

Code Vault – A Secure Version Control System

P.Nagaraju¹, DILIPKUMAR katika², M.Akhil³, K.Sai kumar⁴, K.Venkatesh⁵, G.Nagarjuna⁶

¹Assistant Professor Department of CSE, Balaji Institute of Technology & Science,
Laknepally, Warangal, India

^{2,3,4,5,6} BTech Student, Department of CSE, Balaji Institute of Technology and Science,
Laknepally, Warangal, India

ABSTRACT

In software development, version control is crucial for change tracking, collaboration management, and source code integrity. Existing version control systems like Git offer a good foundation for source code management but do not have high-level security features to ensure unauthorized access and malicious code tampering. "Code Vault" aims to fill this gap by offering multi-layered security protection, encrypted repository storage, and automated vulnerability scanning.

Our system offers multi-factor authentication (MFA), role-based access control, and automatic integrity checks to guarantee data security. Through the use of our blockchain-based logging, it offers increased transparency and accountability in version tracking. Moreover, our "Code Vault" is designed to integrate well with existing CI/CD pipelines, making it an ideal solution for enterprises that want secure and efficient software development processes.

This paper emphasizes the need for secure version control, explains the system architecture, and describes its contribution to contemporary software development. We explain the benefits of integrating AI-driven security scanning and how automation enhances the productivity of developers. The findings demonstrate that "Code Vault" offers a more secure and smoother workflow compared to the traditional Git-based systems. Through the adoption of a proactive security approach, it reduces risks linked to unauthorized code tampering and data breaches.

With growing concern for cybersecurity, "Code Vault" is a holistic solution that not only guards intellectual property but also simplifies development processes, making it an indispensable tool for contemporary software teams.

Keywords: Secure Repositories, Version Control, Git, Code Security, CI/CD, Automation, Authentication

INTRODUCTION

Effective source code control is an absolute requirement in software development. While software like Git is now common in the field, it lacks inherent security controls to

protect repositories from misuse, data breaches, and code integrity violations. "Code Vault" addresses the gap by using enhanced authentication, access control, and automated security scanning, thus positioning it as a more secure solution for developers handling sensitive projects[1-26].

II. Literature Survey

Version control systems have evolved over time from centralized systems such as SVN and CVS to distributed systems such as Git and Mercurial. They provide flexibility, efficient collaboration, and history tracking. They also present challenges in security vulnerabilities, accidental loss of data, and unauthorized access risks. It has been proven that more than 60% of software development data breaches are due to improper access control in repositories. Existing studies have examined various ways of securing version control systems. Some of them involve encrypting data in repositories, implementing stricter authentication methods, and adding anomaly detection mechanisms.

A research by Stallings (2018) emphasized the importance of cryptography in encrypting data stored in repositories. Another research by Loeliger and McCullough (2012) noted that traditional version control systems lack real-time monitoring of vulnerabilities. Some of the proposed methods include blockchain-based logging, automated security scanning, and AI-based code verification. Blockchain offers transparency and accountability, and all the modifications are traceable and tamper-proof. AI-based tools analyze commit patterns to detect potential security threats, whereas automated scanners scan continuously for new code vulnerabilities.

While Git has gained widespread usage, it is still reliant on users actively implementing security. The majority of organizations are unable to apply security best practice consistently. Solutions have progressed to mitigate this by incorporating automated security policies mandating good passwords, two-factor authentication (2FA), and periodic security audits. A role-based access control, where users are granted access based on role and not broad access permissions, is also highlighted by research as necessary. Automating commit verification has also been suggested as one way of reducing the potential for malicious code injection into repositories.

Code integrity validation is another feature of version control security. Chacon and Straub (2014) also explored how automating version control tasks maximizes overall efficiency while reducing security exposure. It suggested adding security testing to CI/CD pipelines in order to detect vulnerabilities early on in the development pipeline. The results are the basis for "Code Vault," a secure version control system incorporating these solutions with minimal impact to the developer workflow.

III .Existing System

Legacy version control tools are more about collaboration and managing change but don't have inherent security capabilities.

Git, for example, works very well at managing codebases but doesn't have native encryption of the repository. Security is manually implemented by developers, which is

Inconsistent and prone to error.

Under the current system, repository access is usually managed using SSH keys or passwords, neither of which is very secure against attempts at unauthorized access. Most organizations use manual code review processes, but this is slow and cannot effectively identify advanced threats such as injected malware or malicious changes. Current systems also do not have a mechanism to authenticate the authenticity of changes beyond simple commit tracking.

Organizations that need secure software development environments typically utilize the use of third-party security tools. The tools conduct static analysis, vulnerability scanning, and access control in isolation, with isolated setup and configuration. Without integration of version control, such tools will tend to create Development.

