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

Safeguarding Large Datasets: A Multifaceted Approach to Database Security

Sumit Bhise[1], Asst. Prof. Bindy Wilson[2]

[1]Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra
[2] Guide, Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra

ABSTRACT

This research explores innovative techniques to beautify database security, inclusive of homomorphic encryption for privacy-preserving computations, blockchain for data integrity, behavioral biometrics for user entry and control, and differential privacy for balancing data software and privacy. It also addresses quantum computing threats, dynamic generation of access to manipulate, AI-push anomaly detection, and computational-physical database security. The proposed Onion model adds, in addition, layer through robotically erasing records in cases of unauthorized get entry to imparting strong safety capabilities for organizations.

Keywords: Database Security, Homomorphic Encryption, Blockchain for Data Integrity, Behavioral Biometrics, Differential Privacy, Quantum Computing Countermeasures, Dynamic Access Control Policies, Secure multi-party computation, AI-driven anomaly detection, federated learning, Cyber-Physical Database Security, Onion Model, Data Privacy, Encryption Techniques, Tamper-Proof Ledgers, Trust and Reliability, User Access Control, Real-time Access Control, Collaborative Computations, Anomaly Detection, Distributed Learning, Cybersecurity, Privacy-Preserving Techniques, Threat Mitigation, and Preemptive Security Measures.

INTRODUCTION

In the ever-evolving panorama of information generation, ensuring the security of organizational databases is a paramount concern. This study paper embarks on an adventure to discover modern-day strategies aimed at fortifying database security throughout multifaceted dimensions, tackling present-day challenges even as looking ahead to the looming specter of destiny threats.

At the forefront of this exploration is the pragmatic assessment of homomorphic encryption, an innovative method poised to reshape the security paradigm of databases. By allowing computations on encrypted statistics inside the confines of databases, this technique pioneers a route that not only safeguards record privacy but also ensures the computational process, imparting a promising trajectory for steady information processing.

Another pivotal domain under scrutiny is the mixing of blockchain and data integrity. The research seriously assesses how blockchain generation, with its decentralized and tamper-evident ledgers, can function as a strong mechanism to enhance the integrity of big databases. The attention is on establishing blockchain as a trustworthy basis that enhances reliability and engenders acceptance as true with problematic database architectures.

Delving into the realm of behavioral biometrics, the paper scrutinizes the feasibility of incorporating diffused nuances together with typing patterns or mouse actions as extra layers for personalized get-right of entry to manage. Insights garnered from this investigation contribute to the development of greater security features grounded in the complicated behavioral patterns of personal customers.

The observation further navigates the delicate balance between facts' utility and privateness in massive-scale datasets via the lens of differential privacy. By implementing nuanced mechanisms, the studies seek to shield personal statistics from prying eyes during database queries, offering a nuanced method for privacy upkeep.

In reaction to the looming risk of quantum computing, the studies explore quantum computing countermeasures. This section unveils and evaluates encryption strategies that exhibit resilience in opposition to quantum threats, serving as preemptive measures for stable databases in a generation of rising quantum skills.

Beyond those, the exploration encompasses dynamic access control policies, secure multi-party computation, AI-driven anomaly detection, federated learning, and cyber-physical database security. Each topic contributes to a holistic comprehension of database security, presenting insights into actual-time access manipulation, collaborative computations, anomaly detection, dispensed studying, and the complicated intersection between cyber and physical security.

In addressing the pervasive problem of information leaks, the proposed onion model emerges as a sturdy shield. This modern method subdivides layers in the database, routinely erasing statistics in the face of unauthorized admission attempts, adding an extra layer of safety to the organizational data citadel. In essence, the culmination of these research findings aspires to serve as a guiding compass for agencies, empowering them to put into effect sturdy security features and fortify their databases against potential threats correctly.

