International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

A User-Centric Data Protection Method for Cloud Storage Based on Invertible DWT

Dr. P. M. Joe Prathap, M. Kushmitha, R. Subhasree, V. Sruthi

Department of Information Technology, RMD Engineering College, Chennai, India

ABSTRACT: Distributed registrations based on cases and desired cases are considered to be the things handed over by royalty organizations. Re-integration of both approaches can be an additional cost when resources are hired from the cloud. However, it is also an important test for selecting the right amount of captured resources and demanding customer service. In this paper, the issue of performance reservation with both managed and demand models is considered. The main objective is to apply the rental cost under the due date reduction. In this paper an opinion on the matter is presented mathematically. A separate high-speed and time-consuming development process is proposed to compile workflow plans. Four exciting theories are used to create incorrect cycle schemes. The type and estimate of benefits are resolved by the time-based schedule of the class that is part of the development. New groups are created with a different neighbour search strategy. Experiments, actual experiments, and results indicate that this proposed production can be a significant cost savings when coming from measure ements with demand models or database models.

KEYWORDS: Selected encryption, security cloud storage, GPU, DWT, security analysis.

I. INTRODUCTION

The development of computer and cloud computing technology has set a trend in recent years for the outsourcing of information storage and processing of cloud-based services. Nowadays, cloud-based services for individual end users are gaining popularity especially for data storage. By relying on large storage space and reliable communication channels, cloud-based service providers such as Dropbox, Google Drive, or Amazon Drive to name just a few, are providing nearly infinite and low-cost storage space to individual users. This situation brings into question the reliability of cloud service providers. Many data security and privacy incidents are seen in today's cloud services. On the other hand, cloud service providers deal with a large number of external attacks. For example, in 2018, a total of 1.5 million Sing Health path non-medical personal data were stolen from the health system in Singapore. In some other cases, cloud service providers may not be fully trusted. Personal data can be used in malicious ways such as Facebook and the Cambridge Analytical data scandal in which 87 million users were affected in 2018. Thus, it becomes necessary for end-users to efficiently protect their data such as text, images, or videos independently. From cloud service providers. A reasonable solution is to protect data on secure end-user machines before outsourcing to clouds that naturally become traditional ciphers such as AES. However, the encryption algorithm is transferring security over data that provides security over keys which, in turn, introduces key management problems. Once the key is exposed, data security will be threatened. In Worst case, if the end users have no cryptographic practice and try to reuse the same key for different data protection; A major exposure will give rise to a large range of data leakage. Thus, other than ciphers, other data protection schemes are necessary to support such scenarios

II. RELATED WORKS

There are some new criteria that can also be used to compare our results with existing ones. The two most commonly used criteria for multimedia SE methods are shown as histogram analysis and correlation analysis. However, the criteria for evaluation of data security methods should be extended according to practical use cases, such as secure data storage from end users to the clouds described in this paper. For example, execution speed should be measured on practical hardware platforms and compared with the encryption algorithm [(Ie) AES-128 in this paper]. The safety level should also be evaluated according to the design objective. Data integrity is a fundamental requirement for realizing formatagnostic and it is also important to be evaluated. In the case of secure data storage of end users for cloud users, consideration of storage allocation optimization and resistance to error propagation is also necessary. To evaluate execution speed, it is important to first consider whether the design level has additional pre-processing steps such as the DCT process. For this method, pre-processing steps based only on DCT are slower than using AES on the entire data found on a modern CPU, taking into account performance issues. Such a problem is always ignored by the transformation based SE method. In our method, we use GPGPUs to speed up the computation tasks and execution time is evaluated to prove efficiency when comparing with the AES or AES-NI algorithm. In this paper, a method called in-depth security analysis is performed to prove whether a high security level is achieved with the protection of both private pieces and public pieces.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

