Cloud Computing – Key Hashing Cryptographic Implication based Algorithm for Service Provider based Encryption and Decryption

D. Ramesh[#1], Dr. B, Rama[*2]

[#]*Department of Computer Science & Kakatiya University, Warangal, Telangana, India*

Abstract *:The cloud computing data storage and retrieval based service providers are representing the client environmental based encryption techniques to avoid and restrict the unauthorized access along with privacy of the data, it provides the services of high securable data delivery and flexible data storage. The main role of encryption is to provide the provision to protect the sensitive data and play the key role for business developments. The main problem will be raised when the system will maintain the ownership control and to present the latest set of technical and business concerns. Many complex problems and challenges are waiting for the optimistic solutions, some of the problems, such as in the structured storage based environment, the provision of encryption environment for the data when it preserve self-ability to access the key elements along with their files which necessitate belonging to the plaintext; the data owners must maintain the privacy based control over their own data to make certain inclusive service based functionalities; and the data owners will face difficult to control their own data which available in cloud and their cloud based internal services such as type of data based topology architecture along with their functionalities, related security active models for employ the data security within their schemes and organizational services along with the encrypted based data access control. To overcome theses in convinces this paper is proposing the technical ideal through the algorithmic methodology along the graphical flow architecture. This paper is proposing the key hashing based cryptographic algorithmic flow chart implications and hashing algorithm techniques for service provider encryption and decryption end pointing mechanism to reduce the above mention complex difficulties; it describes the primary encryption based techniques and various levels of cryptographic algorithms with their implications. And also it has expressed how the hash functions can be extended in cloud based data security and digital forensics based applications.*

Keywords— *Encryption based Integrity (EbI), Key-Logging Facility (KLF), Cloud based Service Providers (CbSP), Information based Security (IbS), single mode encryption (SME), Application based Desired Plain Text (AbDPT), Application based Other Plain Text (AbOPT), pure-plaintext (PPT), pure-ciphertext (PCT), Fixed-Length-Sliding Window (FLSW), Message-Digest-Algorithm-5 (MD5), Secure-Hash-Algorithm-1 (SHA-1).*

I. INTRODUCTION

Cloud computing (CC) is a circulated wide area network with the provision of centralized cloud dependable service to the clients on regular and payment basis [16] [18]. Owners of data store their data in cloud which therefore need to be secured. By storing data in encrypted form, one can maintain the confidentiality and privacy of data in cloud. In CC the various cryptographic based approaches are formulated to address the subject of secrecy and privacy of authenticated-user generated. The authors Prasanna and Akki did detail descriptive investigation on cloud computing based privacy concern, security issues, challenges and cryptographic based algorithms [17]. Cryptography is the knowledge of writing in top secret code and is an ancient art [7]. In the cloud computing environment, the maintenance of authorization and provision of control over the data is a distinct prerequisite over and above assess and to authenticate the primary security of the cloud service providers based environment [6]. The unfortunate information revelation will cause affects the data possessor status, economic reputation, and impact their regulatory and legal compliance needs. The encryption techniques are the best and sophisticated data protection mechanism to derive the methods to protect the treasured data, the protection layers formed in the forms of secret keys to represent the privacy based data [2]. The Encryption based Integrity (EbI) is based on the technologies and progression of leading the cryptographic security depended services. Encryption is a crucial and important data along with their application based protection technique and the encryption keys should be accurately supervised and protected. The appearance of cloud based services will liberation of effective security based services, and also it implicated the encryption based capabilities which are utilized to secure the privacy data especially in the cloud based environment, and also it provide the chances and to enable the all kinds of organizations to easily protect their sensitive data through the internal key-logging facility (KLF). When cryptography is used to protect treasured data, the risk is transferred from the content to the keys and the protection of cryptographic keying material becomes paramount once the encryption has been designed in a systematic way. The crucial concern positioned in the way of cloud depended adoption based boundary is the requisite for trading to retain the possession and also to control of their own data while it is in progression and accumulate at cloud based service providers (CbSP) [6]. In present days, many organizations are willing to move towards to the cloud based environment it may capitulate the information based security (IbS) enhancement where the CbSP stick on to the third-party dependent frameworks. In cryptography mechanism, the un-encrypted data (UED), referred to as pure-plaintext (PPT). The PPT can be transmitted and encrypted into pure-ciphertext (PCT), which will in turn (usually) be decrypted into usable plaintext. The encryption and decryption is based upon the type of cryptography scheme being employed and some form of key. For those that like formulas, this process is sometimes written as***:*** $PCT=En_k(PPT)$ $PPT = De_k(PCT)$

