Intelligent and Secured Cloud Service Management Using Smart Data Hashing Algorithm

Keturu Madan Mohan[1,*,†], Ponaganti Srinivasa Rao[1,†], SriRamakavacham PrudhviRaj[1,†] and Chennuri Nagendra Sai[4,†]

[1]*Sreyas Institute of Engineering and Technology, Nagole, Bandlaguda, Hyderabad*

Abstract

The primary goal of this system is to provide a duplication-free cloud server with strong encryption and decryption information logical reasoning without the need of registration centers. With the fast growth of cloud computing, an increasing number of clients want to preserve their information in the cloud servers. New security issues must be addressed in order to assist more clients in processing their data on the public cloud. All clouds have particular space management issues, necessitating the development of a novel method in the proposed system that enables duplication-free data services in a cloud environment. Security is the primary restriction in a cloud computing environment, illustrating the necessity of avoiding third-party registration centers in a distant server-based data maintenance scheme. We follow the maximizing of security utility principle in our system by utilizing a strong Smart Data Hashing Algorithm (SDHA) that processes data using a 256-bit unbreakable encryption technique.

Keywords

Cloud Computing, Security, Smart Data Hashing Algorithm, Duplication Free System, SDHA, Encryption, Decryption

1. Introduction

Cloud Computing enables on-demand access to cloud resources by integrating cloud computing into the mobile environment [1, 2]. Cloud Computing has garnered considerable interest in recent years, both in business and academics. According to a recent research conducted by Heavy Reading, the Cloud Computing industry will produce over 68 billion dollars in direct revenue by the end of 2017. According to many sources such as ABI research, the global Cloud Computing user base has skyrocketed, the number of users has increased from 42.8 million in 2008-998 million by 2014. Cloud computing applications, infrastructures, and frameworks (such as Gmail, Facebook, and others) are increasingly being used by IT companies (like Google App Engine, Amazon web service etc.). Cloud computing [3, 4] is becoming more and more popular, both with IT pros and with everyday users. Global smartphone app use and development is also on the rise. Rapid development and implementation of various Cloud Computing services necessitate extensive security investigation. The following figure, Fig. 1 illustrates a distributed Cloud Computing architecture.

ACI'23: Workshop on Advances in Computational Intelligence at ICAIDS 2023, December 29-30, 2023, Hyderabad, India

[*] Corresponding author.

[†] These authors contributed equally.

madan.keturu@gmail.com (K. M. Mohan); psrinivasraocse@gmail.com (P. S. Rao); prudhvirajraj98@gmail.com (S. PrudhviRaj); nagendrasai.ch@sreyas.ac.in (C. N. Sai)