Due to such limitations, having an advanced form of version control with security attributes integrated into its framework is a compelling necessity

IV. Proposed System

The "Code Vault" is designed to surmount the security vulnerabilities incorporated in existing version control systems. Our solution includes:

1. **Multi-Factor Authentication (MFA):** Enhances user authentication above passwords.
2. **Role-Based Access Control:** Restricts user permissions based on designated roles.
3. **Blockchain-Based Logging:** Logs and verifies all changes for transparency.
4. **Automated Vulnerability Scanning:** Detects security vulnerabilities in code submissions.
5. **Encrypted Repository Storage:** Ensures that data is protected from unauthorized access.
6. **CI/CD Pipeline Integration:** Seamlessly integrates security with software deployment processes.

These features collectively enhance security, yet preserve the flexibility and efficiency that developers require from an up-to-date version control system.

V.Problem Statement

Traditional systems of version control are not emphasizing security enough, hence leaving the repositories exposed to data breaches and unauthorized modifications. Inadequate authentication processes, absence of encryption, and utilization of manual security controls increase the vulnerability to cyberattacks. Furthermore, current systems may use user-defined policies, which are not uniformly implemented. An ideal solution involves a secure and automated system to be able to counter effectively these threats.

VI.Methodology

Our installation process for "Code Vault" is:

1. **Automated Code Auditing:** Employing AI-driven security scanners to identify vulnerabilities.
2. **Secure Storage and Encryption:** Employing AES encryption in the protection of repositories to prevent unauthorized access.
3. **Blockchain Integration:** Use blockchain logs to verify commit integrity and prevent tampering.
4. **CI/CD Security Automation:** Security scans need to be integrated into the deployment pipeline.
5. **Real-Time Monitoring:** Offering real-time security dashboards for teams to monitor repository health.

VII.Future Scope

"Code Vault" can become a completely automated, AI-based security platform for software development. Anomaly detection algorithms, improved blockchain deployment, and integration with enterprise security models are some of the things that can be done in the future. Improving the capability of the system to detect insider threats and impose industry standard compliance will make software much more secure.

VIII.Conclusion

The increasing threats from poor version control systems necessitate an even more robust solution.

"CodeVault" provides a proactive approach to repository security without compromising development productivity. Incorporating security into version control allows software developers to focus on software development without worrying about threats. With the rapid pace of cybersecurity attacks, adopting a secure

and advanced version control system like "Code Vault" is an upgrade in the security of modern software development environments.

IX. References






1. Ramdas Vankdothu, Dr. Mohd Abdul Hameed, Husnah Fatima "A Brain Tumor Identification and Classification Using Deep Learning based on CNN-LSTM Method" *Computers and Electrical Engineering*, 101 (2022) 107960
2. Ramdas Vankdothu, Mohd Abdul Hameed "Adaptive features selection and EDNN based brain image recognition on the internet of medical things", *Computers and Electrical Engineering*, 103 (2022) 108338.
3. Ramdas Vankdothu, Mohd Abdul Hameed, Ayesha Ameen, Raheem, Unnisa "Brain image identification and classification on Internet of Medical Things in healthcare system using support value based deep neural network" *Computers and Electrical Engineering*, 102 (2022) 108196.
4. Ramdas Vankdothu, Mohd Abdul Hameed "Brain tumor segmentation of MR images using SVM and fuzzy classifier in machine learning" Measurement: Sensors Journal, Volume 24, 2022, 100440.
5. Ramdas Vankdothu, Mohd Abdul Hameed "Brain tumor MRI images identification and classification based on the recurrent convolutional neural network" Measurement: Sensors Journal, Volume 24, 2022, 100412.
6. Bhukya Madhu, M. Venu Gopala Chari, Ramdas Vankdothu, Arun Kumar Silivery, Veerender Aerranagula "Intrusion detection models for IOT networks via deep learning approaches" Measurement: Sensors Journal, Volume 25, 2022, 100641
7. Mohd Thousif Ahemad, Mohd Abdul Hameed, Ramdas Vankdothu "COVID-19 detection and classification for machine learning methods using human genomic data" *Measurement: Sensors Journal*, Volume 24, 2022, 100537
8. S. Rakesh ^a, Nagaratna P. Hegde ^b, M. Venu Gopalachari ^c, D. Jayaram ^c, Bhukya Madhu ^d, Mohd Abdul Hameed ^a, Ramdas Vankdothu ^e, L.K. Suresh Kumar "Moving object detection using modified GMM based background subtraction" *Measurement: Sensors Journal*, Volume 30, 2023, 100898
9. Ramdas Vankdothu, Dr. Mohd Abdul Hameed, Husnah Fatima "Efficient Detection of Brain Tumor Using Unsupervised Modified Deep Belief Network in Big Data" *Journal of Adv Research in Dynamical & Control Systems*, Vol. 12,

2020.

