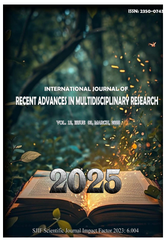
ISSN : 2350-0743

International Journal of Recent Advances in Multidisciplinary Research

Vol. 12, Issue 03 pp.10877-10881, March, 2025



RESEARCH ARTICLE

SECURE HEALTHCARE DATA RETRIEVAL FROM CLOUD STORAGE USING BLOWFISH DECRYPTION

Chaitanya Vasamsetty[1], Subramanyam Boyapati[2], Rajani Priya Nippatla[3], Sunil Kumar Alavilli[4], Bhavya Kadiyala[5] and Purandhar, N[6, *]

[1]Elevance Health, Georiga, USA; [2]American Express, Arizona, USA; [3]Kellton Technologies Inc, Texas, USA; [4]Sephora, California, USA; [5]Parkland Health, Texas, USA; [6]Assistant Professor, Department of CSE(Artificial Intelligence) School of Computers Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India

ARTICLE INFO

Article History

Received 19th December, 2024
Received in revised form
17th January, 2025
Accepted 26th February, 2025
Published online 28th March, 2025

Keywords:

Cloud Storage, Key Generation, Blowfish Decryption, Secure Data Retrieval, Threat Intelligence Platforms(TIPs), Data Masking.

Corresponding author:
Purandhar, N.

ABSTRACT

The advent of cloud computing in healthcare has made it possible for storage to become scalable and cost effective, which allows sensitive healthcare data to be accessed remotely and promotes collaboration among healthcare providers. The challenge in this data during the time of storage and retrieval will need to be secured and have privacy because it is at risk from cyber threats and unauthorized access existing solutions that do not protect healthcare data from vulnerabilities during decryption and usage.The study proposes developing a methodology for retrieving healthcare data from cloud storage for sensitive information. The system generates a key that will enable a decryption process by using the Blowfish algorithm in order to perform fast and secure decryption of healthcare data. Auditing and monitoring mechanisms are implemented to keep track of unauthorized activities while Threat Intelligence Platforms(TIPs) are used for detecting threats in real time. Further, sensitive information is protected from other forms of misappropriation through data masking. Thus, it suffices to say that all these components make secure handling of healthcare data in compliance with privacy regulation possible.The outcomes show that the key generation time increases linearly with the increase in prime sizes and varies from 200 ms for 0 bits to 1400 ms at 2000 bits. Similarly, the decryption times have risen with the rise of the number of files: the decryption time is 0.82 seconds for 0 files at one point, whereas, for 1000 files, it goes up to 9.33 seconds. There is a suitable match between the predicted CPU usage values and the actual observed values, and thus it confirms the efficiency of the system.This study provides secure methodologies for retrieving health care data from clouds using decryption, monitoring, and masking for sensitive information. This would add value by giving a framework for acquiring fairly secure health data from the cloud in a way that advances health data protection and minimizes vulnerabilities.

Citation: Chaitanya Vasamsetty, Subramanyam Boyapati, Rajani Priya Nippatla, Sunil Kumar Alavilli, Bhavya Kadiyala and Purandhar, N. 2025. *"*Secure Healthcare Data Retrieval from Cloud Storage Using Blowfish Decryption*", International Journal of Recent Advances in Multidisciplinary Research,* 12,(03), 10877-10881.

INTRODUCTION

The phenomena of data being stored, accessed, and processed in industrial sectors have fundamentally changed because of the rapid growth of cloud computing (Dondapati, 2019). Cloud technology provides cost-effective, scalable, and flexible access to enormous amounts of stored data in enabling organizations to gain access to their data from anywhere with internet connectivity (Allur, 2020). Its application has been utilized in all spheres of interest, with health care taking a significant focus since it is a sector that is always in need of secure and efficient data storage solutions (Deevi, 2020). Cloud computing in health care enables secure transmission, storage, and access sharing of sensitive patient information by the health care facility professionals with peer providers toward improving patient care (Allur, 2016). Digitization of medical records and the growth of Electronic Health Records (EHRs) in India have caused heavy accumulation of sensitive information(Dondapati, 2024). Thus, large quantities of sensitive data that must be stored and managed under strict security controls are being generated (Deevi, 2024). Patient's personal and sensitive information is meant to be confidential and, if exposed, could lead to serious breaches of privacy and legal issues(Deevi, 2021). Healthcare data needs to be encrypted and stored in a way that does not restrict utilization but denies access to unauthorized users (Allur *et al.*, 2025).