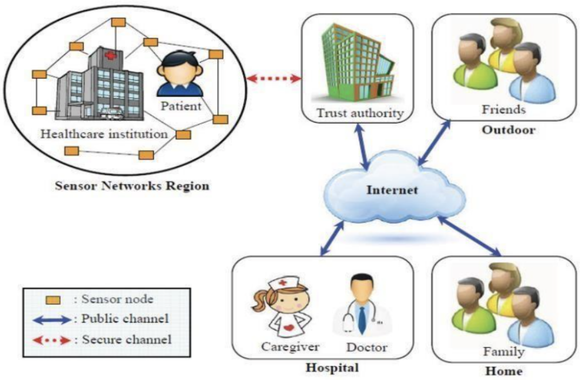

Figure 1: System Architectural View of Cloud Computing in Distributed Nature

To utilize a Cloud-Computing service, a mobile user MUi must first request the service using a mounted cellular application or internet browser. Following that' the user's mobile application or browser performs the data in the cloud and mobile user interface are authenticated with each other CSj. Both MUi and CSj must pass through a safe mutual authentication procedure that meets certain minimum standards. It includes compute competence, secrecy and session input defense among others to safeguard against a variety of threats sent across an unsecured channel. Cloud Computing services are intrinsically highly scattered and diverse. Thus, enrolling for each cloud service provider individually and keeping a distinct user account is a near-impossible effort. To be exact, MUi needs a single registered user account to access multiple cloud services from CSj. However, the standard two-party single-server authentication technique is incompatible with a multiple mobile device server scenario. SSO needs a single login and registration to access numerous Cloud Computing services. SSO involves three distinct parties: the network operator service as well as a verified identity supplier for mobile users. However, secret authentication may be performed with or without the involvement of an IdP/SCG/RC. Numerous ISPs and sites are now using 'Open- ID' to develop dispersed security solutions. Both the user and the service provider must register with the IdP in advance in this situation. An Open-ID is transmitted to the cloud service provider upon log in, who subsequently forwards it to the user authentication verification. This approach has two significant flaws. To begin, excessive IdP participation may become a bottleneck for the standard SSO system. Second, the OpenId approach necessitates the transmission of messages through an SSL- encrypted network connection. Regrettably, SSL-based methods have a significant computational cost due to the fact that security relies heavily on public-key-crypto-systems, like RSA, in order to secure communications [5]. By looking at the fundamentals of two-factor authentication, Wang and Wang were able to identify the reasons why user privacy is so important. Developing a privacy-preserving technique based only on lightweight cryptographic primitives like one-way hashing is difficult without public-key approaches, they highlighted. Cryptographic hash functions is almost impossible. Additionally, Wang and Wang demonstrated many security flaws in earlier user authentication techniques. They made three significant recommendations although analyze individual's authentication via: (a) preserving secrecy through the use of public-key

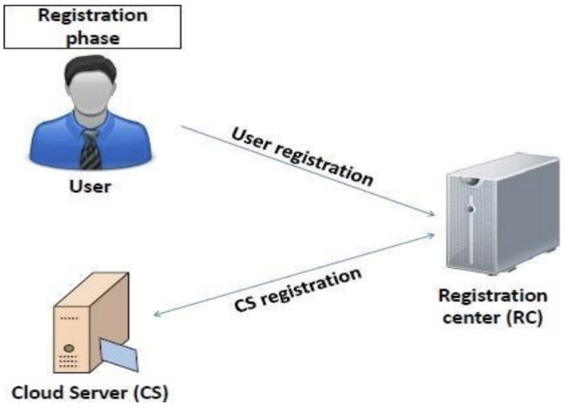

Figure 2: Cloud Server Registration Model

approaches, (b) utilizing a fuzzy-verifier to strike a balance between usability and security, and (c) preventing privileged insider attacks through the use of secret keys. Wang'et-al., proposed a set of assessment criteria for building unnamed 2-factor user verification and discussed how to strike a balance between stability, usefulness and security. Huang-et.al., noted that developing password assisted verification systems with smartcard necessitates the development of detailed security models in addition to prescribed security research. Huang'et-al., suggested a general multi factor authentication technique that utilizes the consumer's secret-word, a smartcard and other related may successfully authenticate a user even if the distant server's connection is down [6]. Ma et al. emphasized three design considerations for more resilient user verification solutions. Huang-et.al., examined a methodical method to client authentication employing three factors: a password, a smartcard and bio-metrics. The researchers suggested a generic and safe paradigm for transitioning from two-factor to three-factor authentication. It's worth noting but the renovation not only increased in turn declaration greatly at a minimal expenditure, other than preserved consumer isolation in circulated structure. This system proposed a novel authentication mechanism and combines simplicity, applicability, and robust concepts. Additionally, they offered an adversary model and set of criteria that may be used to assess existing as well as sequent 2- factor verification techniques. Additionally, Wang-et'al., noted that distinct attack scenarios, each of which may result in an authentication technique failing to achieve true two- factor security [7]. Additionally, they performed a major relative assessment of twenty-six exemplary two-factor methods, with their findings highlighting the need for improved dimension when evaluating novel verification techniques.

2. Related Study

Academics and businesses are increasingly using Cloud-Mobile Augmentation (CMA) approaches. A cutting-edge mobile augmentation paradigm, CMA uses cloud computing resources to augment, enhance, and optimize the mobile device's computing capabilities for the purpose of running resource-intensive applications. Mobile devices that can do sophisticated computations and store vast quantities of data while leaving the smallest possible footprint and vulnerability are called enhanced mobile devices. Cloud computing resources (e.g., faraway clouds and nearby mobile nodes) are used by researchers to meet the different computing demands of mobile users. There is no one-size-fits-all solution to utilizing cloud computing resources.

