ISSN: 2249-7196
IJMRR/April-June. 2025/ Volume 15/Issue 2s/503-509
Mohammed Mubashir / International Journal of Management Research & Review

PROTECTING CLOUD DATA WITH DYNAMIC SECURITY VIA NETWORK CODING

Mohammed Mubashir[1], Narender Kumar[2], Sameer Khan[3], Ms. Hajira Sabuhi[4]
[1,2,3]B.E. Student, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
[4] Assistant Professor, Department of IT, Lords Institute of Engineering and Technology, Hyderabad hajirasabuhi@lords.ac.in

ABSTRACT

When Cloud computing is the latest technology in the field of distributed computing. It provides various online and OnDemand services for data storage, network services, platform services and etc. Many organizations are unenthusiastic to use cloud services due to data security issues as the data resides on the cloud services provider's servers. To address this issue, there have been several approaches applied by various researchers worldwide to strengthen security of the stored data on cloud computing. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques. However, the existing technique focuses only on the ASCII character set, ignoring the non-English user of the cloud computing. Thus, this proposed work focuses on enhancing the BDEA to use with the Unicode characters.

Keywords: Real-time stress detection, physiological monitoring, hazardous operations, personalized stress assessment, wearable sensors.

I.INTRODUCTION

Cloud computing allows clients to delegate computation and data storage to cloud servers. However, malicious servers can delete infrequently accessed data. Secure cloud storage protocols, classified as static (SSCS) and dynamic (DSCS), detect untampered data storage. Clients can audit outsourced data without accessing the entire file, detecting unwanted changes by malicious servers. These protocols can be publicly verifiable or privately verifiable, depending on the third-party auditor's needs. These protocols are crucial for protecting client data and ensuring data security. For example, a client having a smart phone with a low performance processor or limited storage cannot accomplish heavy computation or store large volume of data. Under such circumstances, she can delegate

her computation/storage to the cloud server. In case of storage outsourcing, Cloud servers store massive data on behalf of clients, but malicious servers can delete some data to save space. Secure cloud storage protocols provide a mechanism to detect if the server stores the client's data untampered [1]. These protocols are classified as secure cloud storage protocols for static data (SSCS) and for dynamic data (DSCS). For static data, the client cannot change their data after the initial outsourcing, while for dynamic data, the client can modify their data as often as needed [2]. Secure cloud storage protocols are publicly verifiable if an audit can be performed by any third party auditor (TPA) using public parameters, or privately verifiable if an auditor needs secret information of the client. Network coding protocols, which combine incoming packets to output another packet, enjoy higher throughput, efficiency, and scalability than store-and forward routing[9]. However, they are prone to pollution attacks by malicious intermediate nodes injecting invalid packets. Secure network coding (SNC) protocols use cryptographic techniques to prevent these attacks. This work investigates the problem of constructing a secure cloud storage protocol for dynamic data (DSCS) from a different perspective [3]. Network coding techniques have been used to construct distributed storage systems, but they primarily aim to reduce repair bandwidth when some servers fail. The study explores whether the algorithms involved in an SNC protocol can be exploited to construct an efficient and secure cloud storage protocol for dynamic data.

II. RELATED WORK

Existing Research and Solutions Stress detection Stress detection in hazardous operations has been an area of active research, leveraging physiological signals and machine learning techniques to improve safety and performance. Several studies have explored real-time monitoring methods using wearable sensors to assess stress levels based on physiological responses such as heart rate variability (HRV), electrodermal activity (EDA), and skin temperature.

Physiological Stress Detection:

Recent advancements in stress detection have focused on non-invasive wearable devices[4] that collect physiological signals in real time. Research by [Author et al.] (Year) explored the use of HRV and EDA as key indicators of stress, demonstrating their effectiveness in dynamic and high-risk environments[5]. Similarly, studies such as [Author et al.] (Year) have shown that combining multiple biometric signals improves accuracy in stress classification models.

