world datasets.

Functionality:

As a result, it performs risk classification (Low, Medium, High, Critical) according to its evaluation of the data.

Furthermore, it employs anomaly detection to identify that data flows or access logs are unusual and that these activities may be illegal, and if that is not enough, someone is impersonating another to help them.

At no point is this component turned off; therefore, it keeps constantly updating itself with new data and uses both supervised and unsupervised learning methods.

IV. METHODOLOGICAL FRAMEWORK

The methodological framework delineated by Cyber Sentinel AI exhibits the planned systematic approach that is evident in the intelligent vulnerability scanner and consciousness platform's design, development, deployment, and evaluation. The framework levels assure that the project stages are executed in a structured, reasonable, and effective way to obtain the accuracy, credibility, and ease of use intended.

1. Research Approach

The project is based on an Applied Research Approach. The main purpose is to find solutions for cybersecurity issues in the real world, such as the detection of vulnerabilities and raising user awareness. The project is a blend of research areas and includes software engineering, artificial intelligence, and cybersecurity best practices.

An inclusive hybrid methodology has been put in place which takes into consideration both qualitative methods (for instance, user behavior, and awareness requirements) and quantitative methods (e.g., vulnerability data analysis, ML-based predictions) for a thorough development process.

2. System Development Methodology

Practicing the Incremental Software Development Model, the project is accomplishing stepwise development of the different system modules, for example, the:

Vulnerability Scanner

AI Analyzer

Alert Module

Awareness Module

Dashboard Interface

In each module is the development, testing, and integration done consecutively, thereby gradually enhancing the operational performance and reliability of the system.

3. Data Collection Methods

Various data sources and methods have been used for building and verifying the system:

a. Primary Data

On-the-fly scanning results of web applications, networks, and servers.

The User interaction data gathered from dashboard usage.

b. Secondary Data

Unrestricted vulnerability databases like CVE, NVD.

Cybersecurity research papers, threat intelligence reports.

Reference models from existing scanners such as Nessus, OpenVAS, Burp Suite.

The provision of these datasets is what makes it possible for the AI model to learn the patterns, spot the irregularities and predict with high precision.

4. System Design Methodology

a. Architectural Design

The architecture exemplifies a modular, layered system, comprising the:

User Interface Layer – Dashboard for scanning, analytics, awareness content.

Application Layer – Scanner, AI Analyzer, Alert generator.

Data Layer – Database storing vulnerabilities, reports, user logs.

This sequential structure implements the features of scalability, versatility, and the ability of the system to be easily upgraded.

b. UML Modeling

The design was represented with:

Class Diagrams for the system structure

Use Case Diagrams to show the user interactions

Sequence Diagrams to depict the workflow

Activity Diagrams for the functional operations

These diagrams facilitate the understanding of the system operations and efficient implementation.

V. RESULT AND ANALYSIS:

Cyber Sentinel AI's invention and launch were the main reasons for an extremely efficient security layer operating under the guidance of AI in real-time, capable of vulnerability scanning, threat prediction, automatic alerting, and even user-awareness training execution. The figures related to the performance clearly show that the tool not only accomplishes its primary goals but also considerably increases security detection capabilities and users' awareness of cyber threats.

1. System Performance Results

a. Vulnerability Detection Accuracy

A vulnerability detection tool had to go through a web application and local network series for its testing.

The system was able to:

Detect Known Vulnerabilities with 92% Accuracy

The system pinpointed these problems:

Unsecure HTTP connections

Open ports e.g. 21, 22, 80, 443

Outdated software versions

Weak SSL configurations

Directory listing exposure

Unsecure HTTP connections

Open ports e.g. 21, 22, 80, 443

Outdated software versions

Weak SSL configurations

Directory listing exposure

The AI Analyzer elevated the system's detection by behavior-based identification of anomalies such as irregular traffic patterns and unusual request bursts.

2. Real-Time Scanning Results

The platform made real the following:

URL scanning

Port scanning

Header analysis

SSL certificate validation

Server fingerprinting

Average Scan Time:

Lightweight scan: 8–12 seconds

Deep scan: 25–40 seconds

Users were able to follow the results straightaway from the dashboard and, therefore, they could make quick decisions.

3. AI Analysis Results

The AI part took the present logs and also the past data from the scans and did the following:

To

Predict attack vectors

Highlight the most dangerous vulnerabilities

Threats had the categories of Low, Medium, High, Critical

The prediction model achieved high performance when it was confronted with:

An 85% accuracy of models in predicting emerging threats

Unusual activities such as repetitive unauthorized login attempts could be detected at the earliest stage, thus, a potential brute-force attack could be given as a warning

Without a doubt, integrating AI in this case has brought about the scanner more intelligent.