It is difficult to adjust to CMA if you don't take into account the current state of the mobile client and distant resources, as well as the best cloud-based resource type. An in-depth analysis of mobile augmentation and a taxonomy for CMA approaches are presented in this study [8]. Use of remote resources in augmentation methods will be demonstrated in this study, as well as issues related to the use of a range of cloud-based resources to enhance mobile devices. A taxonomy of augmentations is discussed, which includes both traditional and cloud-based augmentations. Our taxonomy is based on an in-depth review of current CMA approaches and four categories: distant fixed, proximal fixed, proximate mobile (and hybrid), and remote fixed. We provide an example of a decision- making flowchart for future CMA approaches and discuss how decision-making and performance constraints impact the adoption of CMA techniques. Mobile computing is discussed in the article, which cites open research questions as possible avenues for future study.

Cloud computing platforms like as Amazon Web Services, GoogleApp Engine, and Windows Azure have grown in popularity among IT businesses and developers in recent years. Simultaneously, we've witnessed a meteoric rise in the global adoption and deployment of smartphone platforms and apps. This article describes the present state of the art in the fusion of these two widely used technologies, dubbed Mobile Cloud Computing (MCC). We demonstrate how MCC may be used to a variety of sectors, including mobile learning, commerce, health/wellness, and social media. Additionally, we highlight research gaps related to important components of implementing and efficiently using MCC at scale. These improvements include increased resource allocation in the MCC environment through efficient task distribution and offloading, as well as increased security and privacy [9].

Users of the cloud may expect reliable, tailored, and quality service-assured computing environments thanks to the new paradigm of cloud computing. The cloud is a term used to describe a large, centralised data centre that houses applications and databases. Users may not be able to fully trust the cloud's stored data and computation results because of resource virtualization, global replication, and migration, and the lack of data and machines in the cloud. The vast majority of prior cloud security research has focused on protecting data stored in the cloud, rather than protecting data stored in the cloud itself. In this research, we introduce SecCloud, a privacy cheating deterrent and secure computation auditing system. Secure storage and computation auditing on the cloud have never been done before, but SecCloud makes this possible through the use of verifier signatures, batch verification and probabilistic sampling techniques. For the most cost-effective sample size, an in- depth analysis is offered. The SecHDFS cloud computing experimentation environment established in this paper is an important addition, since it serves as a test bed for SecCloud implementation. SecCloud's effectiveness and efficiency have been proven by additional testing results [10].

Using the Internet, cloud computing provides cost-effective, scalable, flexible, and powerful resources on demand. By maximizing and sharing resources, cloud computing substantially expands the capabilities of hardware. It's because of these reasons that organizations and individuals alike are moving their apps and services to the cloud, as outlined above. For example, power generation and distribution are moving to the cloud paradigm. There are additional security concerns when using cloud services provided by other parties. There are more security concerns in a shared environment with multiple users when user assets (data, applications, etc.) are moved outside of administrative control Cloud computing's fundamental nature raises security challenges, which are addressed in this paper. As an added bonus, the research also looks at recently published solutions to current security issues. In addition, a brief introduction of mobile cloud computing security challenges is presented. Lastly, there is a discussion of outstanding issues and future study fields [11]. When it comes to patient data security and privacy, cloud-enabled wireless body area networks (WBANs) constitute a big threat to both. Most studies have focused on the typical scenario in which patients are kept inside. A more realistic usage of cloud-aided WBANs in m- healthcare social networks, where patients travel outdoors and WBANs are more vulnerable to sophisticated attacks, such as node compromise, is examined in this study.

For hierarchical and dispersed systems, we provide a safe and privacy-preserving key management technique that is resistant to both time-based and locational attacks. As a further security, it uses a blinding strategy to protect the patient's identity, sensor deployment and location, as well as Blom's symmetric key system with modified proactive secret sharing. Using the cloud server to do the computationally intensive privacy-preserving key material update decreases energy usage for energy-constrained WBANs dramatically. When it comes to mobile assault resistance, storage, computation, and communication overhead [12], our approach outperforms previous systems.