II. FOCUSED PROBLEMS AND ISSUES

The main role of encryption is to provide the provision to protect the sensitive data and play the key role for business developments. The main problem will be raised when the system will maintain the ownership control and to present the latest set of technical and business concerns. Many complex problems and challenges are waiting for the optimistic solutions, some of the problems, such as

- In the structured storage based environment, the provision of encryption environment for the data when it preserve self-ability to access the key elements along with their files which necessitate belonging to the plaintext.
- The data owners must maintain the privacy based control over their own data to make certain inclusive service based functionalities.
- The data owners will face difficult to control their own data which available in cloud and their cloud based internal services such as type of data based topology architecture along with their functionalities, related security active models for employ the data security within their schemes and organizational services along with the encrypted based data access control.
- The cloud based service provider will not isolate the primary functionality of data-owners self control mechanism from their own privacy data.
- The reduction of generated keys along with its offsets by its necessitate to frequently make sure that the public depended segment of the key-pair securely allied with the possessor of its private based secret segment [3].

III. PAPER OBJECTIVES

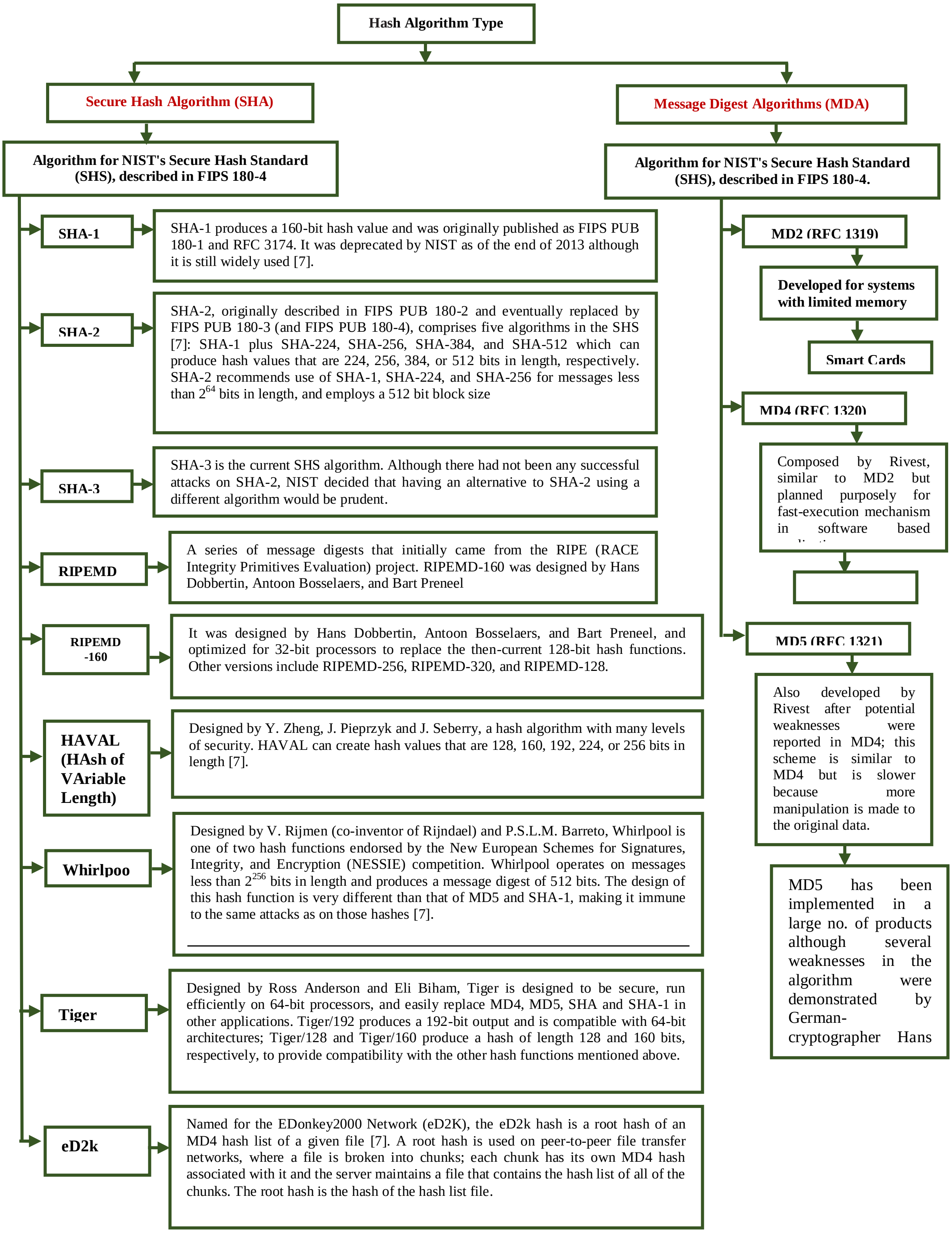
This paper is proposing the technical ideal through the algorithmic methodology along the graphical flow architecture. This paper is proposing the key hashing based cryptographic algorithmic flow chart implications and hashing algorithm techniques for service provider encryption and decryption end pointing mechanism to reduce the above mention complex difficulties; it describes the primary encryption based techniques and various levels of cryptographic algorithms with their implications. And also it has expressed how the hash functions can be extended in cloud based data security and digital forensics based applications.

