Usage of Social Spider Optimization Algorithm for Cryptography Technique for the Data Security in Cloud Network

Srinivas Reddy Baddam[1], Dr. M. Raghvender Sharma[2], Retired Prof. M V Ramana Murthy[3]

[1]Department of Computer Science, University College of Science, Osmania University
[2]Department of Statistics, University College of Science, Osmania University
[3]Department of Mathematics, University College of Science, Osmania University, India - 500007
[3]Department of Computer Science, King Abdul Aziz University, Saudi Arabia

***Abstract*: Cloud computing is an Internet-based computing model that uses a pay-per-use approach and makes a variety of resources available to Cloud Users (CU) through Cloud Service Providers (CSP) on demand. It encourages the virtualization of physical resources to increase productivity and the simultaneous completion of many tasks. The Cloud Computing Environment (CCE) offers a variety of deployment patterns to reflect different cloud categories that are controlled by organizations or academic institutions. Data storage in the cloud (also known as "cloud computing") provides a rapid and efficient means to gain access to one's information via a third-party service provider, enabling corporate expansion at a lower cost. Systems for storing larger amounts of data on storage servers are made possible by cloud data storage. Since the data saved in the cloud are kept for a longer period of time and are accessible through the internet, hackers can take the data stored there and send it elsewhere. This compromises data integrity and makes cloud data consumers unhappy. In order to improve security in cloud environments and cut down on the time required for cryptographic encryption, this article introduced unique cryptographic algorithms.**

***Keywords*: Cloud-Storage, Cryptographic-Tactics, Data Confidentiality, Data Integrity, Data Storage**

Introduction

Every year, the requirement for storage systems for firms, businesses, and enterprises increases by about 50%. As a result, underutilized storage facilities receive significant investment from organizations. Nevertheless, managing massive amounts of data comes at a significant cost. In the meantime, every businessperson wants to reduce risk and maximize profit. As a result, many small and medium-sized businesses decide to outsource the storage of their organization's data to third-party storage service providers that provide storage management services and on-demand storing space. The most recent approach available today for reducing operational costs and losses in the information, communication, and technology (ICT) age and corporate world is cloud computing. Cloud users can easily store and retrieve data in the cloud via remote storage, which offers them a convenient method of data sharing. Because the user is unaware of who actually has physical ownership of the outsourced data, maintaining data integrity in the cloud has been a worry. Cloud computing enables customers to keep their data in the cloud so they may access on-demand services. Using cloud-based services like project management to boost employee collaboration, small and medium-sized organizations with limited resources and budgets can achieve significant cost reductions and productivity improvements.

For the enhancement of the cloud performance, all modules should be given equal importance so that it allows the clients to use required resources optimally as per the tasks utilization. The resource placement is a process of distributing the task set to the resources. This module targets the resources and maps the tasks over it for execution [1].

In contrast to the dedicated providers used in conventional networked data storage, cloud storage technology allows users' confidential information to be stored on a variety of third-party providers. The providers offer consumers and other users of the Internet a data storage service.

Resource management, which is concerned with resource pooling, configuration, and task distribution performed by services providers, is significant at several levels. The task scheduler, which is a key component of resource management in cloud computing systems, uses optimization techniques to distribute user workloads across allocated logical resources known as "virtual machines (VM)"

Cloud computing aims to apply conventional supercomputing, or superior computing power, typically used by military and research facilities to carry out tens of trillions of computations per second in consumer-oriented applications

like financial portfolios, deliver customized information, produce information storage, or power massive, immersive computer games. Cloud computing distributes data-processing tasks across networks of big groups of machines, typically running low-cost consumer computer technology with specialised connections. This enormous network of interconnected systems is part of the common IT infrastructure. Virtualization methods are frequently used to enhance the power of cloud computing.

We attempt our best to review current secure cloud storages that have been designed using cryptographic approaches in this work as we concentrate on the subject of cloud storage. We also evaluate these cloud storage options from several angles. With this effort, we hope to learn more about the kinds of cryptographic approaches that can be used in secure cloud storage systems as well as how those techniques are deployed. The security of cloud storage is protected in large part by cryptographic approaches, and the desire for secure cloud storage may help advance cryptography research. We expect that by providing some guidance for future study, this evaluation will enable the quick development of more secure cloud storage solutions.

Benefits Of Cloud Computing

There are no costs associated with purchasing hardware, software, or licence. increasing access. You may access information at any time, anyplace, which makes life simpler! The monitor arrives more successfully. keep inside budget and complete projects faster than expected. Personnel coaching is not as necessary. With a negligible learning curve on hardware and software system issues, more work can be done on a cloud with fewer employees. Reduce the number of new software systems licenced. Extend and develop without having to buy expensive software or computer code licences. boost your adaptability. In the absence of significant "people" or "money" issues, you will be able to change course.

Fig. 1: Benefits of Cloud Computing

Cryptography

Whom the data is intended for and how it will be scanned. Technology-related terms like "cryptography" and "algorithms" are used to describe secure information and communication methods that transform communications in difficult-to-decipher ways using mathematical concepts and a set of rule-based calculations. These widely accepted methods are employed for the creation of cryptological keys, digital signing, and verification in order to protect information privacy, online browsing, and private communications like MasterCard transactions and email. The fields of cryptography and cryptology are strongly related to cryptography. It covers methods like microdots, word-and-picture fusion, and several ways to conceal information while it is being stored or transported. However, in today's computer-centric world, cryptography is most often associated with changing plaintext (often known as cleartext) into ciphertext, then back again (a process known as encryption) (known as decryption). Cryptographers are those who study this area of study.