3. Methodology

Among the most popular cloud services is data storage. Cloud storage has immensely benefited cloud users since they can store large amounts of data without having to upgrade their equipment and access them from any location at any time. It's still possible to have issues with cloud storage services provided by Cloud- Cloud-Service-Providers. First and foremost, cloud-based data may necessitate a variety of security measures based on the sensitivity of the data. The data saved in the cloud includes sensitive personal information, data that is publicly published, data that is shared with a group, and so on. Providing sensitive information in a cloud environment is a big no-no since outsourced data might expose users' sensitive or even confidential material. The following are the limitations presented over the past cloud handling methodology, such as:

- Encrypted Data could incur much waste of cloud storage and complicate data sharing among authorized users.
- We are still facing challenges on encrypted data storage and management with deduplication.

The following systems are emphasized more in the proposed development method, and they are described as follows: We need to manage and protect data security and privacy in order to save cloud storage across numerous third parties. Deduplication methods and secured data storage are essential in a variety of scenarios. Deduplication and access control are both supported by a Secure Minimal Remote User Authentication Scheme, which may be tailored to

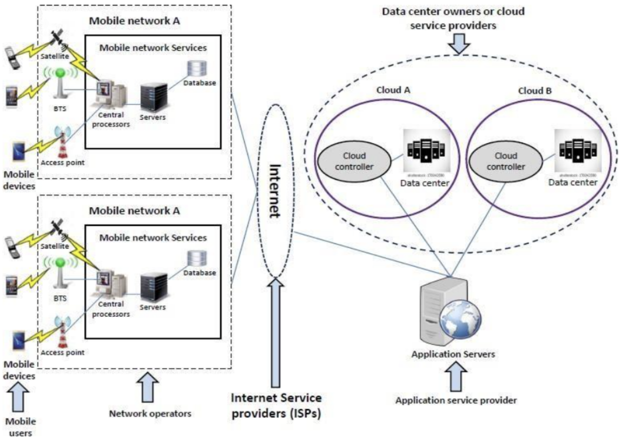

Figure 3: SDHA-based Cloud Handling Scheme – System Architectural View

meet the needs of data owners in a variety of application situations. The data owners or other trusted parties, or both, may be able to regulate the sharing of their data in a flexible manner. Proposed schemes are supported by security analysis, and the SDHA security principles used to execute them are quite powerful. The following are the advantages presented over this methodology, such as:

- Flexible Cloud Data Deduplication with proper Access Control facilities
- The proposed scheme is more secured, advanced and efficient.
- SDHA cryptography scheme is introduced to provide efficient and secured data storage over cloud environment.

3.1. Authorization and Authentication of Users

An important part of getting access to portals and apps is the User Authorization and Authentication module. Users (Data Owners and Data Users) may register and identify themselves in the system using relevant identifiers such as their Name, Mobile Number, E-Mail-Id, address, Username, and Password in this enhanced authentication and authorization standards module. A user's access to the application is provided when he or she has been through the necessary authentication and authorization processes. As part of the User Authorization and Authentication module, users may access three tiers of authentication services, including Password Generation, Password and Username, and Key Generation. It is through the authentication module that users enter the system and get access to its features. This is true for all users.

3.2. Maintenance of Secured and Encrypted Data

Protected as well as Encoded Data Processing allows the data owner to store data on a remote cloud server using proper authentication and security methods. The foundation for this module is the Smart Data Hashing Algorithm (SDHA), which is used to quickly handle the Encryption and Decryption processes, converting plain text to encrypted text and then maintaining the data on a distant server. Thus, no one can compromise the server or the data it contains. For all intents and purposes, the complete module of Secured and Encrypted Data Maintenance assists data owners in safely storing data in distant locations without fear.

3.3. Data Search for Authorized Parties

The Authorized Party Data Search module enables data users to conduct searches for records that have been saved on the server. The user must go through multiple levels of validation, including three-factor authentication, and must request the relevant data, which is then submitted to the server. The system generates a random master password for the customer and offers them to enter it on the portal after the request has been submitted. When a user enters a valid password, the server allows the user to download the information requested; if the password is invalid, the user is immediately prevented from doing so.

3.4. Scenario Regarding Page Ranking

Page Rank is a ranking algorithm that search engines employ to determine the order of the items in their search results. Page Rank is a metric used to determine the significance of online sites. According to Google, Page Rank is calculated by analyzing the quantity and quality of links to a page in order to assess the website's relative importance. The basic idea is that more authoritative websites will obtain a greater number of links from other authoritative websites. It is not the only algorithm used by Google to organize search engine results, but it is the company's first and most well-known algorithm. The following algorithm illustrates the overall process flow of the proposed algorithm called Smart Data Hashing Algorithm (SDHA) in detail with proper specification.