Additionally, reliance on analytics and telemedicine is proving to be a major driving force behind growing demands for highly reliable and secure data handling processes (Allur, 2020). The combination of cloud computing with health systems can bring about solutions to cater to the emergent needs for security and efficient data management (Kodadi, 2023). Security in vast amounts of health data can be ensured through cloud infrastructure for secure, scalable, and centralized storage where such data can be accessed by authorized healthcare professionals (Dondapati, 2020). However, it comes with the possible challenges of maintaining data security and privacy (Allur, 2020). It is flexible in the way the data found in the cloud is retrievable and processible, but strong encryption, decryption, and monitoring must be in place for protection and compliance with healthcare laws, mainly for example HIPAA (Deevi, 2023). Secure healthcare data retrieval from cloud storage, combined with advanced encryption techniques like Blowfish and modern monitoring systems, ensures that patient information remains confidential and accessible only to authorized individuals (Dondapati, 2020). Organization of this paper is as follows. Section 2 contains a literature review on securing healthcare data stored and retrieved from cloud environments. Section 3 describes the proposed methodology in detail, which includes processes for decryption of data, application of masking and establishing monitoring. Section 4 discusses the results, including performance metrics and security effectiveness, whereas Section 5 presents the conclusion.

LITERATURE SURVEY

In this study, the effects of cloud computing on management accounting practices of Small and Medium-Sized Enterprises (SMEs) are analysed. Content Analysis, Partial Least Squares Structural Equation Modelling (PLS-SEM), and Classification and Regression Trees (CART) are lightly mixed in assessing the role of cloud computing to improvement of financial data management, operational efficiency, and decision-making in (Deevi, 2020). The study, therefore, concludes that these cloud accounting solutions exhibit feasibility for real-time data access for compliance and strategic decision making. There is now a new hybrid approach which yields HGA-HPSO. Here, HGA is modifying the standard Genetic Algorithm using immune mechanism concepts to overcome premature convergence, while HPSO is combining some of the PSO with genetic operators to address ordering of jobs and production times (Deevi, 2024). Therefore, the hybridization seems to be efficient and cost-saving among the options.

The current project relates in some regard to the time series data on forecasting the manufacturing system, which experiences much of the associated difficulty with non-linearity and non-stationarity. Specifically, here, it hybridizes the temporal ARIMA linear model for time series with a non-linear Bi-directional GRU (Bi-GRU) model interested in error correction (Allur, 2021). Six real-world time series were used for experimentation, and hybridization between the two showed improvement with respect to all three-error metrics; thus, MSE, MAE, and MAPE. Hence, the proposed method is more accurate in enhancing the forecasting accuracy compared to others found in the literature. Case study of the Mayo and Cleveland clinic's stipulates that the threats and vulnerabilities will each be identified for ensuring data confidentiality through encryption and intrusion detection (Kodadi, 2021). Hence, data protection and compliance requirements are fulfilled along with the enhanced quality of services in patient care. The present paper brings in yet another hybrid approach to advance workload forecasting for intelligent cloud computing systems through Backpropagation neural network algorithm combined with game theory (Chetlapalli, 2023). Resource allocation and service delivery are guaranteed by mutual Service Level Agreements (SLAs) to cloud users and service providers at Nash equilibrium engendered through this approach. Real data experimentation has proved effectiveness in research to underpin cloud operation. This second phase of the study attempts to explore some of the high-end artificial intelligence underpinnings for fraud investigation in the IoT sector. The main distinguishing line is often modelled by supervised and unsupervised learning across historical transaction data with AI systems[20]. Major techniques, datasets, and evaluation metrics regarding adaptive learning will be covered in the study.