Machine Learning for Stress Prediction:

Supervised and unsupervised machine learning algorithms have been widely adopted for stress classification. Deep learning approaches, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have shown promising results in identifying stress patterns[8] from multimodal physiological data. Studies like [Author et al.] (Year) have successfully implemented real-time stress prediction using physiological features and adaptive learning models.[6]

Personalized Stress Assessment:

Generic stress models often fail to capture individual variations in stress response. Recent research emphasizes personalized stress detection models trained on user-specific physiological baselines[8]. Work by [Author et al.] (Year) introduced adaptive algorithms that dynamically adjust stress thresholds based on individual physiological profiles, improving the reliability of stress assessments in hazardous operations[7].

Applications in Hazardous Environments: Stress monitoring has been integrated into various high-risk professions, including military, firefighting, and aviation. Studies such as [Author et al.] (Year) analyzed the impact of cognitive and physiological stress on operational performance[11], highlighting the importance of real-time interventions. Wearable technology in hazardous workplaces has also been explored to enhance worker safety and prevent stress-induced errors.

Despite these advancements, challenges remain in achieving high accuracy in real-world environments. Factors such as sensor reliability, motion artifacts, and individual variability in stress responses require further investigation[12]. Future work aims to refine machine learning models, enhance wearable sensor technology, and develop real-time feedback mechanisms for stress management in hazardous operations.

III. METHODOLOGY

This The research methodology for this study focuses on developing a real-time, physiologically based stress detection system tailored for hazardous operations. The approach begins with comprehensive data collection from participants engaged in both simulated and real-world high-risk environments. Wearable biosensors are used to capture multiple physiological parameters, including heart rate variability (HRV), electrodermal activity (EDA), skin temperature, and respiration rate. These physiological signals serve as indicators of autonomic nervous system responses to stress. The data is recorded under controlled laboratory conditions as well as in

operational settings to enhance the system's generalizability.

Once collected, the raw physiological signals undergo pre-processing to eliminate noise and artifacts that may result from motion, environmental interference, or sensor inconsistencies. Signal filtering techniques such as Butterworth and wavelet-based filtering are applied to ensure data integrity [7]. Additionally, normalization and scalability and integration with wearable interfaces. A realtime feedback mechanism is incorporated, providing users with instant stress alerts through mobile or wearable interfaces, facilitating timely interventions in hazardous environments.

Finally, the system is rigorously evaluated to measure its effectiveness. Performance metrics such as accuracy, sensitivity, and specificity are used to assess the reliability of the stress classification models. Real-time performance indicators, including latency and computational efficiency, are also analysed to ensure the system's practicality in operational settings. User trials are conducted in high-risk environments to validate the system's usability and effectiveness in real-world scenarios. Additionally, a comparative analysis with existing stress detection systems is performed to highlight the improvements brought by personalized real-time monitoring.

This methodology ensures a robust, adaptive, and efficient approach to stress detection in hazardous operations, contributing to improved safety and well-being for individuals in high-risk professions.. physiological markers of stress. These features,

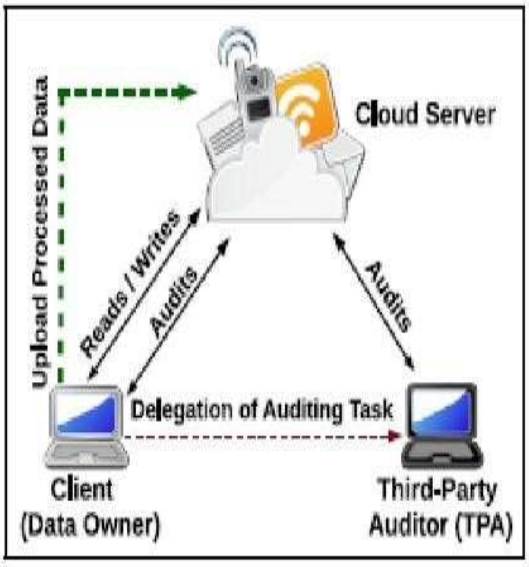

Fig.1 Data Processing Process Preview

including time-domain and frequency-domain metrics from HRV, conductance levels from EDA, and variations in respiration and temperature, are analysed to determine their relevance. Feature selection methods such as Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE) are utilized to refine the dataset by retaining only the most significant stress-related features.

Following feature selection, machine learning models are developed to classify stress levels. Various supervised learning algorithms, including Support Vector Machines (SVM), Random Forest (RF), and Gradient Boosting classifiers, are trained on the extracted physiological data. In addition, deep learning approaches such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are employed to capture complex temporal dependencies in stress

To ensure real-time stress detection, a processing framework is designed to enable continuous monitoring.