III.LITERATURE SURVEY

KKGai (2017) had introduced a rapidly emerging technology, smart grid network (SGN) has been dramatically accepted by the current power supply industry to achieve high performance power governance systems. Wireless SGNs (WSGNs) have enabled a number of flexible power management solutions without the restrictions of wired infrastructure. Cognitive radio network (CRN) is one of the widely deployed wireless networking approaches. Communication security is a major concern when using CRN in WSGNs. Currently, jamming and spoofing are two common attack approaches that are active in the deployment of WSGN when using CRNG. This paper proposes an attack strategy that maximizes an attack strategy using spoofing and jamming (MASS-SJ) methods, which uses an optimal power distribution to maximize adverse effects. Spoofing and jamming attacks are launched in a dynamic manner to interfere with the maximum number of signal channels. Our proposed approach has been evaluated by our experiments and the results have shown positive performance using MAS-SJ.

KK Gai (2016) had implemented a cloud computing empowers multiple paths for web-based computing service offerings to meet a variety of needs. However, privacy information security has also become an important issue in cloud data security to restrict cloud applications. One of the major concerns in security is that cloud operators will have a chance to access sensitive data, which dramatically increases users' concern and the ability to adopt cloud computing in many areas such as the financial industry and government agencies Reduces to. This paper focuses on this issues and proposes a novel approach that can efficiently split a file and store data in a distributed cloud server, with data not directly accessible by cloud service operators. The proposed scheme is entitled as Security-aware Efficient Distributed Storage (SAEDS) model, which is mainly supported by the proposed algorithm, as Secure Efficient Data Distribution (SED2) algorithm and Efficient Data Configuration (EDCon) algorithm. Has been named. Our experimental evaluation has assessed both safety and efficiency performance.

Xiangong (2014) had designed high-performance interconnection between a host processor and an FPGA accelerator is high in demand. Between the various interconnection methods, a PCIe bus is an attractive alternative to a loosely coupled accelerator. Because there is no standard host-FPGA communication library, FPGA developers must write significant amounts of PCIe related code on both the FPGA side and the host processor side. A high-performance host-FPGA PCIe communication library is critical to broaden the use of the FPGA accelerator. The main goal in this paper is on efficiency and flexibility as they are two important features in a library. Let us discuss the challenges that these facilities are providing, and present our solutions to these challenges. We propose EPEE, an efficient and flexible host-FPGA PCIe communication library and describe its design. We implemented EPEE in different generations of Xilinx FPGAs in PCIe Gen2 X8 mode with 26.24 Gbps half-duplex and 43.02 Gbps full-duplex total throughput; These are at the best usage level that a host-FPGA PCI library can achieve. The EPEE library is integrated into four different FPGA applications with different data usage patterns in different institutions.

Dongjinhuang (2016) had introduced a new contrast media diffusion simulation algorithm is proposed to reduce invasive convective interference. On the basis of smoothed particle hydrodynamics (SPH), the algorithm can be mainly divided into two parts such as fluid – fluid interaction and fluid – solid interaction. In fluid – fluid interactions, an absorption model of iodine particles is built, and adjacent bloodstream particles moving around can be quickly obtained by Eulerian grids and space sparse hashes. In fluid – solid interactions, the couplar friction friction model is used to realize the frictionless contact between the fluid particles and the internal walls of the vessel. To improve computational speed, the algorithm uses multi-thread parallel technology to solve the complex diffusion problem of contrast media on Computer Unified Device Architecture (CUDA). Experimental results suggest that this algorithm is feasible, and may enhance the effect of developing blood vessels with real-time performance, particularly for capillaries.

IV. EXISTING SYSTEM

A reasonable solution is to protect data on a secure end-user's machine before outsourcing it to clouds, which naturally become traditional ciphers such as AES. However, encryption algorithms are transferring security over data providing security for keys which in turn introduce some new keys. Selective encryption method is a new trend in image and video content security. It is used only to encrypt subsets of data. The main objective of this selective encryption method is to reduce the amount of data to be encrypted while preserving a sufficient level of security.

