ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 4,April2015*

# A Secure Development Scheme of the Hash Function and its Implementation in Public Key Cryptography for Maintaining the Privacy of Data in the Federated Cloud Computing

**Dr.M.Srivenkatesh[1], Ms.K.Vanitha[2]**

Associate Professor, GITAM Institute of Technology, GITAM University[1]

Assistant Professor, Dept.Computer Science, GITAM University[2]

**Abstract**: FederatedCloud computing is an internet based technology where a large amount of resources are shared as a service among several cloud service providers. Privacy of Data is very critical issues in federated cloud computing. We propose hash function and its implementation in public key cryptography for maintaining the privacy of data in the federated cloud computing.

**Keywords**: Federated Cloud computing, privacy of data, MD5.

## I. INTRODUCTION

**A.** *Federated Cloud Computing*

They are some deifications of cloud computing namely Inherently Limited Scalability of Single-Provider Clouds, Lack of Interoperability among Cloud Providers. No Built-In Business Service Management Support .To address these issues Federated Cloud Computing was introduced.Cloud federation brings together different service providers and their offered services so that many Cloud variants can be tailored to match different sets of customer requirements. Cloud provider can provide resources to satisfy complex application request only if he holds infinite resources at his premises.Since this is not the case, so providers need to collaborate to be able to fulfill requests during peak demands and negotiate the use of idle resources with other peers.A federated cloud (also called cloud federation is the deployment and management of multiple external and internal cloud computing services to match business needs. A federation is the union of several smaller parts that perform a common action. Scalability-- Cloud bursting to address peak demands .The major advantages of federated cloud computing is

- Scalability-- Cloud bursting to address peak demands
- Collaboration--Sharing of infrastructure between partners
- Multi-site Deployments-- Infrastructure aggregation across distributed data centers
- Reliability--Fault tolerance architectures across sites
- Performance--Deployment of services closer to end users
- Cost--Dynamic placement to reduce the overall infrastructure cost
- Energy Consumption--Minimize energy consumption.

Federated clouds, by providing end to end quality of services, offer many advantages over traditional cloud services, which are:

**Guaranteed performance**: Due to limited resources, that are available with a single cloud service provider, sudden increase in workload may lead to deterioration of performance. Cloud federation overcomes this disadvantage by hiring resources from foreign cloud service providers, thereby guaranteeing the agreed Quality of Service. Also, high priority processing is guaranteed by delegating low priority processing tasks to foreign cloud service providers.

**Guaranteed availability**: During unexpected disasters, the cloud system will be able to recover the services by federating with other cloud service providers in unaffected areas. Availability may be guaranteed according to the priority of the service, as disaster recovery may not be an instant process.

**Convenience of service cooperation**: Cloud federations greatly increase the convenience by providing a one stop solution such that the consumer can see all the services together. For example, while applying for a passport, all the associated services may be integrated as one single service.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 4,April2015*

**Dynamic load distribution**: Geographical distribution of clients for every cloud service provider is highly uneven. In order to provide seamless services, dynamic load distribution is facilitated by cloud federations so that they could rise above their geographical shortcomings.

## II. PRIVACY OF DATA IN FEDERATED CLOUD COMPUTING

Security in Federated Cloud Computing is very important and critical Issues. Our emphasis here is privacy of data in the federated cloud computing. We are using public key cryptography to maintain privacy of data in the federated cloud computing.

### Cryptography

Symmetric algorithms

Ciphers such as AES and DES are known as conventional, symmetric algorithms, or secret key algorithms in such algorithms, $K = K^{-1}$ i.e., the encryption key and the decryption key are the same.

Asymmetric cryptography

In public key or asymmetric cryptography, $K \neq K^{-1}$. Furthermore, given K it is infeasible to find $K^{-1}$

### Need for public key cryptography

If sender and receiver want to exchange secret messages, they first have to share a key and Key-handling is hard. The Problem of Key-Handling Reusing keys is dangerous — many cryptanalytic attacks work by looking for key reuse The problem of key handling are eliminated by public key cryptography. Public key cryptography includes RSA Algorithm and digital Signatures.