PROBLEM STATEMENT

Research existing and epitomising technologies for secure healthcare data retrieval from cloud storage have dealt with a number of problems (Chetlapalli, 2021). First, many studies have appealed to traditional encryption methods that are endangered by quantum attacks, making the sensitive data in health domains vulnerable (Kodadi, 2022). Next, the key management systems adopted are usually weak for cloud environments, allowing for data unauthorized decryption (Kodadi, 2020). Lastly, there is rarely an adequate monitoring and auditing system that can capture unauthorized access or tampering with sensitive data in real time, allowing someone to play havoc with potential security violations (Chetlapalli, 2021). These gaps stress the need for more robust integrated solutions, providing security as well as efficiency in healthcare data management.

METHODOLOGY

The process of securely retrieving healthcare data from cloud storage involves a series of interconnected steps as shown in Figure 1. The cloud storage of healthcare data contains an encrypted and secured environment. Afterwards, key generation is performed to allow for decryption the data in a secure manner, whereupon Blowfish algorithm is used to speed up the process while ensuring security. This is followed by an audit and monitoring mechanism whereby after decryption, any access to data is continuously tracked, and unauthorized activities can be detected. During sensitive data usage, data masking will protect the information from being exposed. Performance metrics will be observed to test the system's efficiency, whereas Threat Intelligence Platforms (TIPs) offer protection through real-time threat detection for possible vulnerabilities. Hence, an integrated approach guarantees secure handling of healthcare data following any of its retrieval processes.

Data Collection: The healthcare data is stored securely in the cloud terminal providing you with a scalable and efficient solution to data resources. The cloud storage offers that a large amount of sensitive healthcare data can be accessed and managed remotely with high availability. The cloud infrastructure allows strong security features such as encryption and access controls to secure the data from unauthorized access. Benefiting from cloud storage, healthcare organizations can economically store data, and in consequence flexibly access and process it. The cloud environment also fosters collaboration and data sharing between health providers in compliance with stringent data privacy laws.

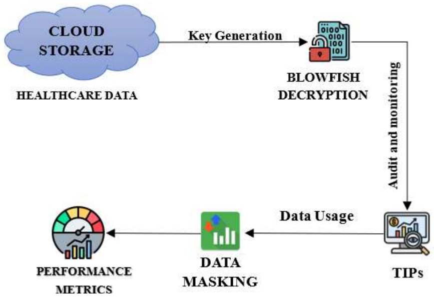


Figure 1. Secure Healthcare Data Retrieval Process from Cloud Storage

Key Generation: Key generation is essential for a very secure encryption and decryption of healthcare information. The strong algorithm used in this study is the most secure means through which encrypted data can be decrypted. The generated key material will be used to decrypt healthcare data stored in the cloud from which only authorized users can gain access to the private information. Adequate key management policies are put in place to ensure that generation keys are kept safe from misuse. Most importantly, it pertains to ensuring the integrity of the key generation process, thus the overall security of the system and, therefore, patient information.

Data Decryption: Data decryption is the technique of transforming health-related encrypted data into its original, readable format. Blowfish is within the study concerning decryption because it is faster coupled with its strong security features. Decryption occurs only after appropriate cryptographic key has been generated and verified because these are the steps involved in ensuring that sensitive and personal healthcare data remains under sealed access during retrieval by the authenticated users. That is why proper decryption mechanisms should always apply to try to maintain the confidentiality of data thus preventing unauthorized entry into patient is given in equation(1).

$$\boldsymbol{D(K,C) = P} \quad (1)$$

Were, D is the decryption function, K is the decryption key, C is the ciphertext, P is the plaintext.

Audit and Monitoring: Audit and monitoring will make healthcare data secure and ensure its integrity. In this study, monitoring systems were put in place to track all accesses to this healthcare data, directly recognizing any unauthorized access or suspicious behaviours. Audit is mathematically represented in equation(2).

$$A = \{(u_i, a_t) \mid u_i \in U, a_t \in A_t\} \quad (2)$$

Were, A is the audit log, u_i is the user accessing the data, a_t is the action taken at time t, A_t is the set of actions at time t, U is the set of all users.

Threat Intelligence Platforms(TIPs): Threat Intelligence Platforms(TIPs) have become a cornerstone in securing healthcare data by way of real-time assessment of threats and possible vulnerabilities. TIPs provide good collation, aggregation, and analysis of threat data to identify forthcoming threats and their patterns to prevent a security breach from happening. The efficacy of TIPs is given in equation(3).

$$T = f(D, V, R) \quad (3)$$

Were, □ represents the threat intelligence output, □ is the data collected from various sources, □ is the vulnerability data, □ is the risk assessment derived from the analyzed threat data.