Literature Study

The first paper addresses the pivotal position of database safety and the growing reliance on databases. It proposes a strong methodology concerning threat assessment, security evaluation, multi-layered defense, least privilege enforcement, everyday updates, protection audits, patron training, information encryption, activity tracking, incident reaction planning, and non-preventive development. By emphasizing proactive measures, the technique ensures the continual safeguarding of essential data in the face of evolving threats and ability breaches. [1]

The second paper involves a focused exploration of techniques for ensuring data and persistent stored database modules' integrity, aligning with the Clark-Wilson model's recommendations. This study relies on a database structured on a universal basis of relationships. It integrates relational database theory, Row Level Security technology, blockchain models, and database management system capabilities. The developed mechanisms effectively control database integrity, prevent unauthorized modifications, and maintain the correctness, integrity, and protection of stored data and programs. This establishes robust protection for databases, employing the universal basis of relationship schema. [2]

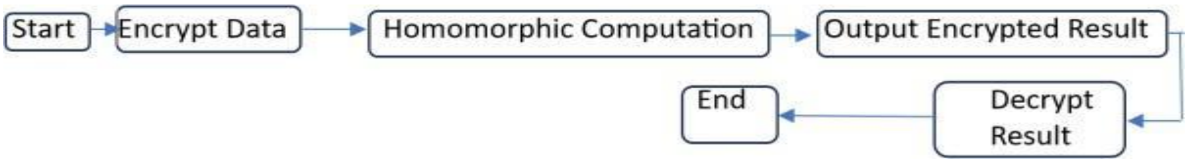
The third paragraph examines the escalating cyber threats resulting from increased internet usage and emphasizes the need for effective cybersecurity policies. Recognizing the impact on individual users, corporations, and national security, the study delves into the cybersecurity regulations and attributes of seven nations. Forty common cybersecurity attributes, including communication, network, cloud computing, online banking, e-commerce, identity theft, privacy, and smart grid, were identified. The research highlights variations in policy emphasis among nations, aiding academics and policymakers in developing comprehensive cybersecurity strategies. The next revolution may broaden this investigation to include other countries' cybersecurity policies. [3]

DESCRIPTION OF THIS TOPIC:

Homomorphic Encryption Homomorphic encryption represents a groundbreaking paradigm shift within the realm of database protection. Traditional encryption methods usually contain decrypting facts before acting computations, exposing them to potential vulnerabilities. However, homomorphic encryption introduces a unique approach with the aid of enabling computations without delay on encrypted records within databases. This transformative technique ensures a heightened level of data privacy and computational efficiency.

In essence, homomorphic encryption allows complicated operations to be completed on encrypted information without the need for decryption, retaining the confidentiality of sensitive facts throughout the processing pipeline. This now not only shields records from unauthorized entry but additionally mitigates the risk of publicity in the course of computational methods.

The protection implications are profound, as homomorphic encryption establishes a strong defense against capacity threats and manipulations of sensitive facts. It provides an advanced solution for scenarios wherein information privacy is paramount, together with healthcare, finance, or other industries managing sensitive private information. By preserving computational functionality while safeguarding confidentiality, homomorphic encryption emerges as a transformative device, ushering in a new era of secure and privacy-centric database control. Its adoption signifies a proactive and advanced approach to information safety in a more and more interconnected and information-driven global.



Blockchain Integration for Data Integrity

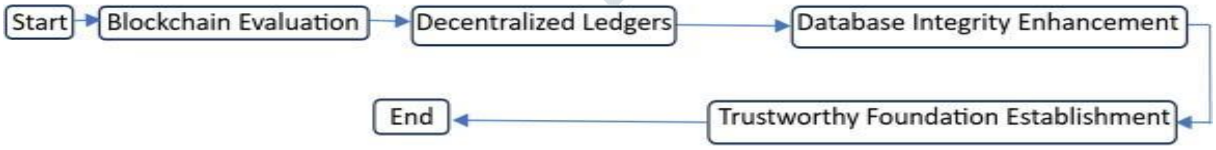
Blockchain Integration for Data Integrity entails an essential assessment of blockchain technology as a modern method to enhance the safety and reliability of databases.

Blockchain involves evaluating its core functions, which consist of decentralization and tamper-obtrusive ledgers.

In the flowchart, the technique starts with a complete assessment of the blockchain era. Blockchain operates on a decentralized network of nodes, wherein every participant holds a copy of the ledger. This decentralized nature ensures that there's no unmarried point of failure, improving the general protection of the machine.

The tamper-obtrusive nature of blockchain, as represented within the flowchart, ensures that once facts are recorded in a block, they become practically immutable. This feature ensures the integrity of the facts saved in the database.

