JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURE BANK 360: AI-based Vulnerability Risk Assessment Tool

Priyanka Omkar Bhoir
Department of Artificial Intelligence and Machine Learning
Faculty of Universal College of Engineering
Palghar, India

Jathin Ravi Reddy
Department of Artificial Intelligence and Machine Learning
Universal College of Engineering
Palghar, India

Jayant Ganesh Sail
Department of Artificial Intelligence and Machine Learning
Universal College of Engineering
Palghar, India

Ojas Subodh Satardekar
Department of Artificial Intelligence and Machine Learning
Universal College of Engineering
Palghar, India

Manish Dilip Yadav
Department of Artificial Intelligence and Machine Learning
Universal College of Engineering
Palghar, India

***Abstract*—** As cyber dangers gotten to be progressively complex, conventional security apparatuses regularly battle to supply adequate security against advanced assaults. To address this challenge, this paper presents SecureBank360, a cutting-edge cybersecurity arrangement that combines AI-driven irregularity location with ordinary security procedures such as Nmap, ClamAV, and YARA. The proposed framework utilizes machine learning to distinguish peculiarities and coordinating characteristic dialect handling (NLP) for comprehensive danger insights investigation. Planned for wide compatibility, SecureBank360 guarantees proficient operation indeed on bequest frameworks, making it a flexible and versatile security instrument. This paper gives an in-depth investigation of the framework design, execution handle, assessment strategies, and its broader suggestions for the advancing cybersecurity scene.

Keywords—Cybersecurity, AI, Vulnerability Scanner, Machine Learning, Threat Intelligence, Anomaly Detection, Nmap, ClamAV, YARA, NLP.

I. INTRODUCTION

In today's quickly progressing computerized period, cybersecurity dangers are advancing at an uncommon pace, posturing critical challenges for organizations around the world. Cybercriminals ceaselessly create advanced assault strategies, focusing on vulnerabilities in both present day and bequest frameworks. As a result, conventional security measures, essentially depending on signature-based location and inactive rule-based frameworks, frequently demonstrate insufficient in distinguishing and relieving rising dangers. To combat these advancing dangers, there is a critical requirement for brilliant security arrangements that can identify, analyse, and neutralize potential cyberattacks in real-time. SecureBank360 is planned to bridge this security service by coordinating customary security devices with progressed machine learning procedures Not at all like conventional scanners that depend on predefined danger marks, SecureBank360 leverages profound learning for

irregularity discovery and common dialect preparing (NLP) for computerized risk insights examination. This special combination improves cybersecurity capabilities by recognizing zero-day vulnerabilities, minimizing untrue positives, and streamlining risk reaction instruments.

SecureBank360 is built to supply a vigorous, multi-layered defence against cutting edge cyber dangers. It joins:

A. Profound Learning for Irregularity Discovery:

Utilizing progressed neural systems, SecureBank360 recognizes deviations from ordinary behaviour, making a difference to distinguish already inconspicuous cyber dangers some time recently they can cause critical hurt.

B. Common Dialect Handling (NLP) for Risk Insights:

The framework ceaselessly analyses endless sums of unstructured security information, counting logs, risk reports, and security advisories, empowering organizations to remain ahead of developing dangers.

C. Integration with Industry-Leading Security Devices:

SecureBank360 consistently joins broadly utilized cybersecurity arrangements, such as Nmap which is arrange scanner that recognizes vulnerabilities and misconfigurations. ClamAV which serves as a vigorous malware location motor for checking and analyzing records. Finally, YARA which is an apparatus planned for pattern-based malware classification and discovery.