Data Usage: Data usage is how decrypted health care data are accessed and utilized by authorized users. The use of data becomes open for analysis, decision-making, and other health-related purposes within the limits of maintaining patient confidentiality once the data have been securely decrypted. In turn, data is masked during that process to prevent accidental exposure of sensitive information. It is only for those who have the right to use it legitimately. The process is also very much tight in terms of enforcing stringent controls to access the data and governance policies, concerning the data's security and compliance to healthcare regulations being followed.

Data Masking: Masks data are an essential technique to keep the sensitive healthcare information obfuscated at the time of usage. It makes sure that only an authorized user would be able to look at the full details. For this research, data masking will replace real data with fictitious but realistic values, thus the data could be utilized without revealing private details for any kind of analysis or testing. Keeping the data private and compliant with data privacy regulations will, however, still preserve the integrity of the data for legitimate purposes. Masked data allow sharing and processing with minimum unauthorized access to confidential patient information. Data masking is a great protector of the breach and lets one analyses the data with a click.

RESULTS

The outcome of this research shows that the method proposed for securely retrieving healthcare data from the cloud storage is quite effective. The metrics for performance maintained that the key generation and decryption scheme are efficient, with Blowfish encryption allowing fast and secure data retrieval. Further--by comparing actual CPU usage to its prediction--we were able to demonstrate that the system works very efficiently with minimal variations between predicted and actual resource usage. These findings attest to the strength of the practical implementation of the integrated security approach.

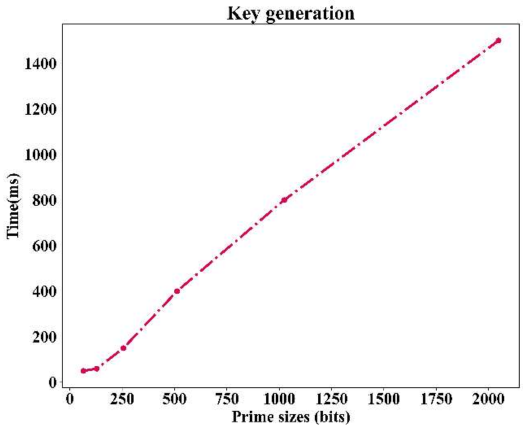


Figure 2. Key Generation

Figure 2 depicts the association between prime sizes and the time required for key generation. As it shows an almost linear rise in time with the increase in prime size, it mentions that the time increases in almost a straight line with the increase in prime size. For instance, the prime size is 0 bits, and the key generation time computes at about 200 ms, while for a prime size of 2000 bits, the time reaches about 1400 ms. Thus, larger prime sizes have longer key generation times, making it evident that more time is required for an operation that is very complex in terms of the computations involved in making this secure process work.

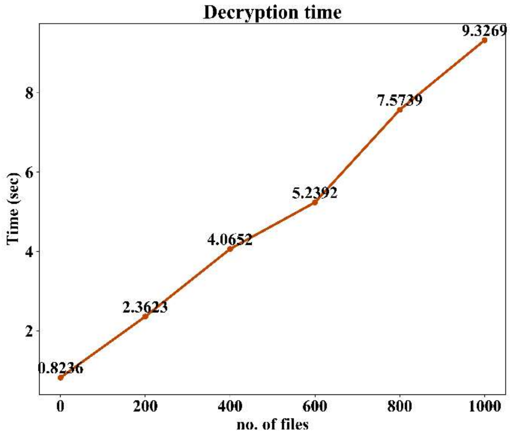


Figure 3. Decryption Time

The relationship is represented in Figure 3 in terms of the number of files and the decryption time in seconds. In general, as the number of files increases, there is a nearly linear increase in the amount of time it takes to decrypt them. As an example, it takes approximately 0.82 seconds to decrypt 0 files, while for 200 files, it takes 2.36 seconds. This process lasts around 5.24 seconds with about 600 files and takes 9.33 seconds for 1000 files. Thus, it is evident that the more the amount of data that increases over time, the more time it requires for decryption due to the increased number of files going through the process.