The integration of blockchain enhances database integrity by providing a steady and transparent framework. Each transaction is recorded in a block, connected to the preceding one via cryptographic hashes, forming an unchangeable chain of facts. This is not the simplest safeguard in opposition to tampering, but it also establishes a straightforward foundation for reliability and belief. The decentralized and tamper-obtrusive capabilities of blockchain together make contributions to elevating the overall integrity and safety of databases in a transparent and decentralized way.


Start
Blockchain Evaluation
Decentralized Ledgers
Database Integrity Enhancement
Trustworthy Foundation Establishment
End

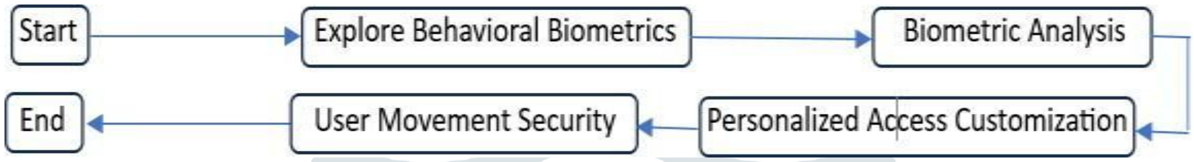
Biometric Security Measures for Future Threats

In the world of advanced cybersecurity, this paper delves into three pivotal subjects addressing futuristic challenges. First, Behavioral Biometrics for Personalized Access Control explores the intricacies of personal behavior as a security layer. By scrutinizing typing styles and mouse actions, this method develops personalized access to controls, bolstering protection based totally on precise user movements.

Next, Differential Privacy in Large-Scale Datasets navigates the delicate equilibrium between facts, software, and privacy. Implementing nuanced mechanisms takes a look at seeking to guard personal data during database queries. This nuanced method ensures that the statistic's utility is preserved while concurrently safeguarding the privacy of character users, an essential situation in the era of big facts.

Lastly, the paper delves into quantum computing countermeasures to preemptively cope with the rising hazards of quantum computing. This entails unveiling and evaluating encryption strategies for proof against quantum talents and securing databases against potential quantum threats.

Together, those subjects form a comprehensive exploration of current security features, from the expertise and making use of behavioral biometrics for admission to manipulation to preserving privateness in large-scale datasets and making ready databases for quantum technology. The integration of those measures represents a holistic approach to toughening facts and safety in the face of evolving technological landscapes.


Start
Explore Behavioral Biometrics
Biometric Analysis
Personalized Access Customization
User Movement Security
End

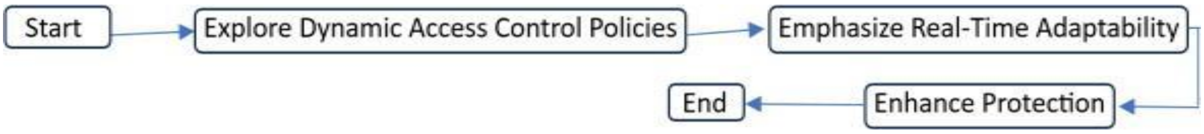
Holistic Database Security: A Comprehensive Approach

This paper navigates numerous dimensions of database security through three key subjects. Firstly, it explores dynamic access control policies, emphasizing actual-time adaptability to enhance protection. Next, Secure Multi-Party Computation allows collaborative computations without compromising record confidentiality, fostering secure collaboration. AI-driven anomaly detection takes a proactive stance, identifying security threats before they expand.

Further, Federated Learning introduces a paradigm for privacy-retaining device learning in disbursed databases. Finally, Cyber-Physical Database Security investigates the intersection of cyber and physical threats, imparting nuanced information.

The paper introduces the Onion Model as a robust shield, offering an innovative approach to dealing with record leaks. Subdividing layers inside the database ensures more desirable protection, robotically erasing data in response to unauthorized access attempts.

In a holistic approach, cumulative insights from those topics contribute to comprehensive expertise in database security. The integration of real-time admission management, collaborative computations, anomaly detection, and distributed mastering empowers agencies to put into effect powerful and sturdy security measures. This holistic approach reflects a proactive and superior method of safeguarding databases in an ever-evolving cybersecurity panorama.