IV. CRYPTOGRAPHIC ALGORITHMS AND THEIR IMPLICATED VARIATIONS:

The encryption techniques are the best and sophisticated data protection mechanism to derive the methods to protect the treasured data, the protection layers formed in the forms of secret keys to represent the privacy based data. The cryptographic based algorithms are classified into various ways and it will be characterized by the number of key-points are deployed for generating the encryption and decryption mechanisms and by their implicated application sequences.

V. HASH ALGORITHMS AND THEIR IMPLICATIONS::

The hashing based algorithmic (HbA) principles will act like as significant responsibility in terms of securing the systems by certify the reliability of the trusted based data communication. The HbA translates the variable-depended-length text field into a fixed-size-string and it primarily used in a security implicated systems with the two concerns [19] which are single mode hashing method**:** the derived the hash based output, it is complex to reverse the hashing based functions to generate the original message and non-**c**ollision based output method: for a hashing based algorithm, it is computationally infeasible to find any two messages which are the same hash output. Here the hash is treated as message digest or digital fingerprint by considering these two properties. The individuals are producing a small-hash-output from a bulky-document and use the digital fingerprint of the document as the hash based output. This type of digital fingerprint will be used to make sure that the data has not been interfering while it is transmission mode when is passing through the low-secure communication media. In addition, from the digital fingerprint, it is not possible to disclose the content of the original message. The message-digest-algorithm 5 (MD5) and Secure Hash-Algorithm-1 (SHA-1) are the widely used and implemented cryptographic hash based algorithms. These two types of hashing algorithms have been measured as the one-way and powerfully collision-free hashing algorithms. 128-bit output has been formed by MD5 and 160-bit output has been formed by SHA-1. Normally, the SHA-1 is measured as high-securable based on its larger size, but computationally it's more expensive than MD5. The SHA-1 is the favoured hashing based algorithm for implicating the VPN deployment mechanism. With the hardware and software implementation in today's networks, the performance difference is usually not a concern [19].


Hash Algorithm Type
Secure Hash Algorithm (SHA)
Message Digest Algorithms (MDA)
Algorithm for NIST's Secure Hash Standard (SHS), described in FIPS 180-4
Algorithm for NIST's Secure Hash Standard (SHS), described in FIPS 180-4.
SHA-1
SHA-2
SHA-3
RIPEMD
RIPEMD -160
HAVAL (HAsh of VAriable Length)
Whirlpoo
Tiger
eD2k
MD2 (RFC 1319)
Developed for systems with limited memory
Smart Cards
MD4 (RFC 1320)
MD5 (RFC 1321)

SHA-1 produces a 160-bit hash value and was originally published as FIPS PUB 180-1 and RFC 3174. It was deprecated by NIST as of the end of 2013 although it is still widely used [7].