V. PROPOSED SYSTEM

The proposed methodology is demonstrated to establish its level of safety. The private piece of a data chunk must be securely protected. We assume that it is encrypted with AES128, but can be replaced by other encryption algorithms as a form of flexibility. AES (Advanced Encryption Standard). Encryption system supported by the Enconol Institute of

Standards and Technology (NIST). AES is a cryptographic cipher that uses a block length of 128 bits and a key length of 128, 192 or 256 bits.

The proposed system has three module are listed below:

1. Use the user interface
2. File UPLOAD
3. Additional data in public and private clouds

Use the user interface:
This is the basic module of our project. The required part for the client is to move the login window into the information proprietor window. This module is primarily designed to provide security reasons. In this login page we have to enter client id and secret key. It will check if the username and puzzle word is orchestra (generous customer ID and true blue watchword). In the event that we enter any invalid username or puzzle word, we cannot go into the login window in the client window, it will show the screw up message. So we are preventing unauthorized clients from going from login window to client window. All this will not be a terrible security for our security process. So the server has a client ID and a secret key. The server also checks the client's confirmation. This will redesign the security and go into the structure preventing the proprietor without notice. In our venture we are using SWING to create game plans. Here we support login client and server confirmation.

File Upload:
The user will log into their account and upload a file or image, and that files / image can be encrypted and stored on the admin side. Even the uploaded user cannot submit the file without obtaining permission from the administrator.

Additional data in public and private clouds:
In this part the uploaded file stores more than two clouds, they are public CLOUDS and private CLOUDS. Here the files will be split and then stored under public and private clouds. In public clouds, we can show the file that we have already uploaded, but in private clouds, we cannot access the file, because that uploaded file will be encrypted in private

VII. ARCHITECTURE DIAGRAM

A system architecture is a conceptual model used to define the structure, behaviour, and more considerations of a system. An architectural statement is a formal description and representation of a system, organized in a way that supports arguments about the system's structures and behaviours. A system architecture may also include the development of system components and sub-components of the system and it will work together to implement the overall system. There have been several attempts to formalize languages to describe system architecture and are collectively called architecture description languages.