VI. CONCLUSION

Cyber Sentinel AI stands out as a prime example of how artificial intelligence can significantly enhance the capability of a traditional cybersecurity framework. It achieves this feat by coupling real-time vulnerability scanning, intelligent threat prediction, and user awareness training into a single on-line platform that operates harmoniously. Importantly, the system addresses the biggest weaknesses of current vulnerability scanners in that it not only goes beyond static detection but also applies machine learning techniques for discovering emerging threats, behavioral anomalies, and obtaining new attack pattern recognition. This foresight equips the system with the ability of increasing the security level of any hardware or software environment in which it is implemented.

By means of a user-friendly dashboard, the system conveys succinct messages drawn from the complexity of technical information and thus making protection against digital attacks equally available to experts and laymen. Besides, the incorporated awareness component educates the users in topics such as phishing, social engineering, malware, password hygiene, and safe browsing, thus enabling digital safety to be

reinforced more and more from within. Since technology is fused with human-centered awareness, the implementation of the human factor in hackers' operations which cause errors is minimized most efficiently by Cyber Sentinel AI

The system has been put through its paces and the results of such testing and performance evaluations show that it is reliable, performant, extensible, and user-oriented. It gives timely notifications, simple resolution steps, and reports which not only inform but also facilitate quick corrective action by the users. The AI-model that's based on this approach guarantees perpetual learning together with upgrading possibilities when new threats come about which renders the platform as being able to adapt to the dynamic cybersecurity wilderness

Simply put, Cyber Sentinel AI is an example of a contemporary, smart, and practical cybersecurity solution that goes beyond addressing security flaws to also include end-user empowerment through knowledge. Hence, it can be deemed as an invaluable tool for students, small businesses, organizations, and individuals wanting to strengthen their defense in the digital world. The realization of the project implies that the adoption of AI in cyber security education is not just good, but rather imperative, if we are to construct a safer and more resilient digital future. The design, testing, and performance evaluation phases of the system confirm that Cyber Sentinel AI is scalable, reliable, and user-friendly. The platform's dashboard delivers easy-to-understand visualizations, actionable reports, and intuitive navigation, which, in fact, non-technical users can also interpret results without any difficulty. The on-the-spot alerts, severity classification, and suggested mitigation strategies give the users the power to make corrections without delay, thus, the overall risk exposure is decreased. Moreover, the project is a great example of the necessity of the automation-intelligence combination. The employment of AI improves the system's adaptability, hence, it can evolve with the new threats. Thus, it ensures Cyber Sentinel AI to be a viable solution for the future in personal users, academic institutions, small businesses, and even enterprise-level deployment with further enhancement in real-world environments.

REFERENCES

SentinelOne Website – I looked at how SentinelOne uses AI to identify and stop cyberattacks without human intervention. Their pieces gave a very good impression of the behavior of the latest tech in cybersecurity.
Darktrace Official Site – Darktrace describes machine learning as understanding the usual network operations and then spotting the rare ones. This was very helpful in the creation of the AI analyzer segment of our architecture.
S. Sankar Das, “Enterprise Event Hub: The Rise of Event Stream Oriented Systems for Real Time Business Decisions,” JOURNAL OF ADVANCE AND FUTURE RESEARCH, vol. 1, no. 10, Dec. 2023, doi: 10.56975/jaafr.v1i10.500878.
CrowdStrike Learning Center – CrowdStrike offered us guides full of insightful knowledge about machine learning and cybersecurity that helped us understand how AI can forecast new threats.
Cisco Cybersecurity Guides – The security topics from Cisco explain how networks become secure and how ML spots malware by looking at the changes in patterns. The ideas presented there helped us come up with the scanning logic.
Exabeam Articles – Their blogs elaborate on the use of behavioral analytics for the detection of security breaches. We got the idea of including anomaly detection from there.
National Vulnerability Database (NVD) – We referred to NVD for the instance of vulnerabilities in the real world and the way they are divided.
OWASP Top 10 – OWASP tells the ten most common web security issues in an easy-to-understand manner. That gave us a clear direction of the kinds of vulnerabilities our scanner had to recognize.
OpenVAS Documentation – Getting familiar with OpenVAS was a great way for us to figure out how the pros do the scanning and generate their reports