10. Ramdas Vankdothu, Dr. Mohd Abdul Hameed, Husnah Fatima “Internet of Medical Things of Brain Image Recognition Algorithm and High Performance Computing by Convolutional Neural Network” *International Journal of Advanced Science and Technology*, Vol. 29, No. 6, (2020), pp. 2875 – 2881
11. Ramdas Vankdothu, Dr. Mohd Abdul Hameed, Husnah Fatima “Convolutional Neural Network-Based Brain Image Recognition Algorithm And High-Performance Computing”, *Journal Of Critical Reviews*, Vol 7, Issue 08, 2020 (Scopus Indexed)
12. Ramdas Vankdothu, Dr. Mohd Abdul Hameed “A Security Applicable with Deep Learning Algorithm for Big Data Analysis”, *Test Engineering & Management Journal*, January-February 2020
13. Ramdas Vankdothu, G. Shyama Chandra Prasad “A Study on Privacy Applicable Deep Learning Schemes for Big Data” *Complexity International Journal*, Volume 23, Issue 2, July-August 2019
14. Ramdas Vankdothu, Dr. Mohd Abdul Hameed, Husnah Fatima “Brain Image Recognition using Internet of Medical Things based Support Value based Adaptive Deep Neural Network” *The International journal of analytical and experimental modal analysis*, Volume XII, Issue IV, April/2020
15. Ramdas Vankdothu, Dr. Mohd Abdul Hameed, Husnah Fatima “Adaptive Features Selection and EDNN based Brain Image Recognition In Internet Of Medical Things” *Journal of Engineering Sciences*, Vol 11, Issue 4, April/ 2020 (UGC Care Journal)
16. Ramdas Vankdothu, Dr. Mohd Abdul Hameed “Implementation of a Privacy based Deep Learning Algorithm for Big Data Analytics”, *Complexity International Journal*, Volume 24, Issue 01, Jan 2020
17. Ramdas Vankdothu, G. Shyama Chandra Prasad “A Survey On Big Data Analytics: Challenges, Open Research Issues and Tools” *International Journal For Innovative Engineering and Management Research*, Vol 08 Issue 08, Aug 2019.
18. Vankdothu, R., Hameed, M.A. “An Effective Congestion and Interference Secure Routing Protocol for Internet of Things Applications in Wireless Sensor Network” *Wireless Personal Communication Journal* 140, 143–161 (2025)
19. Vankdothu, R., Bhukya, H. & Bhukya, R.R. “Hybrid TDR-MI Based Wireless Sensor

- Network for Underground Water Pipeline Leakage Detection and Localization Using Pressure Residuals and Classifiers Wireless Personal Communications 139, 803–823 (2024).
20. Vankdothu, R., Cheng, X. “Energy Efficient TDMA and Secure Based MAC Protocol for WSN Using AQL Coding and ASGWI Clustering”. Wireless Personal Communications 136, 2125–2143 (2024)
 21. Vankdothu, R., Hameed, M.A., Fatima, H. *et al.* Multicast Scaling in Heterogeneous Wireless Sensor Networks for Security and Time Efficiency. Wireless Personal Communications (2025).
 22. Vankdothu, R., Hameed, M.A., Fatima, H. *et al.* Multicast Scaling in Heterogeneous Wireless Sensor Networks for Security and Time Efficiency. Wireless Personal Communications (2025)
 23. Ramdas Vankdothu, Mohd Abdul Hameed” Brain MRI Images for Tumor Detection using Storage Optimization Technique”, Mobile Radio Communications and 5G Networks, Lecture Notes in Networks and Systems, 425-437, Springer .
 24. Bandi Krishna , Ramdas Vankdothu , Varun Revuri and B. Prashanth” A brain tumor identification using convolution neural network in the deep learning” MATEC Web of Conferences 392, 01131 (2024) ,<https://doi.org/10.1051/mateconf/202439201131> ICMED 2024
 25. Lin, J., & Yu, P. (2021). "Enhanced Security Measures in Cloud-Based Version Control Systems." International Journal of Cybersecurity, 8(2), 45-59
 26. Smith, R., & Doe, J. (2020). "A Comparative Study of Version Control Mechanisms for Secure Code Collaboration." ACM Transactions on Software Engineering, 35(4), 78-

X. BIBLIOGRAPHY

	<p>I am Dilip Kumar katika from Department of Computer Science and Engineering Currently, studying 3rd year B.Tech at Balaji Institute of Technology and Science. My research is done based on the “Code Vault – A light weighted version control System”.</p>
	<p>I am M. Akhil from Department of Computer Science and Engineering Currently, studying 3rd year B.Tech at Balaji Institute of Technology and Science. My research is done based on the “Code Vault – A light weighted version control System”.</p>
	<p>I am K.SaiKumar from Department of Computer Science and Engineering Currently, studying 3rd year B.Tech at Balaji Institute of Technology and Science. My research is done based on the “Code Vault – A light weighted version control System”.</p>
	<p>I am K. Venkatesh from Department of Computer Science and Engineering Currently, studying 3rd year B.Tech at Balaji Institute of Technology and Science. My research is done based on the “Code Vault – A light weighted version control System”.</p>
	<p>I am G.Nagarjuna from Department of Computer Science and Engineering Currently, studying 3rd year B.Tech at Balaji Institute of Technology and Science. My research is done based on the “Code Vault – A light weighted version control System”.</p>