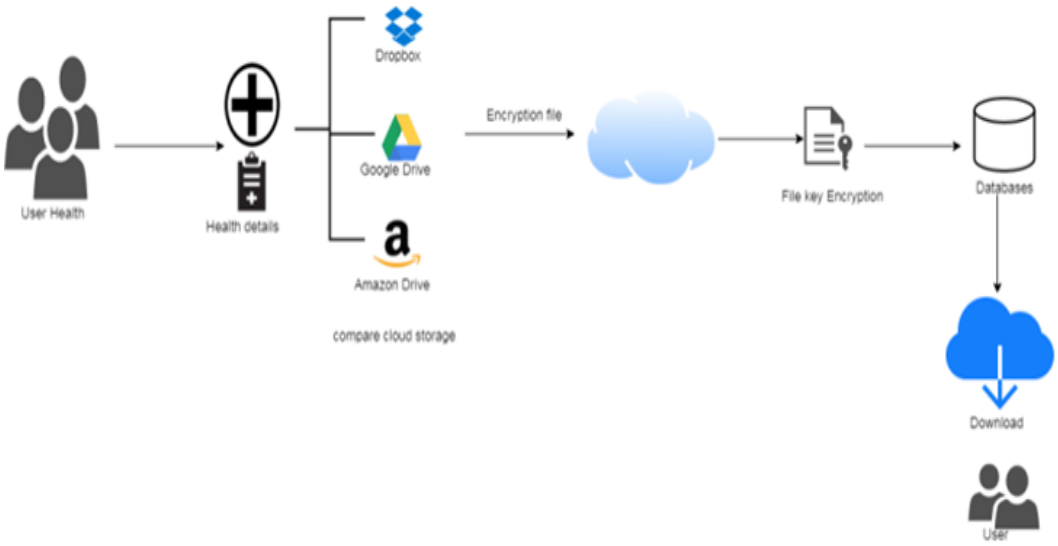

Fig 1: Architectural Diagram

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

VIII. EXPERIMENTALANALYSIS

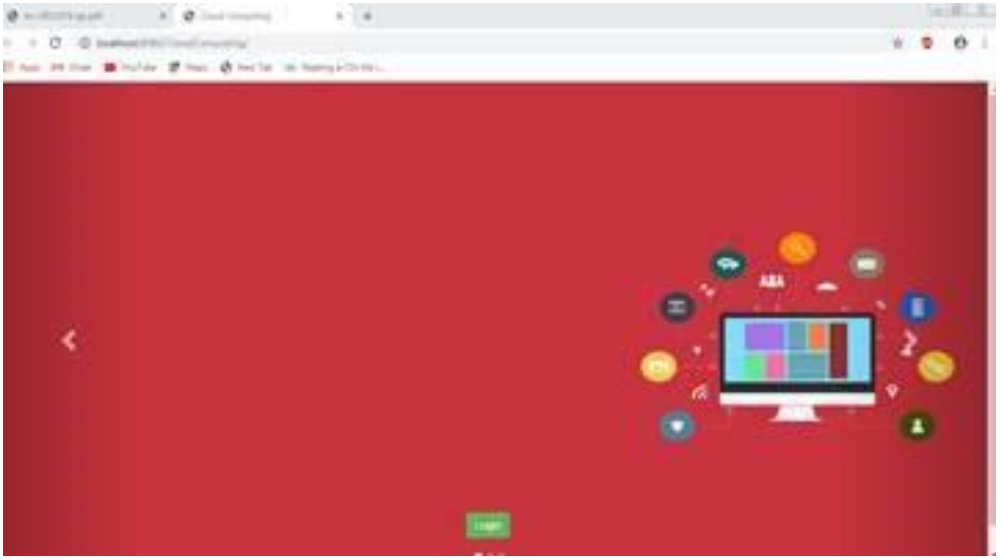

Fig 2: User Interface Diagram

Fig 3: User Register Form

Fig 4: Login Form

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

Fig 5: Data Request

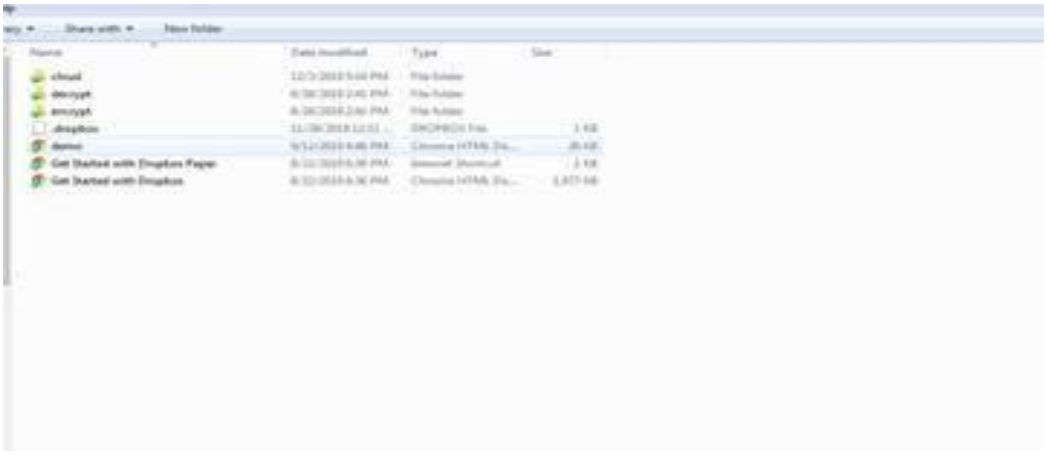

Fig 6: File Accept

Fig 7: Cloud Storage

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

IX. FUTURE EXPANSION

We know that encryption was a shared key and symmetric stuff; But we have no idea how it works. So this limits practical applications. However, the encryption that is built on machine learning is quite impressive which makes us wonder where encryption might go in the future. As our technology furthers our ability to encrypt data with neural networks, it is now able to learn how to protect data. With much innovation at our fingertips, Davey Winder figured out where encryption could go in the future.