SHA-2, originally described in FIPS PUB 180-2 and eventually replaced by FIPS PUB 180-3 (and FIPS PUB 180-4), comprises five algorithms in the SHS [7]: SHA-1 plus SHA-224, SHA-256, SHA-384, and SHA-512 which can produce hash values that are 224, 256, 384, or 512 bits in length, respectively. SHA-2 recommends use of SHA-1, SHA-224, and SHA-256 for messages less than 2^{64} bits in length, and employs a 512 bit block size

SHA-3 is the current SHS algorithm. Although there had not been any successful attacks on SHA-2, NIST decided that having an alternative to SHA-2 using a different algorithm would be prudent.

A series of message digests that initially came from the RIPE (RACE Integrity Primitives Evaluation) project. RIPEMD-160 was designed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel

It was designed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel, and optimized for 32-bit processors to replace the then-current 128-bit hash functions. Other versions include RIPEMD-256, RIPEMD-320, and RIPEMD-128.

Designed by Y. Zheng, J. Pieprzyk and J. Seberry, a hash algorithm with many levels of security. HAVAL can create hash values that are 128, 160, 192, 224, or 256 bits in length [7].

Designed by V. Rijmen (co-inventor of Rijndael) and P.S.L.M. Barreto, Whirlpool is one of two hash functions endorsed by the New European Schemes for Signatures, Integrity, and Encryption (NESSIE) competition. Whirlpool operates on messages less than 2^{256} bits in length and produces a message digest of 512 bits. The design of this hash function is very different than that of MD5 and SHA-1, making it immune to the same attacks as on those hashes [7].

Designed by Ross Anderson and Eli Biham, Tiger is designed to be secure, run efficiently on 64-bit processors, and easily replace MD4, MD5, SHA and SHA-1 in other applications. Tiger/192 produces a 192-bit output and is compatible with 64-bit architectures; Tiger/128 and Tiger/160 produce a hash of length 128 and 160 bits, respectively, to provide compatibility with the other hash functions mentioned above.

Named for the EDonkey2000 Network (eD2K), the eD2k hash is a root hash of an MD4 hash list of a given file [7]. A root hash is used on peer-to-peer file transfer networks, where a file is broken into chunks; each chunk has its own MD4 hash associated with it and the server maintains a file that contains the hash list of all of the chunks. The root hash is the hash of the hash list file.

Composed by Rivest, similar to MD2 but planned purposely for fast-execution mechanism in software based

Also developed by Rivest after potential weaknesses were reported in MD4; this scheme is similar to MD4 but is slower because more manipulation is made to the original data.

MD5 has been implemented in a large no. of products although several weaknesses in the algorithm were demonstrated by German-cryptographer Hans

Fig.1. Hash algorithm type, Implications, Type of variation, Implications

VI. HASH FUNCTION EXTENSION IMPLICATIONS IN DATA SECURITY AND DIGITAL FORENSICS APPLICATIONS:

Type of hash function extension	Implications	Application based environments
Hash based Libraries (HbL)	Through the HbL, the hash libraries are formed by the concern hash values based the initial files. HbL is well suitable for implicating the recognized composed files [7]	As the application side, It capable be a group of files known to be a component of an operating system, while a hash library of known bad files might be of a set of known child based pornographic images.
Rolling based Hashes (RbH)	RbH will demote to a group of hash based elements which calculated based upon a fixed-length-sliding window (FLSW) through the basic input	In RbH, the hash values will be calculated on bytes one to ten of a file, and also then on the bytes two to eleven, three to twelve, four to thirteen and so on.
Fuzzy based Hashes (FbH)	FbH are the area of passionate explores and it will characterize the hash based elements that correspond to two initial inputs which are equal.	FbH are used to identify the documents, images, or other files which are close to each other with relavent to content.

VII. KEY HASHING CRYPTOGRAPHIC IMPLICATION BASED ALGORITHMIC METHODOLOGY IMPLICATIONS:

As per shown in the flow chart figure.1 and the algorithm, the methodology has been implicated in two levels of execution such as end-user based signatures and application based segments. The application based segments can be processed and implicated from the clients or end-users signatures.

i. END-USER BASED SIGNATURES:

The first level of execution composes the initial authenticated sequences about the end-user based signatures through plain text (PPT) of signature mode1, private key(PK) of signature mode2 along with the derived base class environment. The derived base class can be composing the ciper text (PCT) by making the single set with two various elements of signatures such as PPT and PK.