3.5. Smart Data Hashing Algorithm (SDHA)

Step-1: Acquire the Input Data File from the Data Owner.
Step-2: Receive the data in binary stream variable and process it with 256 bits per second accessibility.
Step-3: Identify the data value pairs for the input content.
Step-4: Check for special characters and maintain that into the separate entity computation. This step evolves the time saving capability to the algorithm and processes it in a faster manner.
Step-5: Assemble the data in proper manner with respect to value chunks and content capability.
Step-6: Estimate the data length with respect to the acquired content value pairs (manipulated over Step-5).
Step-7: For each chunk generate the iteration for manipulating the secret keys to hash the content in fine manner.
Step-8: Cross-validate the key structure based on the chunks and unpredictable formats in nature.
Step-9: Generate one random function using 'Random Number()' class in C# and to create a robust key with respect to the value ranges between 1000 and 9999.
Step-10: Acquire the random value in integer variable called 'Rnd'.

Step-11: Associate the generated random value 'Rnd' (Step-10) into the secret key to make it in unique way.
Step-12: The content is hashed in step by step manner based on the value chunks with respect to the key generated.
Step-13: Assemble the hashed content into the binary data stream object called 'obj'.
Step-14: Terminate the iteration created over step-7 and accumulate the overall values in one entity.
Step-15: Return the overall hashed content to the server and store it in a proper way.

4. Results and Discussions

This section briefly describes the results of the proposed approach and the algorithms are depicted with proper accuracy ratio. The proposed system algorithm called Smart Data Hashing Algorithm (SDHA) provides a clear security over cloud system and also provides multiple features in association with security norms. The overall implementation of the work is completed by using the powerful cloud management code development platform called Microsoft Visual Studio C#. The following figure, Fig.4 provides the performance evaluation of the proposed SDHA approach in clear manner and the performance metrics are cross-validated with conventional Merkle-B Cloud systems.

Figures for Performance Evaluation of the Proposed Approach are given below:

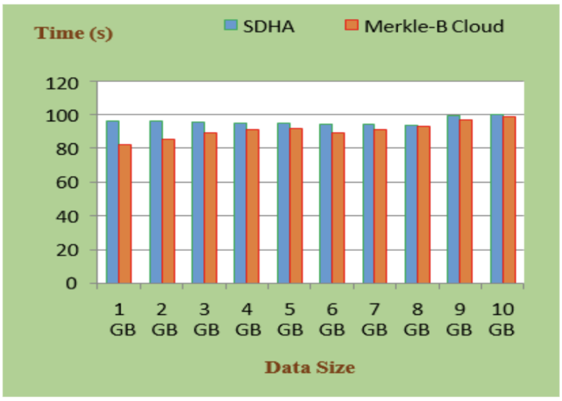

Figure 4: Data Processing Time for the Proposed Approach

5. Conclusion and Future Scope

Data de-duplication is essential in cloud environments, specifically when dealing with large amounts of information. When it comes to cloud data de-duplication and access control, we've suggested a heterogeneous storage management solution. The suggested method is flexible enough to accommodate a wide range of application situations and needs, and it provides cost-effective large data storage management across several CSPs. An evaluation of our scheme's