Literature Survey

Bhaskar Prasad Rimal et.al. [2] delivered a classification of cloud computing and expand the current and new cloud systems. The objective of this paper was to create a disciplined procedure of scattered resources with least expenditure in command to acquire great throughput with comfort in cloud computing. The cloud services involved like (Saas) software as a service, (Paas) platform as a service, (Iaas) infrastructure as a structure and hardware as a service.

Prince Jain [3] firstly discussed various models of cloud computing, security issues and research challenges in cloud computing. This paper presented the data security is a major issue for Cloud Computing. There were several other security challenges included security aspects of network and virtualization.

Kadwe Yugandhara et.al. [4] discussed the concept of data storage or cloud storage. The cloud storage use the service- Iaas (infrastructure as a service) and it shows the security .The best method used to solve the issues of cloud was encryption techniques and this paper discussed the algorithms AES and HMAC (message authentication code) and purposed of this paper was to secure more data in cloud system and store encrypted data into the storage server so its easy for user and data was not to be lost.

Mahmood et. al., [5] proposed a scheme to secure the data in cloud computing while preserving data integrity and confidentiality. In this scheme, a secret image is initially taken and is encrypted using AES algorithm, which is then embedded in the host image with the help of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). Thereafter, a hash is generated for the image using Secure Hash Algorithm -2 (SHA-2) and is then stored in the cloud. When the image is retrieved from the cloud, the hash is again generated using the same algorithm and is then both the hashes are compared in order to check the integrity and confidentiality of the data i.e. the image.

Rahman et. al., [6] proposed a technique for enhancing data security in cloud with the utilization of three techniques, cryptography, steganography and hash function. Here, in the cryptography technique, the Blowfish algorithm is utilized and, in the steganography, the Embedded Least Significant Bit (E-LSB) technique is used. The Secure Hash Algorithm (SHA) 256 bits technique is used to provide data integrity. Firstly, the input data is encrypted using Blowfish algorithm and is then hidden in the image. After this, the data detection and data destruction attacks are applied on the image in order to check the security of the system. Upon attack evaluation, it turns out that the steganography method applied here is sensitive to destruction attack, but it is secure from detection attack.

Steganography is the display of concealing sensitive or secret information inside of something that has all the hallmarks of being outside of the ordinary. Given that both steganography and cryptology are used to protect basic data, the two are frequently associated with one another. The difference between the two is that steganography merges strategies for data concealment, ensuring that no data is ever concealed. If a person sees the misunderstanding that the data is concealed inside, he or she won't recognise that there is any safeguarded data and won't make an effort to unravel the information. The level of the muddle is when steganography devices are used to conceal data that includes any type of data report and picture records, as well as when the client has to save an image and erase a piece of information.

Gupta et. al.,[7] provided an overall view and association of cryptographic procedures, with an importance on symmetric encryption procedures that should be used for cloud environment-based architectures and services that need information and link encoding. Also, the work provided the evaluation for symmetric and asymmetric procedures with prominence on symmetric procedures for safety contemplation on that one must be utilized for cloud centred architectures and facilities that need information and link encoding.

Conclusion

According to the literature review included in this study, the public cloud environment is particularly susceptible to network-based attacks including DoS, DDoS, and MITM. Therefore, it is imperative to address this problem by offering a secure authentication protocol and encryption mechanism to ensure correct user authentication and authorization. As a result, this research offers a hybrid authentication protocol mechanism that, according to analysis, is highly protected against network-based attacks. Furthermore, by making it extremely difficult for attackers to access and remain in the environment, the hybrid encryption mechanism suggested in this work secures both data at rest and data in transit. There are several existing studies on improving data security, accelerating operations, and storing data securely. Analyses of their applicability to the current cryptographic techniques are also conducted. By the application of improved cryptographic algorithms in the suggested framework, these concepts can be used to create effective and safe mechanisms for data security and storage in public cloud environments.

References

[1]. Kumar, S., Sharma, B., Sharma, V. K., Sharma, H., & Bansal, J. C. (2018). Plant leaf disease identification using exponential spider monkey optimization. Sustainable Computing: Informatics and Systems.

[2]. Bhaskar Prasad Rimal; Eunmi Choi; Ian Lumb, (2019) “A taxonomy and Survey of Cloud Scheming Systems”, IEEE Fifth International Joint Conference on INC, IMS, and IDC, vol.10, No.2, pp. 44-51.

[3]. Prince Jain, 2019, “Security Issues and their Solution in Cloud Computing”, International Journal of Computing & Business Research, Vol.3, No.1,pp. 1-7.

[4]. Kadwe Yugandhara; Jadhav Ashwini; Pagar Pooja,;Patil Suchita; Prof.J.S.Pawar, (2020) “ Secure Data Storage and Forwarding in Cloud Using AES and HMAC”, International Research Journal of Engineering and Technology, Vol. 03, No.02 , pp.75-79

[5]. Ghassan Sabeeh Mahmood, Dong Jun Huang and Baidaa Abdulrahman Jaleel. 2019. Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing. International Journal of Network Security. 21(2): 326-332.
[6]. Rahman, M.O., Hossen, M.K., Morsad, M.G and Chandra, A. 2018. An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding. International Journal of Computer Science and Network Security. 18(9): 85- 93.
[7]. Gupta, R., Gupta, P and Singh, J. 2021. Security and Cryptography. In Software Engineering for Embedded Systems. pp. 501-547.