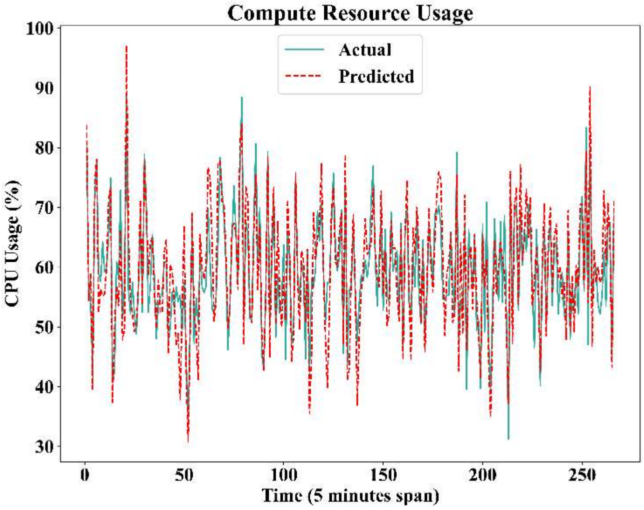


Figure 4. Compute Resource Usage

Figure 4 illustrates the differential depiction of actual yet predicted CPU usage over time in 5-minute intervals. The solid cyan line denotes actual CPU consumption in real-time, and the red dash dotted line represents predicted CPU usage. There lies a comparable fluctuation between these two lines, which, in closer terms, can be said to state that the predicted CPU usage follows very close values to real just like, for example: time '0', when actual CPU usage is about 60% and predicted is just slightly above it at 65%. This is consistently the trend throughout the graph, thus proving that the model for prediction has been aptly accurate in catching the current use of CPU.

CONCLUSION

The study illustrates the secure approach of retrieving healthcare data from cloud storage, using encryption and decryption techniques. The result indicates that Blowfish can be considered an efficient algorithm for key generation and decryption processes, where key generation time almost linearly increases with prime size. In contrast, decryption time shows almost a linear ascent with respect to the number of files, from 0.82 seconds for the occasion of having zero files to 9.33 seconds for 1000 files. CPU usage analysis, however, corroborated the estimated resource usage and actual resource utilization; hence we can safely say that the resource management of the system is indeed efficient. All in all, these findings provide very substantial support for the effectiveness of our proposed security parameters. Future improvements will include a more robust machine-learning modelling for resource optimization, and research into quantum-resistant encryption protocols will certainly enhance flexibility and scalability of the system.

REFERENCES

Dondapati, K. 2019. “Lung’s cancer prediction using deep learning,” International Journal of HRM and Organizational Behavior, Vol. 7, No. 1, pp. 1–10, Jan.

Allur, N. S. 2020. “Enhanced Performance Management in Mobile Networks: A Big Data Framework Incorporating DBSCAN Speed Anomaly Detection and CCR Efficiency Assessment,” Journal of Current Science, 8(4)..

Deevi, D. P. 2020. “Real-time malware detection via adaptive gradient support vector regression combined with LSTM and hidden Markov models,” Journal of Science & Technology(JST), Vol. 5, No. 4, Art. no. 4, Aug.

Allur, N. S. 2019. “Genetic Algorithms for Superior Program Path Coverage in software testing related to Big Data,” Vol. 7, No. 4.

Dondapati, K. 2024. “Leveraging Backpropagation Neural Networks and Generative Adversarial Networks to Enhance Channel State Information Synthesis in Millimetre Wave Networks,” Oct., doi: 10.5281/ZENODO.13994672.

Deevi, D. P. 2024. “Developing an integrated machine learning framework for improved brain tumor identification in MRI scans,” Current Science.

Deevi, D. P. N. S. Allur, K. Dondapati, H. Chetlapalli, S. Kodadi, and L. A. Ajao, 2021. “AI-Integrated Probabilistic Neuro-Fuzzy TemporalFusionNet for Robotic IoMT Automation in Chronic Kidney Disease Detection and Prediction,” Jun., [Online]. Available: https://ieeexplore.ieee.org/document/10895279.

Allur, N. S. D. P. Deevi, K. Dondapati, H. Chetlapalli, S. Kodadi, and T. Perumal, 2025. “Role of knowledge management in the development of effective strategic business planning for organizations,” Comput. Math. Organ. Theory, Jan., doi: 10.1007/s10588-025-09397-2.