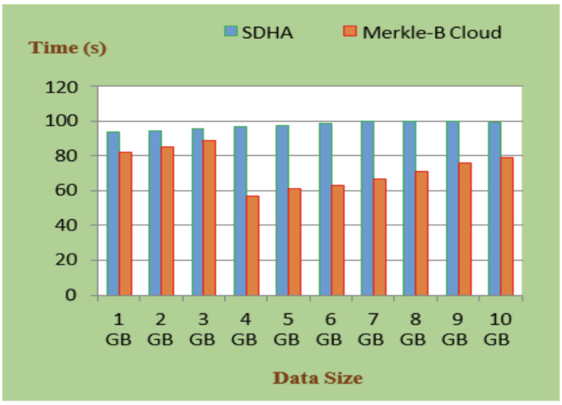

Figure 5: Cloud Service Selection for the Proposed Approach

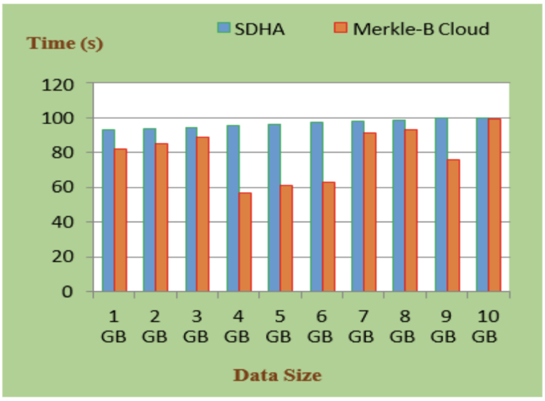

Figure 6: Verification Ability of the Server for the Proposed Approach

security and performance was based on a comparison with prior work and an implementation-based assessment of its efficiency. In the future, the work can further be enhanced by means of adding some cipher policies with modified crypto norms such as Modified Data Cipher Policies (MDCP) to build a robust security scheme to protect the data over the cloud environment.

References

[1] P. Agrawal, A. Zabrovskiy, A. Ilangovan, C. Timmerer, R. Prodan, Fastttps: fast approach for video transcoding time prediction and scheduling for http adaptive streaming videos, Cluster Computing 24 (2021) 1605–1621.

[2] A. Zabrovskiy, P. Agrawal, V. Kashansky, R. Kersche, C. Timmerer, R. Prodan, Fspot: Fast and efficient video encoding workloads over amazon spot instances, Computers, Materials and Continua 71 (2022) 5677–5697.

[3] E. Torre, J. J. Durillo, V. De Maio, P. Agrawal, S. Benedict, N. Saurabh, R. Prodan, A dynamic

evolutionary multi-objective virtual machine placement heuristic for cloud data centers, Information and Software Technology 128 (2020) 106390.

[4] V. Kashansky, D. Kimovski, R. Prodan, P. Agrawal, F. Marozzo, G. Iuhasz, M. Marozzo, J. Garcia-Blas, M3at: Monitoring agents assignment model for data-intensive applications, in: 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2020, pp. 72–79. doi:10.1109/PDP50117.2020.00018.

[5] V. Odelu, A. K. Das, A. Goswami, A secure and efficient ecc-based user anonymity preserving single sign-on scheme for distributed computer networks, Security and Communication Networks 8 (2015) 1732–1751.

[6] J.-L. Tsai, N.-W. Lo, A privacy-aware authentication scheme for distributed mobile cloud computing services, IEEE Systems Journal 9 (2015) 805–815. doi:10.1109/JSYST.2014.2322973.

[7] V. Odelu, A. K. Das, A. Goswami, A secure biometrics-based multi-server authentication protocol using smart cards, IEEE Transactions on information forensics and Security 10 (2015) 1953–1966.

[8] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, R. Buyya, Cloud-based augmentation for mobile devices: Motivation, taxonomies, and open challenges, IEEE Communications Surveys & Tutorials 16 (2014) 337–368. doi:10.1109/SURV.2013.070813.00285.

[9] M. R. Rahimi, J. Ren, C. H. Liu, A. V. Vasilakos, N. Venkatasubramanian, Mobile cloud computing: A survey, state of art and future directions, Mobile Networks and Applications 19 (2014) 133–143.

[10] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A. V. Vasilakos, Security and privacy for storage and computation in cloud computing, Information Sciences 258 (2014) 371–386. URL: https://www.sciencedirect.com/science/article/pii/S0020025513003320. doi:https://doi.org/10.1016/j.ins.2013.04.028.

[11] M. Ali, S. U. Khan, A. V. Vasilakos, Security in cloud computing: Opportunities and challenges, Information Sciences 305 (2015) 357–383. URL: https://www.sciencedirect.com/science/article/pii/S0020025515000638. doi:https://doi.org/10.1016/j.ins.2015.01.025.

[12] J. Zhou, Z. Cao, X. Dong, N. Xiong, A. V. Vasilakos, 4s: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks, Information Sciences 314 (2015) 255–276.