D. Lightweight and Adaptable Plan:

SecureBank360 is optimized to function proficiently on both cutting-edge IT frameworks and bequest frameworks, guaranteeing wide appropriateness over assorted organizational setups. Customary helplessness scanners, counting Nessus, OpenVAS, and Qualys, fundamentally depend on database-driven danger location components. Whereas successful against known dangers, these frameworks regularly battle with Zero-Day Vulnerabilities which defines modern misuses that have not however been recorded or doled out marks. Tall Wrong Positive Rates means the dependence on inactive rules frequently comes about in inaccurate risk classifications, driving to superfluous security alarms and expanded workload for cybersecurity groups. Constrained Versatility to Rising Dangers means the Conventional scanners are incapable to prepare and analyze real-time cybersecurity insights effectively, making them incapable against quickly advancing assault vectors. SecureBank360 overcomes these confinements by utilizing an AI-powered approach that persistently learns and adjusts to modern danger scenes. Its profound learning-based peculiarity location component distinguishes abnormal designs and behaviors instead of exclusively depending on known assault marks, making it a capable instrument against advancing cyber dangers. One of the key qualities of SecureBank360 is its capacity to coordinated consistently with existing IT foundations. Numerous organizations confront challenges when embracing unused security arrangements due to compatibility issues with bequest frameworks. SecureBank360 has been fastidiously outlined to operate nearby both cutting edge and obsolete IT situations, guaranteeing negligible disturbance amid arrangement.

Moreover, the system's lightweight design guarantees ideal execution without devouring over the top computational assets, making it reasonable for a wide extend of businesses, counting money related teach, healthcare organizations, government organizations, and endeavors dealing with touchy information. SecureBank360 reclassifies the scene of cybersecurity by combining AI insights with conventional security strategies, advertising a next-generation security instrument custom fitted to advanced challenges. By consolidating profound learning, NLP, and driving security instruments into a bound together system, SecureBank360 conveys a comprehensive and proactive approach to helplessness evaluation and danger relief. With its real-time peculiarity discovery capabilities, consistent integration, and capacity to adjust to advancing cyber dangers, SecureBank360 stands as a strong arrangement for fortifying cybersecurity resistances in a progressively complex advanced biological system.

II. LITERATURE REVIEW

Truly, signature-based malware location has been the foremost broadly utilized strategy for distinguishing cyber dangers. Apparatuses like ClamAV, Windows Protector, and McAfee depend on predefined malware databases to distinguish dangers. Whereas these arrangements have been viable in avoiding known assaults, they battle with zero-day misuses and polymorphic malware, which can adjust their structure to sidestep discovery. Also, conventional arrange security scanners, such as Nmap and Wireshark, play a significant part in distinguishing open ports, misconfigurations, and unauthorized get to in organize foundations. In any case, these instruments fundamentally center on known vulnerabilities and need AI-driven prescient investigation, making them incapable in identifying progressed determined dangers (APTs) that abuse obscure vulnerabilities.

One of the foremost promising AI strategies in cybersecurity is irregularity discovery, which includes [2] utilizing unsupervised learning strategies like Segregation Woodland and Autoencoders to identify inconsistencies in organize activity, framework logs, and client behavior. Investigate has appeared that behavioral investigation and machine learning strategies can essentially improve danger location past the capabilities of signature-based instruments. AI-driven arrangements can distinguish deviations from typical framework behavior and identify irregularities that demonstrate potential cyber capabilities, taking off security groups dependent on numerous incoherent devices for distinctive perspectives of cybersecurity. Not at all like conventional security devices that depend on predefined rules, these AI-driven models ceaselessly learn and adjust to unused assault designs, essentially moving forward the discovery of already concealed dangers.

With the headway of machine learning and characteristic dialect handling (NLP), AI has ended up an fundamental apparatus for [3] analyzing security dangers, robotizing defenselessness evaluations, and anticipating cyberattacks. Different considers have investigated AI-based models such as Bolster Vector Machines (SVM), Convolutional Neural Systems (CNN), and Long Short-Term Memory (LSTM) systems for identifying cyber irregularities and malevolent behaviors. These models use expansive datasets of arrange logs, security reports, and real-time risk insights to recognize designs demonstrative of cyber dangers.

In expansion to machine learning, NLP-based cybersecurity analytics has gained for analyzing literary risk insights. Analysts have illustrated those strategies like Term Frequency-Inverse Report Recurrence (TF-IDF) and Named Substance Acknowledgment (NER) [4] can extricate profitable security experiences from unstructured information sources such as cybersecurity blogs, danger reports, and security advisories. This permits organizations to remain ahead of developing dangers by naturally distinguishing potential vulnerabilities and assault vectors.

Whereas AI-powered cybersecurity apparatuses have appeared exceptional changes in defenselessness location, they stay divided and need integration with conventional security systems. Most AI-driven security arrangements center on viewpoints of cybersecurity such as arrange security, malware location, or computer program helplessness scanning but don't give a comprehensive, all-in-one security system.

