Indian J.Sci.Res. 17(2): 72 - 81, 2018

ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

UNIQUE KEYS COMPUTED KEY ENCRYPTION ALGORITHM (UKCKEA) FOR PROVIDING SECURITY AND INTEGRITY ON DATA STORED IN CLOUD

[1] G Sudhakar, [2]Dr. S.Durgabhavani,

[1,2] School of IT, JNTUH.

Abstract: In the current technological era Cloud computing has transformed the way organizations approach Information Technology, which enable them to become more agile, provide more services, and reduce IT costs and IT Overhead as well. Today, if you see with the technology like virtualization and the cloud, securing stored data is mostly under the organization's logical control, but physically reside is in infrastructure and is generally owned and managed by another party(except in Private cloud which is managed by the organizations data administrator). In Most of the Scenario Data protection tops the list of cloud concerns today followed by data integrity in the cloud. In the current scenario of security policies the vendor security capabilities will play a key role for establishing strategic value, So we have to make sure that data is not readable by others by making strong key management policy, implementing strong access policies to ensure only authorized users can gain access to sensitive data and not allow even the so called privileged users such as root user to view sensitive data stored in the cloud.

Key Words: Cloud Computing, Data Security, Data Integrity, Strong Key Management, Access Policies.

I. Introduction:

Data protection is a crucial security issue for most organizations. Before moving into the cloud, cloud users need to clearly identify data objects to be protected and classify data based on their implication on security, and then define the security policy for data protection as well as the policy enforcement mechanisms. Data integrity is another important security issue in cloud computing. Such a security assurance is necessary not only for communications between cloud users

and cloud servers, but also for data at rest on cloud servers. In particular, cloud users may have great concerns on data integrity when outsourcing valuable data assets in the cloud for storage. The possible long lifetime of outsourced data would make it more likely vulnerable to intentional or inadvertent modification, corruption, or deletion, be it caused by careless system maintenance or for the purpose of cost saving. While the issue of data integrity for communications can be addressed with off_-the-shelf techniques such as message integrity code that for data storage seems to be more cumbersome because of the many reasons. Like

First: Cloud users may not be willing to fully rely on cloud service providers for providing data integrity protection. Second: Data integrity service should be provided in the timely manner. This is because in practical applications it is usually too late for cloud users to find out data corruption when they are actually retrieving the data. Third: The "self-served" data integrity check requires not only the active involvement of cloud users, but also the necessary expertise and computing power of them. Forth: As data stored on cloud servers may subject to modification by cloud users, the data integrity mechanism should efficiently support such data dynamics. Preferably, a data integrity protection mechanism should address all these issues, i.e., it should support frequent data integrity check on large volume of data when allowing third-party frication and data dynamics.

II.Cloud Computing (5-4-3-2-1 Model)

In my view it is a 5-4-3-2-1 model, which has 5 essential Characteristics, 4 basic Deployment Models, and 3 important Services between 2 parties with 1 strong service level agreement (SLA).

2.1 Definition of Cloud computing

Despite of various definitions given by various organizations, the standard definition which was given by the National Institute of Standards and Technology (NIST) is: *"Cloud Computing is model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The definition accepted universally by many organizations.* [44].

2.2 Essential Characteristics of cloud (5):

1. **On-demand self-service**
2. **Broad network access**
3. **Resource pooling**
4. **Rapid elasticity**
5. **Measured service**

2.2.1 On-demand self-service: A special kind of a service where a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider [44].

[1]Corresponding Author

2.2.2 Broad network access: a special kind of a capabilities available over the network and accessed through standard mechanisms that promote use by various heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations) [1].

2.2.3.Resource pooling: Pooling is done in many other ways but there is a special way provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand, where there is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data enter). Examples of resources include storage, processing, memory, and network bandwidth [1].

2.2.4 Rapid elasticity: Elasticity is provided by many other technologies ,but rapid elasticity either horizontal or vertical elasticity is provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time [1].

2.2.5 Measured service: This is a very special part in the Cloud systems which automatically control and optimize resource usage by leveraging a metering capability (pay-per-use basis) at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service [1].