X. CONCLUSION

In this paper, we have proposed a solution for end users to use cheap cloud storage services and secure their data. Our method can be applied to many different data formats that significantly improved the concept of selective encryption by introducing methods of fragmentation and dispersion. Experimental and theoretical results have verified that our method can provide a high degree of protection with resistance against propagation errors. We also provided rapid runtime on various PC platforms with practical design and implementation based on GPGPU acceleration. In summary, we proposed a safe and efficient data protection method for end users to safely store data on clouds.

REFERENCES

[1] F. Hu, M. Qiu, J. Li., T. Grant, d. Taylor, S. McCaleb, L. Butler, and R. Heimner, "A Review on Cloud Computing: Design Challenges in Architecture and Security," Journal of Computing and Information Technology, Vol. 19, No. 1, pp. 25-55, 2011

[2] H. Lee, K. Ota, and M. Dong, "Virtual network recognition and optimization in SDN-enabled cloud environments," IEEE Transactions on Cloud Computing, 201 Li.

[3] Y. Lee, W. Dai, Z. Ming and M. Qiu, "Privacy Protection to Prevent Data Over-Collection in Smart Cities," IEEE Transactions on Computers, Vol. 65, no. 5, pp. 1339–1350, 2016.

[4] L. Kuang, L. Yang, J. Fang, and M. Dong, "Secure tenor decomposition using a fully homomorphic encryption scheme," IEEE Transactions on Cloud Computing, 2015.

[5] J. Wu, M. Dong, K. Ota, j. Li, and Z. Guan, "Big Data Analysis Secure Cluster Management for Optimized Control Planes in Software-Defined Networks," on IEEE Transaction Networks and Service Management, vol. 15, no. 1, pp. 27–38, 2018.

[6] K. Gai, K. K. R. Chu, M. Qiu, and L. Zhu, "Privacy-Protected Content-Oriented Wireless Communications in Internet Things," IEEE Internet of Things Journal, Vol. 5, no. 4, pp. 3059–3067, 2018.

[7] s. Hembleton et al., "Glimpses of 21st Century Care," Australian Journal of General Practice, Vol. ४ no, no. 10, pp. 670–673, 2018

[8] K. Gai and M. Qiu, "Blend Arithmetic Operations on Tensor Based Fully Homomorphic Encryption on Real Numbers," IEEE Transactions on Industrial Informatics.

[9] O. Solan and O'Laffland, "Cambridge Analytica Concludes After Facebook Data Harvesting Case," The Guardian, 201 Sol.

[11] T. Jiang, J. Hu and J. Sun, "Chaotic Selective Image Encryption Outsourcing for the Cloud with Outlook," Digital Signal Processing, Vol. 43, pp. 28–37, 2015.

[12] H. Qiu, Ji. Memmy, x. Chen and J. Jeong, "Retrieval of DC Coefficients for JPEG Images in Ubiquitous Communication Systems," Future Generation Computer Systems, 2014.

[13] G. O. Karam, c. Sorient, k. Lichota, and S. Capkan, "Securing Cloud Data under Cloud Exposure," Cloud Computing, 201. IEEE Transactions on.

[14] H. Qiu and Ji. Memmi,"Rapidly selective encryption methods for bitmap images," International Journal of Multimedia Data Engineering and Management (IJMDEM), Vol. 6, no. 3, pp. 51–69, 2015.

[15] H. Qiu, "PhD Thesis: An Efficient Data Protection Architecture Based on Fragmentation and Encryption," ArcX Prevent Arxive: 1.03.0880, 0, 201 Qi.