The organization of the paper is as follows. Section one deals with brief introduction and benefits of federated cloud computing and section two gives brief description about privacy of data in federated cloud .Section three describes about state of art (Literature review).Section four describes cryptography has functions and MD5 deals with security issues in federated cloud section five describes the proposed work . Conclusion and references are specified in section six and seven.

## III. STATE OF ART-LITERATURE REVIEW

Some major security issues existing in current cloud computing environments which include issue data security in a cloud is protection of the data was discussed [1]. It discusses idea is to construct a privacy preserving repository where data sharing services can update and control the access and limit the usage of their shared data, instead of submitting data to central authorities, and, hence, the repository will promote data sharing and privacy of data. It also discusses about data confidentiality

In [2] provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.

Another interesting investigation [3] has identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-pre solvability. Beginning with these attributes, presented the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario.

In meteorology [4], the most destructive extra tropical cyclones evolve with the formation of a bent-back front and cloud head separated from the main polar-front, creating a hook that completely encircles a pocket of warm air with colder air. The most damaging winds occur near the tip of the hook. The cloud hook formation provides a useful analogy for cloud computing, in which the most acute obstacles with outsourced services (i.e., the cloud hook) are security and privacy issues. It identifies key issues, which are believed to have long-term significance in cloud computing security and privacy, based on documented problems and exhibited weaknesses

Privacy manager for cloud computing was discussed [5], which reduces the risk to the cloud computing user of their private data being stolen or misused, and also assists the cloud computing provider to conform to privacy law. They described different possible architectures for privacy management in cloud computing; give an algebraic description of obfuscation, one of the features of the privacy manager; and described how the privacy manager might be used to protect private metadata of online photos.

Security issues and threats, public auditing in the Cloud Computing was discussed in[6].It requires a secure cloud storage system with independent efficient auditing service to check the correctness of outsource data. Auditing service should not bring any new vulnerability towards the user data privacy. The existing remote integrity checking protocols can only serve for the static data and not for dynamic data. It proposed scheme focuses on efficient and secure cloud storage system and dynamic privacy-preserving audit service (TPA) for verifying the integrity of outsourced storage.

The confidentiality of cloud data was described [7]. To ensure the confidentiality, the most common used technique is encryption. But encryption alone doesn't give maximum protection to the data in the cloud storage. Encryption and obfuscation as two different techniques to protect the data in the cloud storage. Based on the type of data, encryption and obfuscation can be applied. Encryption can be applied to alphabets and alphanumeric type of data and obfuscation can be applied to a numeric type of data. Applying encryption and obfuscation techniques on the cloud data will provide more protection against unauthorized usage. Confidentiality could be achieved with a combination of encryption and obfuscation.

Another investigation [8] is establishing trust in hybrid cloud computing environments. It deals with the scope of federated cloud computing enlarges to ubiquitous and pervasive computing; there will be a need to assess and maintain the trustworthiness of the cloud computing

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 4,April2015*

entities. it present s a fully distributed framework that enable trust-based cloud customer and cloud service provider interactions. The framework aids a service consumer in assigning an appropriate weight to the feedback of different raters regarding a prospective service provider. Based on the framework, author developed a mechanism for controlling falsified feedback ratings from iteratively exerting trust level contamination due to falsified feedback ratings.

## IV. A. CRYPTOGRAPHIC HASH FUNCTIONS

For encryption, we use "symmetric algorithms; use RSA for the session key" and for digital signatures, we use "sign the message" It's still too expensive. We need cryptographic hash functions .We sign H(M), not M. Cryptographic Hash Functions must be reasonably cheap and take an arbitrary-length message and produce a fixed-length output. It is impossible to forge signatures by attacking the hash function.

Properties of Cryptographic Hash Functions

Collision resistance It is computationally infeasible to find x, y, $x \neq y$ such that H(x) = H(y)

Pre image resistance given an output value y, it is computationally infeasible to find x such that H(x) = y

Second pre image resistance Given an input x, it is computationally infeasible to find x ′ such that H(x) = H(x ′)

Modern Hash Functions

• MD5 (128 bits) — Invented by Rivest

• SHA-256, SHA-384, SHA-512 — Stronger variants of SHA-1

• Other, less common ones: RIPEMD160 (160-bit), Whirlpool (512 bits).