Derived Base [CiperText(PCT)] → F(S(PPT,PK))

The final stage can be prepared from the sender's side environment with help of the function generation with the elements of PPT, PCT, EU-AuthCertificate values.

∫ (se(PPT, PCT, EU-AuthCertificate)

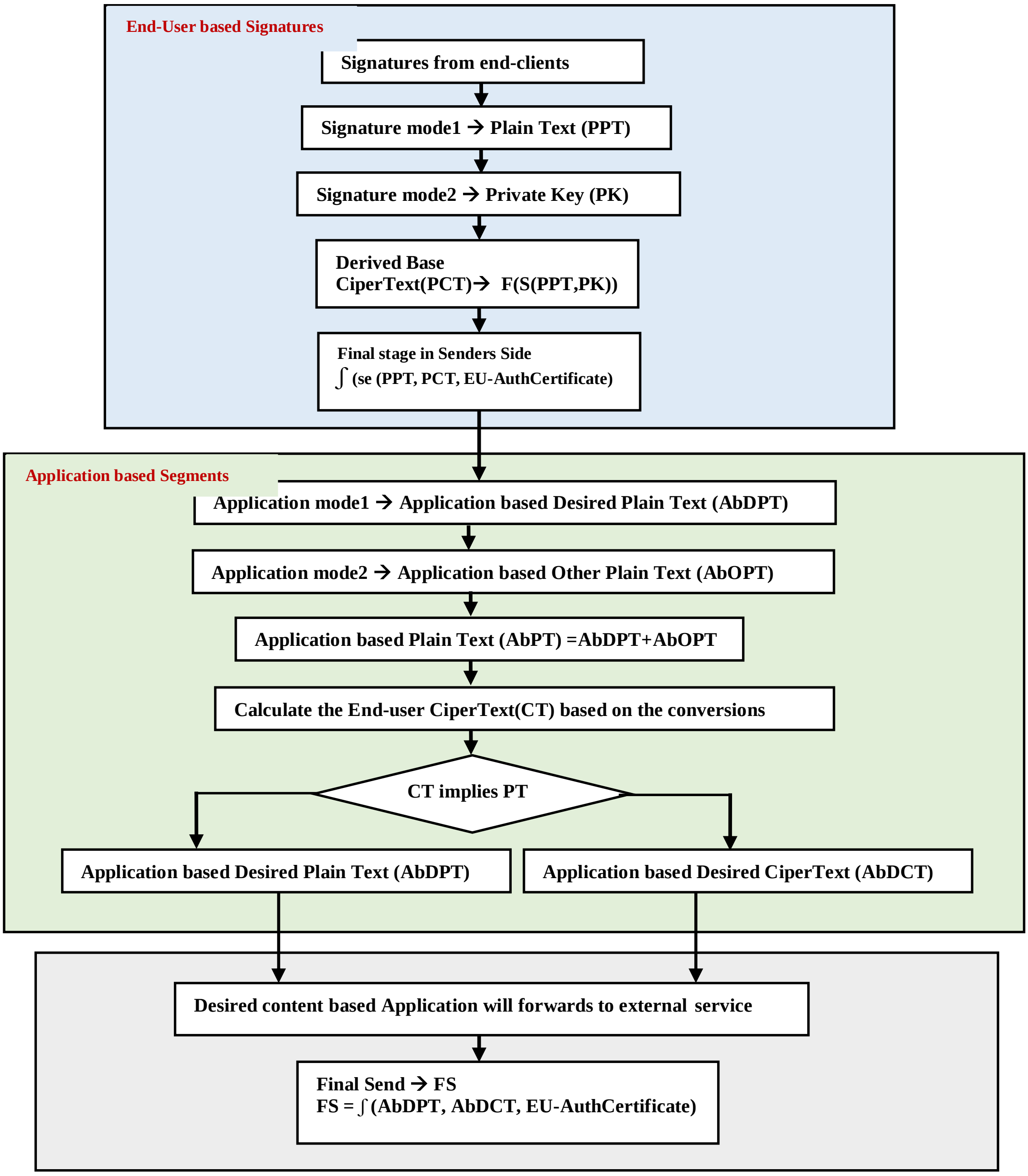
Finally, the generated final stage of operations will be pushed into the second level execution mode of application based segments for further up gradations such as update or modify the existing data or enhancement of new data along with the existing data.

