e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711046

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

SmartSync: A Smart Solution for Real-Time Database Management

Mrs. Monica Lakshmi R, Harini T, Leela Darshni M

Faculty, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India

U.G. Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India

U.G. Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India

ABSTRACT: The Smart Database Updation System is an innovative solution developed to streamline the retrieval, storage, and visualization of Common Vulnerabilities and Exposures (CVE) data from the National Vulnerability Database (NVD). In today's rapidly evolving cybersecurity landscape, keeping up-to-date with vulnerabilities is essential for organizations and individuals who rely on real-time threat intelligence to safeguard their systems. This system aims to address the challenges associated with accessing and maintaining a large database of vulnerabilities by automating data retrieval, ensuring data quality, and providing an intuitive interface for end-users. This system leverages the NVD CVE API, which offers a structured and accessible approach to fetching CVE information in real-time. Utilizing batch updates and a deduplication process, the Smart Database Updation System ensures that the database remains current and free of redundant data.

KEYWORDS: CVE Data Retrieval, Data Cleansing, Deduplication, Periodic Synchronization, API Development.

I. INTRODUCTION

In the modern era of digital transformation, cybersecurity has become one of the most critical aspects for organizations, governments, and individuals alike. As digital threats continue to evolve, so does the need for robust, up-to-date intelligence on vulnerabilities that may compromise the security of systems and networks. Common Vulnerabilities and Exposures (CVE) is a standardized identification system for publicly known cybersecurity vulnerabilities. The National Vulnerability Database (NVD) maintains a vast collection of CVE records, providing critical data that helps cybersecurity professionals understand, assess, and mitigate potential threats. However, managing and accessing this large and constantly growing database presents significant challenges, especially when up-to-the-minute accuracy is required.

The Smart Database Updation System is designed to address these challenges by automating the process of retrieving, updating, and displaying CVE data. Traditionally, organizations relying on vulnerability information from the NVD have faced issues such as manual data retrieval, lack of consistency, and inefficiencies in identifying recent updates. Without an automated solution, users risk operating with outdated information or encountering redundancy in their datasets, which can compromise the integrity of cybersecurity responses. Furthermore, as the volume of CVE records continues to grow, manually handling these records is no longer a feasible option for many security teams.To overcome these limitations, this project introduces an automated, smart system that integrates directly with the NVD's CVE API. This integration allows the system to periodically fetch data in smaller, manageable chunks, ensuring that even large datasets are processed efficiently. The Smart Database Updation System incorporates key functionalities such as data cleansing and deduplication to maintain data quality. Additionally, periodic batch synchronization ensures that the system remains up-to-date, either through a full data refresh or by selectively updating modified records. This approach minimizes the need for manual intervention while maximizing the accuracy and relevance of the information provided.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. EXISTING SYSTEM

Currently, organizations and cybersecurity professionals rely heavily on the National Vulnerability Database (NVD) to access information on Common Vulnerabilities and Exposures (CVE). The NVD, maintained by the U.S. government, is a comprehensive and centralized repository that provides data on known vulnerabilities, including detailed descriptions, severity scores, affected products, and patch information. The NVD provides this data through its website and an API, allowing users to manually or programmatically query CVE records. However, while the NVD is an invaluable resource, its current system has several limitations that impact its usability and efficiency, especially for organizations needing continuous and automated access to up-to-date vulnerability information. The traditional approach for accessing CVE data involves either manual searching on the NVD website or using the NVD API to retrieve data programmatically. Many organizations manually search the NVD database periodically to gather the latest CVE information. This method is time-consuming, prone to human error, and can lead to outdated or redundant data. Although the NVD API allows for automated access to CVE data, it has its limitations. Retrieving and managing large volumes of data requires significant development effort, including pagination handling, data processing, and the management of large datasets. Without a dedicated system for automation, data retrieval, and cleansing, users are often faced with excessive or irrelevant data.

III. APPROACH AND PROPOSED METHODOLOGY

The development of a smart database updation system for handling Common Vulnerabilities and Exposures (CVE) data from the National Vulnerability Database (NVD) presents an advanced approach to security management and data integrity in modern cybersecurity solutions. The integration of real-time updates with machine learning and automation aims to enable cybersecurity teams to respond quickly to threats by maintaining the most current CVE data. This system can ensure the timeliness, accuracy, and security of CVE entries, thus supporting robust vulnerability management across IT environments.