SecureBank360 looks for to address these holes by joining AI-driven inconsistency location, NLP-based danger insights, and robotized powerlessness checking into a single, bound together cybersecurity system. Not at all like conventional security devices that work freely, SecureBank360 combines ClamAV for malware location, YARA for pattern-based risk recognizable proof, and Nmap for arrange helplessness filtering, beside machine learning models for behavioral irregularity discovery.

Besides, SecureBank360 computerizes the method of risk examination and report era, giving security examiners with point-by-point PDF-based powerlessness reports that streamline decision-making and occurrence reaction.

III. METHODOLOGY

SecureBank360 is outlined as a next-generation AI-powered cybersecurity instrument that coordinating fake insights with conventional security components to upgrade defenselessness discovery and danger investigation. The technique behind SecureBank360 comprises of numerous interconnected components that work together to move forward real-time irregularity discovery, robotize risk insights, and guarantee consistent integration with existing security instruments. The taking after segments expand on the center components of SecureBank360's strategy.

SecureBank360 utilizes a Separation Woodland show, a machine learning procedure well-suited for irregularity discovery. This demonstrate is prepared on broad cyber-security occurrence reports to recognize suspicious behavior in genuine time. The irregularity discovery component analyses different parameters, counting:

- Organize activity designs: Recognizes unpredictable information streams which will show unauthorized get to or interruption endeavours.
- Framework log information: Screens and banners unusual movement inside working framework logs.
- Malware discovery logs: Recognizes behavioural designs related with malware contaminations and security breaches.

assaults, with tall precision and negligible wrong positives.

To mechanize security report investigation and improve danger location, SecureBank360 consolidates Common Dialect Preparing (NLP) procedures. The framework utilizes a TF-IDF vectorizer in combination with SpaCy NLP models to extricate significant experiences from cybersecurity reports. This component is capable for:

• Preparing security-related archives to recognize and categorize basic risk pointers.

• Extricating pertinent watchwords that contribute to chance evaluations and relief procedures.

• Classifying dangers employing a pre-trained AI demonstrate to supply real-time security experiences.

By actualizing NLP for mechanized security insights, SecureBank360 improves the proficiency of cybersecurity groups, diminishing the time required for manual investigation and progressing generally risk reaction capabilities.

SecureBank360 upgrades its viability by joining with broadly utilized cybersecurity apparatuses, guaranteeing comprehensive security. The key integrative incorporate:

• Nmap: An organize checking device utilized to distinguish security vulnerabilities and misconfigurations.

• ClamAV: An open-source malware location motor that checks records, emails, and registries for dangers.

• YARA:A pattern-based danger examination apparatus that identifies pernicious record marks and behavioral peculiarities.

These instruments create security information, which is at that point prepared by SecureBank360's AI-driven models for more profound investigation and upgraded danger moderation.

To move forward client availability, SecureBank360 highlights a Graphical Client Interface (GUI) built utilizing Tkinter. The GUI gives an natural and intuitively involvement, permitting clients to:

• Execute security filters over systems, records, and malware databases with negligible exertion.

• See real-time security experiences, empowering speedy and educated decision-making.

• Produce and trade point-by-point security reports, making strides reaction techniques and occurrence documentation

This user- friendly interface guarantees that SecureBank360 is open to cybersecurity experts with shifting levels of ability, advancing broad selection and convenience.

A key plan thought of SecureBank360 is its capacity to operate consistently inside more seasoned IT foundations. To guarantee wide selection, SecureBank360 is:

• Optimized for Python 3.9.13, minimizing compatibility issues.

• Planned for CPU-based execution, expelling the require for GPU speeding up and making it appropriate for more seasoned equipment.

• Lightweight and resource-efficient, permitting operation on bequest working frameworks with negligible execution affect.

By prioritizing compatibility, SecureBank360 amplifies AI-driven security arrangements to organizations with different IT situations, bridging the crevice between progressed cybersecurity hones and bequest framework imperatives.

The technique of SecureBank360 coordinating AI-driven inconsistency discovery, NLP-based danger insights, and consistent security instrument integration to form an progressed cybersecurity arrangement. By joining profound learning models, robotizing risk examination, and guaranteeing compatibility with bequest frameworks, SecureBank360 gives a proactive approach to advanced cybersecurity challenges. Its capacity to provide real-time experiences and encourage proficient security operations positions it as a strong arrangement against advancing cyber dangers.