ii. APPLICATION BASED SEGMENTS:

The second level of execution composes application based segments by deriving the two stages of applications modes such as application mode1 and application mode2. Here the first level of application mode can holds the application based desired plain text (AbDPT) and the second level of application mode can holds application based plain text (AbOPT) which is belongs to other plain text. This second level of application mode is the enhanced version of application mode1, it contains the new added or updated data of the particular specified application of the particular enterprise. These two various levels of application modes can be combined together to update the final version of the genuine data in cloud. The user need to add its final version of the data into the cloud server in his specified storage location without giving or advertising by its own existing or modified network architecture along with its own resources like as current active users, internal private accessibility keys and VPN environments. Generally, the cloud environment can restrict the end users to store their enhanced version of data to their existing data when they changed or modified their internal recourses which are not included when they get the resources services from cloud initially. This algorithmic techniques can transmits enhanced data to cloud storages to patch it with its own existing data with sending any private information about the client or end users. This filtering mechanism can be process through the computing the end-users cipertext(CT) based on their conversions. The CT implies the PT for deriving the AbDPT and AbOPT. Finally, the derived enhanced application based contents will be forwarded to external service and added to the cloud based server by FS implicated sequence.

FS = ∫ (AbDPT, AbDCT, EU-AuthCertificate)

iii. Flow chart:


End-User based Signatures
Signatures from end-clients
Signature mode1 → Plain Text (PPT)
Signature mode2 → Private Key (PK)
Derived Base CiperText(PCT)→ F(S(PPT,PK))
Final stage in Senders Side
∫ (se (PPT, PCT, EU-AuthCertificate)
Application based Segments
Application mode1 → Application based Desired Plain Text (AbDPT)
Application mode2 → Application based Other Plain Text (AbOPT)
Application based Plain Text (AbPT) =AbDPT+AbOPT
Calculate the End-user CiperText(CT) based on the conversions
CT implies PT
Application based Desired Plain Text (AbDPT)
Application based Desired CiperText (AbDCT)
Desired content based Application will forwards to external service
Final Send → FS
FS = ∫ (AbDPT, AbDCT, EU-AuthCertificate)

iv. Algorithm:

Step 0: End-User based signatures Gathering the signatures from the end-users / data owners

Step 1: Gathering the mode1 based signature
Signature mode1 → Plain Text (PPT)

Step 2: Gathering the mode2 based signature
Signature mode2 → Private Key (PK)

Step 3: Compose the derived base class
CiperText(PCT)→ F(S(PPT,PK))

Step 4: Senders side preparation to push the data for upgradation
ʃ (se (PPT, PCT, EU-AuthCertificate)

Step 5: Application based segments: Application mode1
Application mode1→ Application based Desired Plain Text (AbDPT)

Step 6: Application based segments: Application mode2
Application mode2 → Application based Other Plain Text (AbOPT)

Step 7: Application based Application based Plain Text (AbPT) will be generated by combining the Application based Desired Plain Text and Application based Other Plain Text

Application based Plain Text (AbPT) =AbDPT + AbOPT

Step 8: Comparison will be needed without advertising the end-users updated private environment for deriving the Application based Desired Plain Text and Application based Desired CiperText

IF CT implies PT
THEN Application based Desired Plain Text (AbDPT)
THEN Application based Desired CiperText (AbDCT)

Step 9: Desired content based Application will forwards to external service

Step 10: Finally stage of storage the enhanced data
Final Send → FS
FS = ʃ (AbDPT, AbDCT, EU-AuthCertificate)

And the services will verify this message as while the user had generated or sent it directly. The above implicational sequences will well work based on the type of hash algorithm has been implemented to squeeze the PPT also organism of homomorphic generation. Amongst them the homomorphic implicated and searchable encryption methods are largely fashionable where one can perform computation and search on PCT exclusive of revealing the PPT [18].