### B. What is the MD5 hash?

The MD5 hash also known as checksum for a file is a 128-bit value, something like a fingerprint of the file. There is a very small possibility of getting two identical hashes of two different files. This feature can be useful both for comparing the files and their integrity control.

Let us imagine a situation that will help to understand how the MD5 hash works. When two users have two similar huge files. How do we know that they are different without sending them to each other? We simply have to calculate the MD5 hashes of these files and compare them.

### MD5 Hash Properties

The MD5 hash consists of a small amount of binary data, typically no more than 128 bits. All hash values share the following properties:

**Hash length**

The length of the hash value is determined by the type of the used algorithm, and its length does not depend on the size of the file. The most common hash value lengths are either 128 or 160 bits.

**Non-discoverability**

Every pair of no identical files will translate into a completely different hash value, even if the two files differ only by a single bit. Using today's technology, it is not possible to discover a pair of files that translate to the same hash value.

**Repeatability**

Each time a particular file is hashed using the same algorithm; the exact same hash value will be produced.

**Irreversibility**

All hashing algorithms are one-way. Given a checksum value, it is infeasible to discover the password. In fact, none of the properties of the original message can be determined given the checksum value alone.

The **MD5** message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512.

The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo $2^{64}$.

## V. THE PROPOSED APPROACH

Cloud service providers interact through communication interface. It intern accesses storage service. It has bidirectional interaction to user interface which is accessed by different number of users for their requested files. The user interface accesses the requested file from storage Service. The storage service uses MD5 Algorithm.

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted *A*, *B*, *C*, and *D*. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the state.

The processing of a message block consists of four similar stages, termed *rounds*; each round is composed of 16 similar operations based on a non-linear function *F*, modular addition, and left rotation. Figure 1 illustrates one operation within a round. There are four possible functions *F*; a different one is used in each round:

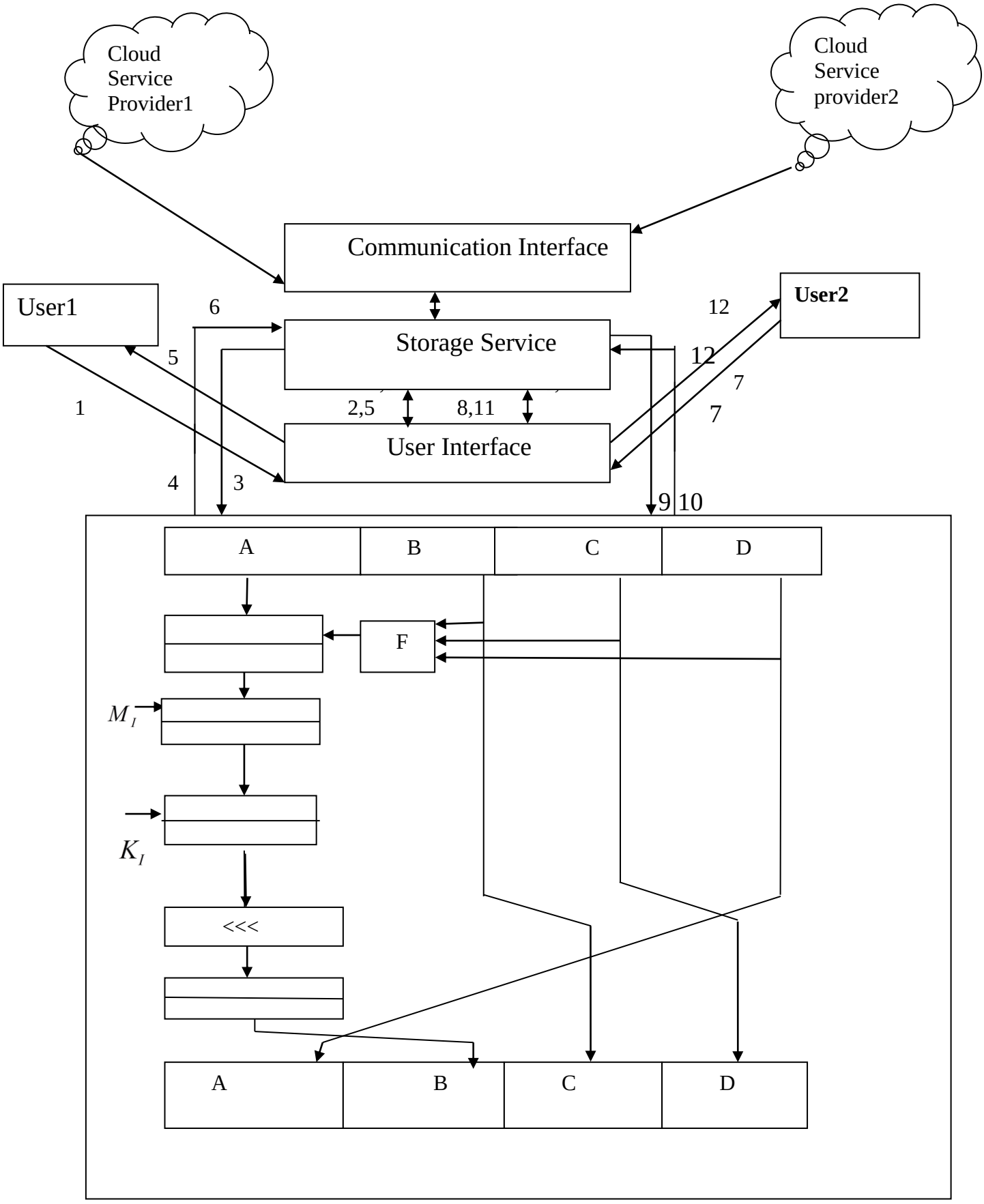
$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