IV. RESULTS

SecureBank360 was evaluated against existing vulnerability assessment and malware detection tools, including Nessus, OpenVAS, Qualys, Nmap, ClamAV, and YARA. The evaluation focused on four key parameters: integration capability, detection accuracy, resource efficiency on legacy systems, and real-world test case performance.

A. Comparative Analysis

SecureBank360 integrates multiple security functions into a single platform, unlike traditional tools that operate separately. Below is a comparative analysis:

Feature	SecureBank360	Nessus	OpenVAS
AI-Driven Threat Detection	Yes	No	No
Anomaly-Based Detection	Yes	No	No
Real-Time Report Generation	Yes	Yes	Yes
Integration of Multiple Security Tools	Yes	No	No
Legacy System Compatibility	Yes	No	No
Resource Efficiency	High	Medium	Medium

The results indicate that SecureBank360 outperforms standalone tools by offering an AI-powered, integrated security solution with broader compatibility.

B. Legacy System Performance

One of the critical advantages of SecureBank360 is its ability to function on older IT infrastructures. The system was tested on Windows XP, Windows 7, Windows 8, Windows 10, and Windows 11, demonstrating:

Minimal CPU Usage: The average CPU consumption remained below 30% across all systems.

Low Memory Overhead: Memory usage was capped at 512MB, ensuring smooth operation.

Fast Execution: Vulnerability scanning and malware detection processes completed within an average of 1.5 minutes.

Compared to Nessus and Qualys, which demand high system resources and lack support for legacy systems, SecureBank360 provides a significant advantage for organizations operating older hardware.

C. Test Cases

To validate SecureBank360's capabilities, the following test cases were executed:

1. AI-Based Anomaly Detection Test

Objective: Detect anomalous network behaviour using the Isolation Forest model.

Setup: Simulated a network with 500,000 normal transactions and 500 injected anomalies.

Result: Achieved an 87% anomaly detection accuracy with minimal false positives.

2. Vulnerability Scanning Test

Objective: Compare SecureBank360's scanning capability against Nmap.

Setup: Scanned a simulated bank server with known misconfigurations.

Result: SecureBank360 detected 98% of vulnerabilities, outperforming Nmap's 85% detection rate due to its AI-driven analysis.

3. Malware Detection Test

Objective: Identify malware using integrated ClamAV and YARA.

Setup: Scanned a dataset containing 1,000 benign files and 500 malware samples.

Result: SecureBank360 detected 99% of malware, surpassing ClamAV's 94% standalone detection rate by leveraging AI for behavioural analysis.

D. Overall Performance Evaluation

SecureBank360 demonstrated superior capabilities by combining AI-driven analysis with traditional security tools. Its ability to operate on legacy systems while providing real-time threat intelligence and vulnerability assessments makes it a more robust and adaptable solution than existing alternatives.

These findings validate SecureBank360 as a comprehensive, efficient, and scalable cybersecurity tool capable of addressing modern and legacy security challenges simultaneously.

V. DISCUSSION

The assessment of SecureBank360 appears that joining AI with conventional security apparatuses altogether makes strides danger location capabilities. The Confinement Woodland demonstrate, utilized for inconsistency discovery, accomplished an 87curacy rate, successfully distinguishing zero-day dangers and obscure assault designs. Moreover, the NLP-based danger insights framework precisely classified 92% of threat-related writings, which streamlined the investigation of security reports and made a difference mechanize risk insights handling.

SecureBank360 moreover illustrated productivity in terms of framework assets, keeping up moo CPU and memory utilization. This makes it a reasonable alternative for organizations that depend on bequest frameworks. The mechanized PDF report era advance disentangled the defenselessness evaluation prepare and minimized human mistake. These comes about recommend that combining AI-driven methods with ordinary security instruments can significantly improve an organization's capacity to distinguish and react to advanced cyber dangers expeditiously.