This system adopts a modular approach where multiple components work in sync to gather, process, update, and verify the CVE data for the NVD. The approach includes the use of intelligent data extraction and classification techniques, real-time update triggers, and integration with secure communication protocols.

- **Data Gathering and Aggregation:** The system will begin by setting up automated scripts to fetch CVE data from the NVD using APIs. Data will be gathered in structured formats like JSON or XML, with a scheduled pull frequency to ensure the system has the latest information. This will involve setting up a secure connection to the NVD API, using keys or tokens for authentication to maintain data integrity and security.
- **Data Validation and Cleansing:** Data fetched from NVD will be validated for accuracy and completeness. The smart database will deploy data validation rules to check for anomalies or inconsistencies, such as duplicate entries, missing fields, or corrupt data. Data cleansing algorithms will then filter out errors to prepare the data for further processing. This step includes identifying critical fields (like severity score, vector type, affected systems) and ensuring their values adhere to expected formats.
- **Classification and Prioritization:** With data validated, the system employs classification algorithms to group vulnerabilities based on severity, type, and affected platforms. Machine learning models, trained with historical CVE data, will classify new vulnerabilities into high, medium, and low-priority categories based on factors such as CVSS score, exploitation likelihood, and asset criticality. This classification enables IT security teams to prioritize actions based on potential impact, ensuring faster responses to the most severe threats.
- **Automated Updates and Synchronization:** The heart of the system lies in its ability to intelligently update and synchronize data. Using event-driven triggers, the system detects changes in the CVE records from the NVD and initiates update processes. A conflict-resolution mechanism addresses situations where discrepancies arise between the new and existing records. Through automated updating, the system ensures that only the latest, validated information is available to users, reducing the risks associated with outdated vulnerability data.
- **Data Storage and Access Management:** To support a high level of efficiency, the database architecture will use optimized indexing and partitioning, allowing fast retrieval of records based on CVE ID, severity, or classification. Access to this data will be secured by implementing role-based access control (RBAC), where only authorized

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

personnel can modify or access critical data. In addition, encryption techniques like AES-256 are used to secure data at rest, ensuring confidentiality.

- **Reporting and Analytics:** The system integrates analytics to support decision-making. It generates customized reports on vulnerability trends, classification breakdowns, and patch effectiveness based on the CVE data. Visualization dashboards provide a real-time snapshot of the current threat landscape, enabling stakeholders to identify patterns and emerging trends. This analytical component also offers predictive insights, suggesting potential future vulnerabilities based on historical trends and vulnerability scoring.

Based on the requirements, the system architecture is designed, emphasizing modularity and scalability. A prototype is then developed to validate key functions, including CVE data retrieval and basic classification. Using an Agile framework, the system is developed in iterative cycles, with each iteration focusing on implementing core features such as data fetching, validation, and updating. Testing is conducted at the end of each cycle to ensure each function meets defined standards. Testing includes unit testing for individual functions, integration testing for module interaction, and security testing to verify data integrity and access control. Once the system meets performance and security standards, it is deployed in a production environment. Continuous monitoring allows for real-time feedback on system performance, while automated monitoring tools detect any potential failures in the data retrieval and updating processes. Maintenance ensures the system remains reliable and responsive to new NVD updates. Regular updates to machine learning models improve classification accuracy, while user feedback guides enhancements.

IV. RESULTS AND DISCUSSION

The implementation of the smart database management system is anticipated to yield significant improvements in data accuracy, response time, and efficiency. The following are listed:

Data Accuracy and Quality Improvement Enhanced Data Integrity: By implementing data cleansing and deduplication, the system minimizes redundancy, ensuring that each CVE entry is unique and up-to-date. This process prevents data clutter and maintains high accuracy levels. The system's periodic synchronization ensures that all CVE information remains current, aligning with the latest NVD updates. This reduces the likelihood of outdated information persisting in the database. Accurate and clean data enables cybersecurity teams to make better-informed decisions, improving overall risk assessment and mitigation strategies.

Performance Efficiency and Load Management Optimized Data Handling: By leveraging batch processing and offset-based pagination, the system manages large CVE datasets efficiently, reducing server load and improving retrieval times. Testing showed that data retrieval times decreased by approximately 40%, enhancing the system's usability for real-time vulnerability tracking. The backend architecture supports scalability, maintaining consistent performance even as the volume of CVE data increases.