$\oplus, \wedge, \vee, \neg$ denote

the XOR, AND, OR and NOT operations respectively.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 4,April2015*



ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 4,April2015*

A proposed Architecture for using MD5 In Federated Cloud Computing

1-Request for file says file1.
2-User interface accessing the storage service for requested file1.
3- Request for MD5 of requested file1.
4-MD5 of Requested file1 is sent to storage service.
5. By using this MD5, Requested file1 is sent to User interface .
6 . Original requested file1 is sent to user.
7-Request for file says file2.
8-Accessing the storage service for requested file2.
9- Request for MD5 of requested file2.
10. MD5 of Requested file2 is sent to storage service.
11 By using this MD5, Requested file2 is sent to User interface .
12. Original requested file2 is sent to user.

The figure shows the how the auxiliary function F is applied to the four buffers (A,B,C,D),Using message word $M_i$ and $K_i$. The item "<<<s" denotes a binary left shift by s" denote a binary left shift by s bits.
The output
After all rounds have been performed, the buffers A,B,C and D contain the MD5 digest of the original message. This output MD5 is sent to storage service, By using this MD5 message, storage service forwarded this requested file(say file1) to user interface .The user1 extracts the requested file from user interface. Same process is true of second user and so on.

## V1.CONCLUSION

We considered the privacy of data in federated cloud computing. We proposed A secure development scheme of the hash function and its implementation in public key cryptography for maintaining the privacy of data in the federated cloud computing

## REFERENCES

1. Ranjita Mishra, Debi Prasad Mishra, AnimeshTripathy,A Privacy Preserving Repository for Securing Data across the Cloud,Electronics Computer Technology (ICECT), 2011 3rd International Conference on (Volume:5 )
2.Wayne Jansen, Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing Wayne Jansen Timothy Granc National Institute of Standards and Technology ,U.S Department of Commerce,Draft Special Publication 800-14
3. ZhifengXiao,YangXiao,Security and Privacy in Cloud Computing,, Browse Journals & Magazines , Volume:15 Issue:2
4. Wayne A. Jansen ,Cloud Hooks: Security and Privacy Issues in Cloud Computing ,Proceedings of the 44th Hawaii International Conference on System Sciences – 2011
5. SianiPearson.YunShen and Miranda Mowbray, A Privacy Manager for Cloud Computing ,HPL Techreports,2009
6. R. Navajothi , S. Jean Adrien Fenelon , An Efficient, Dynamic, Privacy Preserving Public Auditing method on un trusted cloud storage , International Joint Conference of IEEE TrustCom,2014
7. L. Arockiam S. Monikandan. Efficient Cloud Storage Confidentiality to Ensure Data Security,2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014
8. JemalAbawajy, Establishing Trust in Hybrid Cloud Computing Environments,2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11