Start
Explore Dynamic Access Control Policies
Emphasize Real-Time Adaptability
Enhance Protection
End

FINDINGS

1) Homomorphic encryption signifies a groundbreaking shift in database safety, permitting computations on encrypted facts.
2) Blockchain integration for fact integrity strengthens security through decentralized and tamper-glaring ledgers, putting off unmarried points of failure and ensuring system robustness, even as the immutability of recorded records presents transparency and reliability.
3) Biometric safety features, especially behavioral biometrics, introduce customized access to manage layers by incorporating typing patterns and mouse moves, thereby contributing to greater protection and addressing future

threats with advanced cybersecurity measures.

4) Quantum Computing Countermeasures explore encryption techniques resilient to quantum threats, presenting important preemptive measures against the growing abilities of quantum computing.
5) Holistic Database Security integrates real-time adaptability through Dynamic Access Control Policies, allows collaborative and confidential computations with Secure Multi-Party Computation, proactively identifies protection threats with AI-pushed anomaly detection, and ensures privacy-maintaining machine mastering in dispensed databases through Federated Learning.
6) Cyber-Physical Database Security explores the intersection of cyber and physical threats, even as the Onion Model acts as a robust defense, mechanically erasing statistics in response to unauthorized entry attempts, enhancing normal security.
7) The complete approach outlined in the research empowers groups by providing holistic expertise in actual-time access manipulation, collaborative computations, and anomaly detection, contributing to advances in privacy-maintaining strategies tailor-made for evolving technological landscapes.
8) Organizations are suggested to enforce strong safety features by leveraging insights from the studies, incorporating technologies that include homomorphic encryption and blockchain for advanced information protection, addressing destiny threats through biometric and quantum-resistant measures, and adopting a holistic database protection approach to proactively mitigating ability risks.

CONCLUSION

In summary, this research advances the field of database security by embracing cutting-edge technologies and strategies to address present and future challenges. Homomorphic encryption emerges as a transformative solution, allowing secure computations on encrypted data within databases, ensuring privacy without compromising computational efficiency. The critical evaluation of blockchain for data integrity establishes its role in fostering trust and reliability through documented and tamper-evidence laws.

The integration of behavioral biomechanics introduces a personalized level of access control based on individual typing styles and muscle movements, enhancing security. The exploration of differential privacy strikes a nuanced balance between data utility and privacy in large-scale data sets during queries. Quantum computing counts anticipate future threats, evaluating encryption strategies resilient to quantum capabilities.

The paper encompasses various dimensions, including access control policies, secure multi-party computation, anomaly detection, forced learning, and cyber-physical database security, offering a holistic understanding. The proposed Onion model provides an additional layer of security by automatically erasing data in response to unauthorized access requests. Overall, organizations are encouraged to adopt these insights, embrace advanced technologies, and adopt a holistic security approach to fortify their databases against potential risks and ensure resilient data protection in the digital age.

References

[1] Prof.K.R.Ingole, Akshada Hage,Khushali V Dudhabade, Sakshi D Tayade, Radhika S Khewalkar, Supriya N Deshpande, "Database Security," *IJRASET,* vol. 11, 2023.

[2] Yesin, V.; Karpinski, M.; Yesina, M.; Vilihura, V.; Warwas, K., "Ensuring Data Integrity in Databases with the Universal Basis of Relations," *MDPI,* 2021.

[3] Alok Mishra, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, Asif Qumer Gill,, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Science Direct,* 2022.

[4] F. A. Iqra Basharat, "researchgate," May 2012. [Online]. Available: https://www.researchgate.net/publication/235992242_Database_Security_and_Encryption_A_Survey_Study.

[5] A. Mousa, M. Karabatak and T. Mustafa, "IEEE," IEEE, June 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9116436.

[6] Nagamani, Chippada,Suneetha Chittineni, "NETWORK DATABASE SECURITY WITH INTELLECTUAL ACCESS SUPERVISION USING OUTLIER DETECTION TECHNIQUES," sciencegate, 2022. [Online]. Available: https://www.sciencegate.app/document/10.1504/ijaip.2022.10042949.