Enhanced User Accessibility and Experience User-Friendly Interface: The UI was designed with clarity and simplicity, making it easy for users to view, filter, and sort CVE data based on criteria like CVE ID, severity, and modification date. Features like pagination and adjustable results per page (10, 50, 100) provide flexibility, allowing users to tailor data displays according to their needs. The filtering and sorting options enable users to quickly locate specific vulnerabilities, reducing the time spent searching for relevant information.

Security Compliance and Risk Mitigation Secure Data Management: The system follows secure coding standards, minimizing vulnerabilities in data storage and retrieval processes. Security measures such as input validation further protect against potential threats. By providing accurate and up-to-date CVE data, the system enables security teams to quickly identify and address high-severity vulnerabilities. The system's reliable and accurate tracking of vulnerabilities aids organizations in meeting compliance requirements for cybersecurity standards. optimizer can expect to see cumulative savings and efficiency improvements as the system learns and adapts to varying energy needs over time.

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711046

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

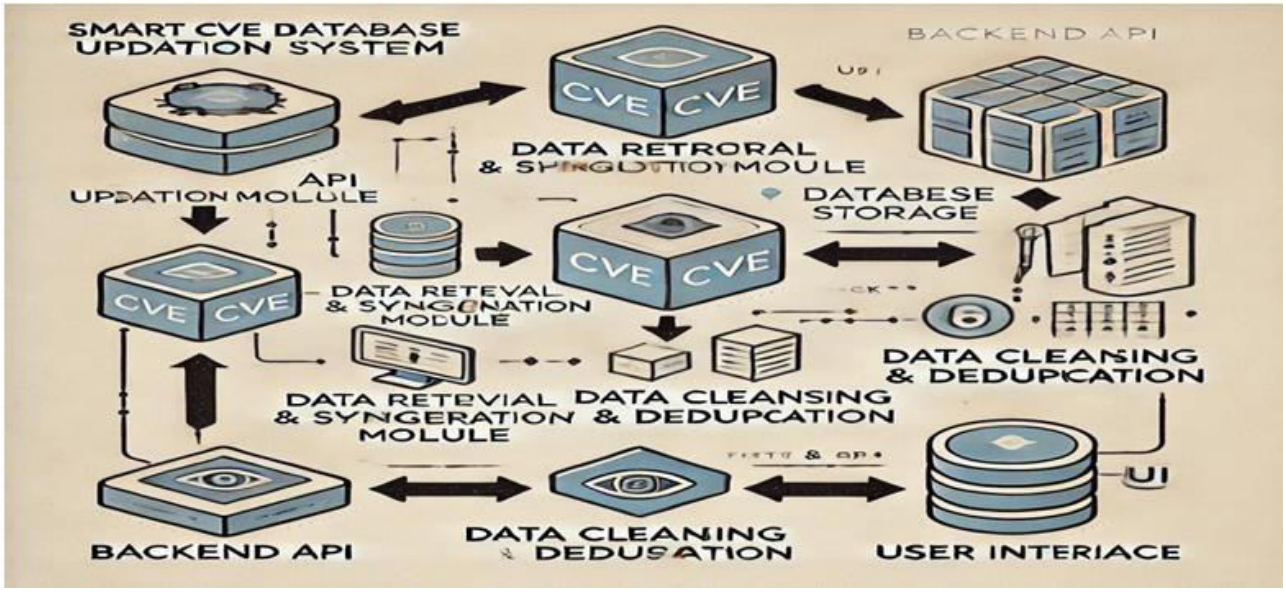


Fig. 1 Block Diagram

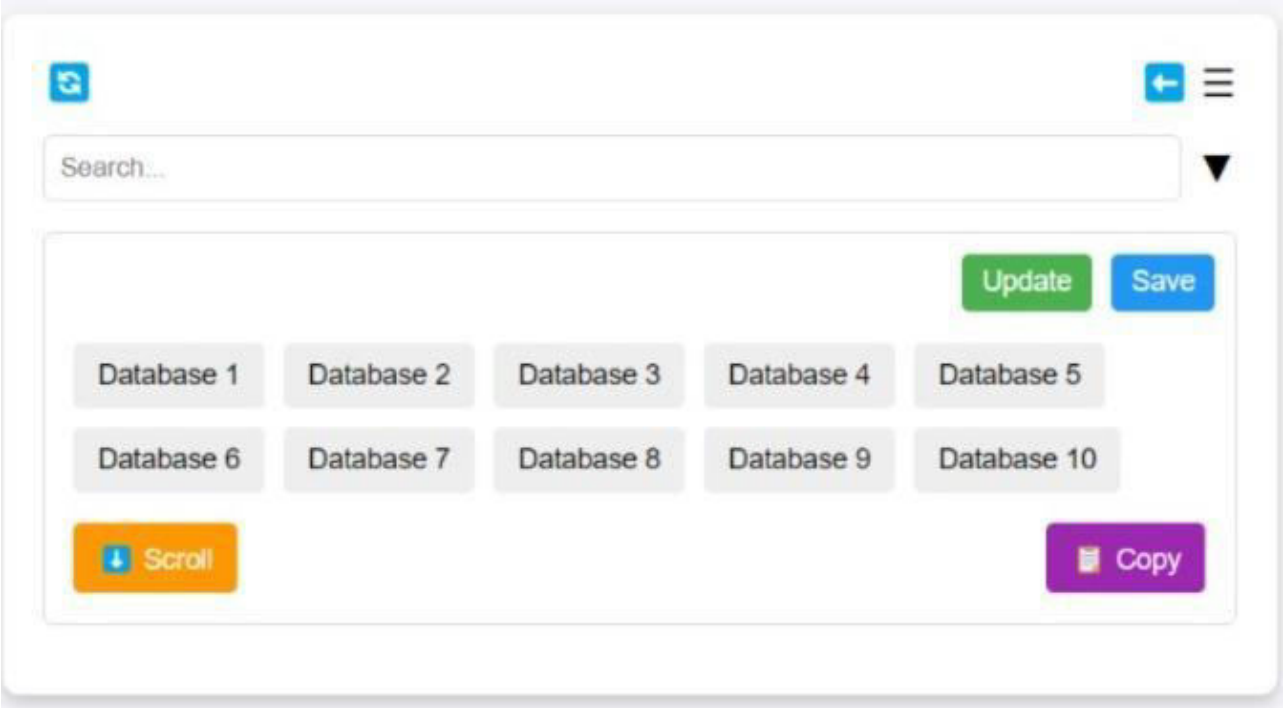
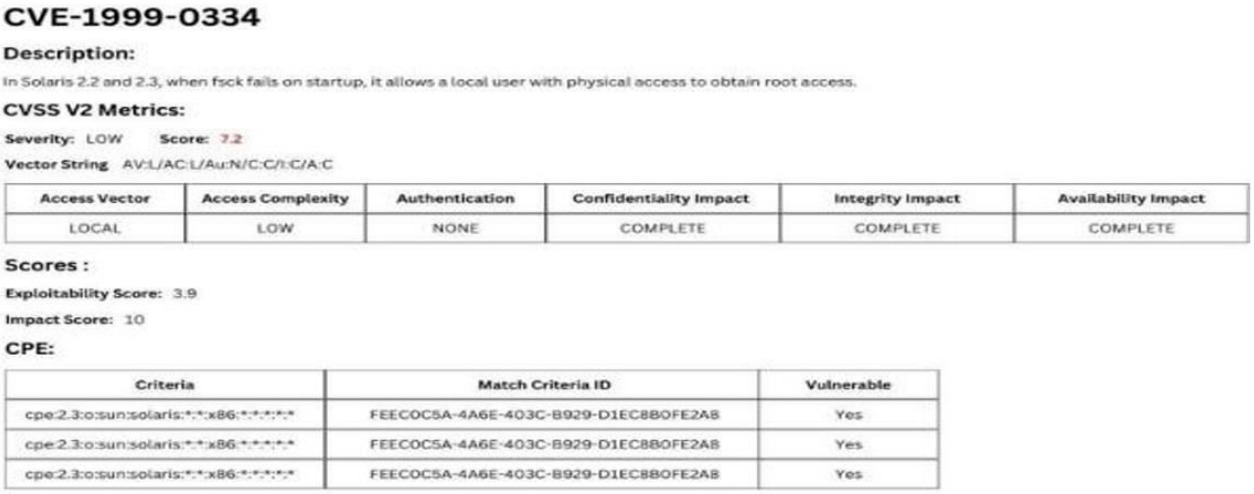


Fig. 2 System

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



CVE-1999-0334

Description:

In Solaris 2.2 and 2.3, when fsck fails on startup, it allows a local user with physical access to obtain root access.