Allur N. S. and W. Victoria, 2020. "Big Data-Driven Agricultural Supply Chain Management: Trustworthy Scheduling Optimization with DSS and MILP Techniques," Current Science.

Kodadi, S. 2023. "Integrating Blockchain with Database Management Systems for Secure Accounting in the Financial and Banking Sectors," Journal of Science & Technology(JST), Vol. 8, No. 9, Art. no. 9, Sep.

Dondapati, K. 2020. "Integrating neural networks and heuristic methods in test case prioritization: A machine learning perspective," International Journal of Engineering, Vol. 10, No. 3, Sep.

Allur, N. S. 2020. "Phishing website detection based on multidimensional features driven by deep learning: Integrating stacked autoencoder and SVM," Journal of Science & Technology(JST), Vol. 5, No. 6, Art. no. 6, Dec.

Deevi, D. P. 2023. "Continuous resilience testing in AWS environments with advanced fault injection techniques," Vol. 11, No. 1.

Dondapati, K. 2020. "Robust software testing for distributed systems using cloud infrastructure, automated fault injection, and XML scenarios," Vol. 8, No. 2.

Deevi, D. P. 2020. "Improving patient data security and privacy in mobile health care: A structure employing WBANs, multi-biometric key creation, and dynamic metadata rebuilding," International Journal of Engineering Research and Science & Technology, Vol. 16, No. 4, pp. 21–31, Dec.

Deevi, D. P. N. S. Allur, K. Dondapati, H. Chetlapalli, S. Kodadi, and T. Perumal, 2024. "The impact of the digital economy on industrial structure upgrading and sustainable entrepreneurial growth," Electron. Commer. Res., Sep., doi: 10.1007/s10660-024-09907-5.

Allur, N. S. 2021. "Optimizing cloud data center resource allocation with a new load-balancing approach," Vol. 9, No. 2.

Kodadi, S. 2021. "Optimizing software development in the cloud: Formal QoS and deployment verification using probabilistic methods," [Online]. Available: https://jcsonline.in/admin/uploads/Optimizing%20Software%20Development%20in%20the%20Cloud%20Formal%20QoS%20and%20Deployment%20Verification%20Using%20Probabilistic%20Methods.pdf.

Chetlapalli, H. 2023. "Enhanced post-marketing surveillance of AI software as a medical device: Combining risk-based methods with active clinical follow-up," Jun.

Deevi, D. P. 2020. "Artificial neural network enhanced real-time simulation of electric traction systems incorporating electro-thermal inverter models and FEA," International Journal of Engineering, Vol. 10, No. 3, Sep.

Chetlapalli, H. 2021. "Novel cloud computing algorithms: Improving security and minimizing privacy risks," Journal of Science & Technology(JST), Vol. 6, No. 2, Art. no. 2, Mar.

Kodadi, S. 2022. "High-performance cloud computing and data analysis methods in the development of earthquake emergency command infrastructures," Vol. 10, No. 9726.

Kodadi, S. 2020. "Advanced data analytics in cloud computing: Integrating immune cloning algorithm with D-TM for threat mitigation," International Journal of Engineering Research and Science & Technology, Vol. 16, No. 2, pp. 30–42, Jun.

Chetlapalli, H. 2021. "Enhancing test generation through pre-trained language models and evolutionary algorithms: An empirical study," Jun.

Kodadi, S. 2024, "Integrating statistical analysis and data analytics in e-learning apps: Improving learning patterns and security," Oct., doi: 10.5281/ZENODO.13994651.

Kodadi, S. 2022, "Big data analytics and innovation in e-commerce: Current insights, future directions, and a bottom-up approach to product mapping using TF-IDF," International Journal of Information Technology and Computer Engineering, Vol. 10, No. 2, pp. 110–123, May.

Chetlapalli H. and T. Perumal, 2024, "Driving business intelligence transformation through AI and data analytics: A comprehensive framework," Current Science.

"Synthetic log data of distributed system," 2025, [Online]. Available: https://www.kaggle.com/datasets/ shubhampatil 1999/ synthetic-log-data-of-distributed-system

****