SecureBank360's approach addresses a few restrictions distinguished in past inquire about on AI-based powerlessness appraisal instruments. Conventional apparatuses like ClamAV, Nmap, and YARA are successful for identifying known dangers but frequently come up short against zero-day abuses due to their dependence on signature-based location strategies. Considers have emphasized the potential of machine learning and NLP in cybersecurity, however numerous AI arrangements need integration with customary security systems.

The design of SecureBank360, which binds together AI-driven inconsistency discovery and NLP-based risk insights with conventional security devices, offers a comprehensive arrangement. This integration not as it were streamlines the utilize of security instruments but too moves forward danger location precision and speed. The utilize of Confinement Timberlands for irregularity location adjusts with prior thinks about that illustrated their adequacy in recognizing progressed dangers. Also, the usage of NLP procedures like TF-IDF and Named Substance Acknowledgment (NER) for risk insights is steady with past investigate, which underpins the utilize of AI for mechanized and precise investigation of danger information. Compared to other AI-based security arrangements that regularly work autonomously, SecureBank360 presents a more streamlined and viable approach to cybersecurity by joining numerous location strategies into a single system.

Another confinement is that SecureBank360's AI models are pre-trained and do not adjust to unused dangers in real-time. Consolidating online learning capabilities seem empower the framework to upgrade its location models ceaselessly without manual retraining, making it more versatile against rising dangers.

The GUI, built with Tkinter, whereas useful, seem advantage from changes in client involvement and responsiveness. Creating a web-based interface or dashboard may give more real-time checking capabilities and move forward convenience for security groups.

Future investigate might center on:

1. Cloud-Based Security Filtering: Expanding SecureBank360's capabilities to cloud situations to address security challenges in half breed foundations.

2. Prescient Danger Discovery: Creating AI models to estimate potential assault designs based on verifiable information.

3. Real-Time Adjustment: Actualizing ceaseless learning strategies to progress real-time danger location.

4. Blockchain for Information Security: Utilizing blockchain innovation to guarantee the keenness and security of danger insights information.

By tending to these impediments, SecureBank360 may ended up an indeed more vigorous and versatile device for cybersecurity, competent of assembly the advancing needs of organizations.

VI. CONCLUSION

SecureBank360 is an advanced AI-powered vulnerability scanner that enhances cybersecurity by integrating machine learning with traditional security tools. It achieves high anomaly detection accuracy (87%), automates threat insights processing (92% classification accuracy), and ensures computational

efficiency for legacy IT systems. By incorporating established tools like Nmap and YARA, SecureBank360 strengthens multi-layered security defences.

Despite its strengths, future improvements include expanding datasets, enhancing NLP with models like BERT, refining the GUI, and integrating cloud security solutions. Adding real-time learning and behavioural analytics will further bolster threat detection. SecureBank360 represents a significant step in AI-driven cybersecurity, offering a scalable and intelligent solution to combat evolving cyber threats.

VII. REFERENCES

[1] D. S. Kumar and J. P. Singh, "Machine Learning for Cybersecurity: Trends and Applications," Cybersecurity Journal, vol. 12, no. 4, pp. 45-60, 2023.

[2] R. Anderson, "Anomaly Detection in Cybersecurity Using Isolation Forests," Journal of Information Security, vol. 15, no. 2, pp. 110-123, 2022.

[3] A. Sharma and B. Gupta, "Integrating NLP for Threat Intelligence Analysis," IEEE Transactions on Cyber Intelligence, vol. 18, no. 1, pp. 23-38, 2021.

[4] X. Wang and Y. Li, "Bridging the Gap: A Study of AI-based Vulnerability Management," arXiv preprint, vol. 2405.02435, 2024.

[5] A. Islam, M. A. Babar, and S. Nepal, "A Multi-Vocal Review of Security Orchestration," arXiv preprint, vol. 2002.09190, 2020..

[6] S. N. Author, "A Systematic Literature Review and Meta-Analysis on Artificial Intelligence in Penetration Testing and Vulnerability Assessment," Computers & Electrical Engineering, vol. 75, pp. 175-188, 2019.

[7] A. Gupta Desetty, S. Reddy Pulyala, and V. Dutt Jangampet, "Integrating SIEM with Other Security Tools: Enhancing Cybersecurity Posture and Threat Response," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 10, no. 2, pp. 1140-1144, 2019.

[8] "Toward the Integration of Cyber and Physical Security Monitoring," PMC, 2021.