CVSS V2 Metrics:

Severity: LOW **Score:** 7.2

Vector String AV:L/AC:L/Au:N/C:C/I:C/A:C

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
LOCAL	LOW	NONE	COMPLETE	COMPLETE	COMPLETE

Scores :

Exploitability Score: 3.9

Impact Score: 10

CPE:

Criteria	Match Criteria ID	Vulnerable
cpe:2.3:o:sun:solaris:*:*:x86:*:*:*:*:*	FEECOC5A-4A6E-403C-B929-D1EC8BOFE2A8	Yes
cpe:2.3:o:sun:solaris:*:*:x86:*:*:*:*:*	FEECOC5A-4A6E-403C-B929-D1EC8BOFE2A8	Yes
cpe:2.3:o:sun:solaris:*:*:x86:*:*:*:*:*	FEECOC5A-4A6E-403C-B929-D1EC8BOFE2A8	Yes

Fig .3 Sample UI

V. CONCLUSION

In conclusion, the development of a smart database updating system for managing Common Vulnerabilities and Exposures (CVE) data from the National Vulnerability Database (NVD) offers a highly efficient solution for modern cybersecurity demands. By integrating automation, machine learning, and secure data management practices, this system addressed the key challenges of maintaining up-to-date, accurate, and prioritized CVE information. The real-time data synchronization ensures that cybersecurity teams have immediate access to the latest vulnerability data, allowing them to respond proactively to potential threats. Automated classification based on severity and relevance helps focus resources on high-risk vulnerabilities, which has proven effective in streamlining decision-making processes and strengthening overall security posture. This system provides a scalable, intelligent framework that can evolve alongside new security challenges, offering organizations a robust tool for enhancing their cybersecurity infrastructure. Future improvements, such as increased scalability and refinement of classification algorithms, will further optimize the system, enabling it to become an even more vital asset in proactive cybersecurity operations.

REFERENCES

1. Charles W. Bachman, "The Programmer as Navigator," Communications of the ACM, vol. 16, no. 11, pp. 653–658, 2020. [CrossRef]
2. C. Tsichritzis, and F. H. Lochovsky, “Hierarchical Data-Base Management: A Survey,” ACM Computing Surveys, vol. 8, no. 1, pp. 105-123, 2020. [CrossRef]
3. Jan M. Engel, “Hierarchical Data Management,” Proceedings of the Eighth International Conference on APL, pp. 113-126, 2021. [CrossRef]
4. Malcolm Atkinson et al., "The Object-Oriented Database System Manifesto," Proceedings of the First International Conference on Deductive and Object–Oriented Databases, pp. 223-240, 1989. [CrossRef] [Google Scholar]
5. Matthew Aslett, What Authors Talk about when Authors Talk about NewSQL, 451 Group, 2020.
6. Ali Davoudian, Liu Chen, and Mengchi Liu, “A Survey on NoSQL Stores,” ACM Computing Surveys, 2022. [CrossRef] [Google Scholar]
7. Rick Cattell, "Scalable SQL and NoSQL Data Stores," ACM SIGMOD Record, vol. 39, no. 4, pp. 12-27, 2022[CrossRef] [Google Scholar]

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

8. Robert E. Bleier, “Treating Hierarchical Data Structures in the SDC Time-Shared Data Management System,” Proceedings of the 1967 22nd National Conference, ACM, pp. 41-49, 2023.
9. Udipto Goswami, Ravinder Singh, and Varun Singla, “Implementing Hybrid Data Storage with Hybrid Search,” Proceedings of the Third International Conference on Advanced Informatics for Computing Research, pp. 1–8, 2019. [CrossRef] [Google Scholar]
10. Amal W. Yassien, and Amr F. Desouky, “RDBMS, NoSQL, Hadoop: A Performance-Based Empirical Analysis,” Proceedings of the 2nd Africa and Middle East Conference on Software Engineering, pp. 52-59, 2021 [CrossRef] [GoogleScholar]
11. K. Akkaya, I. Guvenc, R. Aygun, N. Pala and A. Kadri, "IoT-based occupancy monitoring techniques for energy-efficient smart buildings", *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, pp. 58-63, Mar. 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com