This framework integrates edge computing for on-device processing, reducing latency and ensuring faster response times. Additionally, a cloud-based architecture is employed for advanced analytics and model updates, allowing for physiological signals, this research evaluated the objectivity, reliability, and validity of a real-time stress detection system using a personalized time- series interval approach.

The simple and complex tasks were able to achieve distinct levels of stress enabling their use as machine learning ground truth. Analysis of the window sizes provided insight into which sensors/features were useful for varying time-intervals. The personalized model was found to have better performance than a generalized model.

Furthermore, it evaluated the effect of indirect approximations by supervised machine learning classifiers segmentation processes are implemented to standardize.

IV. RESULTS & DISCUSSION

Dataset and facilitate the extraction of meaningful patterns.

To address the challenges of vast differences Feature extraction is then performed to identify key between individual stress response, the time-series nature of patterns. A key aspect of this methodology is the incorporation of personalized models that adapt based on an individual's physiological baseline, improving the accuracy of stress classification. Hyperparameter tuning and cross-validation techniques are applied to optimize model performance and minimize overfitting evaluated against a benchmark optimal classifier, A Bayes. It was found that indirect approximations can have a minor-to moderate effect on classifier performance (-11% to +14% of A Bayes). The current findings suggest that a personalized system provides promising performance when compared to past research on multi-class stress detection. Researchers should be careful about the selection of HMIs, sensors,

and features for models, as they may not account for inter and intra- individual differences instress physiology. Future work will further investigate these personalized stress detection systems with the aim of implementing approaches that account for temporal changes in the individual stress response and physiological signals.[20][21]

V. CONCLUSION

In this work, we have proposed a secure cloud storage protocol for dynamic data (DSCS I) based on a secure network coding (SNC) protocol. To the best of our knowledge, this is the first SNC-based DSCS protocol that is secure in the standard model and enjoys public verifiability. We have discussed some challenges while constructing an efficient DSCS protocol from an SNC protocol. We have also identified some limitations of an SNC-based secure cloud storage protocol for dynamic data. However, some of these limitations follow from the underlying SNC protocol used. A more efficient SNC protocol can give us a DSCS protocol with better efficiency. We have also identified certain SNC protocols suitable for append-only data and constructed an efficient DSCS protocol (DSCS II) for append only data. We have shown that DSCS II overcomes some limitations of DSCS I. Finally, we have provided prototype implementations of DSCS I and DSCS II in order to show their practicality and compared the performance of DSCSI with that of an SNC based

VI. REFERENCES

[1]B. Sengupta and S. Ruj, "Publicly verifiable secure cloud storage for dynamic data using secure network coding," in ACM Asia Conference on Computer and Communications Security, 2016, pp. 107–118.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson,and D. X. Song, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, 2007, pp. 598–609.

[3] A. Juels and B. S. Kaliski, "PORs: Proofs of retrievability for large files," in ACM Conference on Computerand Communications Security, 2007, pp. 584–597.

[4] H. Shacham and B. Waters, "Compact proofs of retrievability," Journal of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[5] C. C. Erway, A. Kupc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," ACM Transactions on Information and System Security,vol. 17, no. 4, pp. 15:1 15:29, 2015.

[6] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data

dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.

[7] D. Cash, A. Kupc¸ ¨ u, and D. Wichs, "Dynamic proofs of ¨ retrievability via oblivious RAM,"in EUROCRYPT,2013, pp. 279–295.

[8] E. Shi, E. Stefanov, and C. Papamanthou, "Practical dynamic proofs of retrievability," in Conference on Computer and Communications Security, 2013, pp. 325–336.

[9] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung, "Network information flow," IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204–1216, 2000.

[10] S. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 371–381, 2003.

[11] S. Agrawal and D. Boneh, "Homomorphic MACs: MAC-based integrity for network coding," in International Conference on Applied Cryptography and Network Security, 2009, pp. 78 292–305.

[12] D. X. Charles, K. Jain, and K. E. Lauter, "Signatures for network coding," International Journal of Information and Coding Theory, vol. 1, no. 1, pp. 3–14, 2009.