VIII. Conclusions

The main role of encryption is to provide the provision to protect the sensitive data and play the key role for business developments. The main problem will be raised when the system will maintain the ownership control and to present the latest set of technical and business concerns. This paper is proposing the key hashing based cryptographic algorithmic flow chart implications and hashing algorithm techniques for service provider encryption and decryption end pointing mechanism to reduce the above mention complex difficulties; it describes the primary encryption based techniques and various levels of cryptographic algorithms with their implications. And also it has expressed how the hash functions can be extended in cloud based data security and digital forensics based applications.

References

[1] Gutman, P., Naccache, D., & Palmer, C.C. (2005, May/June). When hashes collide. IEEE Security & Privacy, 3(3), 68-71.

[2] CLOUD SECURITY ALLIANCE, SecaaS Implementation Guidance, Category 8: Encryption, September 2012, http://www.cloudsecurityalliance.org,

[3] Cryptography, in an all encrypted world charting the future of innovation volume 92 | #10· 2015 december 22, 2015, Ericsson Technology Review cryptography in an all Encrypted World Security in the post-snowd

[4] Fraunhofer Institute for Secure Information Technology. (2012, March). On the Security of Cloud Storage Services. Retrieved from http://www.sit.fraunhofer.de/de/cloudstudy.html

[5] Vaultive Encryption in Use Platform, Taking Control of Cloud Data: A Realistic Approach to Encryption of Cloud Data in Use, Vaultive Inc. 489 5th Ave, 31st Fl.New York, NY 10017. www.vaultive.com

[6] Gary C. Kessler , An Overview of Cryptography, Handbook on Local Area Networks (Auerbach, Sept. 1998).

[7] Blum, D. (2010, March). Using Encryption to Protect Sensitive Data in Cloud Computing Environments, Retrieved from Gartner database.

[8] Burr, W. (2006, March/April). Cryptographic hash standards: Where do we go from here? IEEE Security & Privacy, 4(2), 88-91.

[9] European Network and Information Security Agency (ENISA). (2009). Cloud Computing benefits, risks, and recommendations for information security. Retrieved from

[10]

http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[11] ACE WG, 2015, Object Security of CoAP (OSCOAP), available at: https://tools.ietf.org/html/draft-selander-ace-object-security

[12] Gigaom Research, 2014, Data privacy and security in the post-snowden era, available at: HTTP://WWW.VERNEGLOBAL.COM/SITES/DEFAULT/FILES/GIGAOM_RESEARCH-DATA_PRIVACY_AND_SECURITY.PDF

[13] PERC, 2015, Secure Real-time Transport Protocol (SRTP) for Cloud Services, available at: https://tools.ietf.org/html/draft-mattsson-perc-srtp-cloud

[14] Proceedings of the 23rd ACM, 2011, CryptDB: Protecting confidentiality with encrypted query processing, abstract available at: http://dl.acm.org/citation.cfm?id=2043566.

[15] Ericsson, 2015, Encryption Performance Improvements of the Paillier Cryptosystem, available at: https://eprint.iacr.org/2015/864.pdf

[16] Mell, Peter and Tim Grace. Draft NIST Working Definition of Cloud Computing, Available at http://csrc.nist.gov/groups/SNS/clouddcomputing/cloud -def-v15.doc, on August 28, 2009.

[17] Prasanna B.T, C.B. Akki, A Survey on Homomorphic and Searchable Encryption Security Algorithms for Cloud Computing. Communicated to Journal of Interconnection Networks, April 2014.

[18] Prasanna B T, C B Akki, “A Comparative Study of Homomorphic and Searchable Encryption Schemes for Cloud Computing”.

[19] Qiang Huang and Jazib Frahim, SSL VPN Technology, Network World | Oct 22, 2008 http://www.networkworld.com/article/2268575/lan-wan/chapter-2--ssl-vpn-technology.html

[20] AccessData. (2006, April). MD5 Collisions: The Effect on Computer Forensics. AccessData White Paper.

[21] Dwyer, D. (2009, June 3). SHA-1 Collision Attacks Now 252. SecureWorks Research blog.

[22] Klima, V. (March 2005). Finding MD5 Collisions - a Toy for a Notebook.

[23] Lee, R. (2009, January 7). Law Is Not A Science: Admissibility of Computer Evidence and MD5 Hashes. SANS Computer Forensics blog.