2.3 Deployment Models and associated security issues (4):

1. **Private cloud**
2. **Community cloud**
3. **Public cloud**
4. **Hybrid**

2.3.1 Private cloud: The better and secure way of deploying a cloud setup is a private cloud. Here the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises and majorly controlled and security policies lies with themselves . [1].

2.3.2 Community cloud: This kind of model is used for units with special communities, where the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises the security here lies in the hands of community, and provider as well [1].

2.3.3 Public cloud: when it comes about security in the cloud data the worst will be the public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider so the total security policies will lie in the hands of the provider [1].

2.3.4 Hybrid cloud: It is also called as a 50:50 policy deployment model. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [1].

2.4 Service Models and associated security issues (3):

2.4.1 Software as a Service (SaaS): This is also called as the top level service in the cloud computing architecture. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [1].

Security in SaaS: SaaS deploys the provider's applications running on a cloud infrastructure; it offers anywhere access, but-t also increases security risk. With this service model it's essential to implement policies for identity management and access control to applications. For example, with Salesforce.com, only certain salespeople may be authorized to access and download confidential customer sales information.[4]

2.4.2 Platform as a Service (PaaS): This is also called as the Middle level service in the cloud computing architecture The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment [1].

Security in PaaS: In the cloud architecture it is between the SaaS and IaaS which is a shared development environment, such as Microsoft™ Windows Azure, where the consumer controls deployed applications but does not manage the underlying cloud infrastructure. This cloud service model requires strong authentication to identify users, an audit trail, and the ability to support compliance regulations and privacy mandates. There is a very big need of more security in this level, where a lot of vulnerabilities are unnoticed. [4]

2.4.3 Infrastructure as a Service (IaaS):

This is also called as the Bottom level service in the cloud computing architecture The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) [1].

Security in IaaS: For any service it is infrastructure which is very important and lets the consumer provision processing, storage, networks, and other fundamental computing resources and controls operating systems, storage, and deployed applications. As with Amazon Elastic Compute Cloud (EC2), the consumer does not manage or control the underlying cloud infrastructure. Data security is typically a shared responsibility between the cloud service provider and the cloud consumer. Data encryption without the need to modify applications is a key requirement in this environment to remove the custodial risk of IaaS infrastructure personnel accessing sensitive data [4]

III.Importance of Security in Cloud Computing:

As most of the surveys say data protection tops the list of cloud concerns today. Vendor security capabilities are key to establishing strategic value, reports the 2013 through 2017 it is the same given in the Computerworld “Cloud Computing” study, which measured cloud computing trends among technology decision makers.

“As we go forward and think about how applications are secured in the cloud, the application should be designed so you don’t know whether it is running in the cloud or your own infrastructure,” says Tumulak a cloud security expert. “The underlying platforms and solutions of the future that these applications run on will have cloud security built right into the DNA of the framework.”

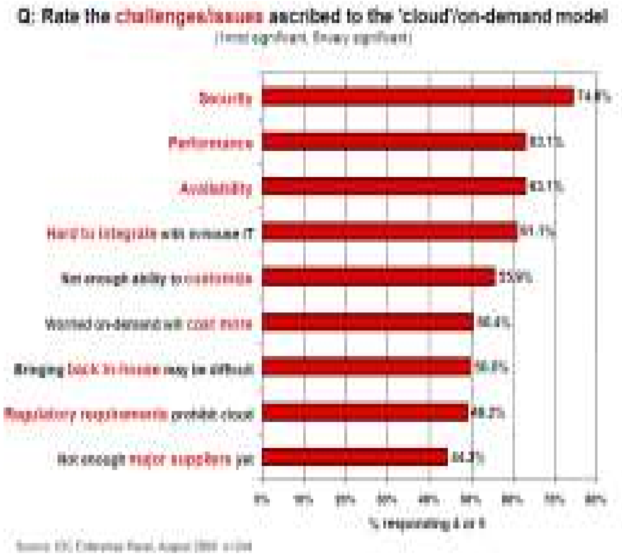


Figure 2.1
(Source:http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt at slide 17.)

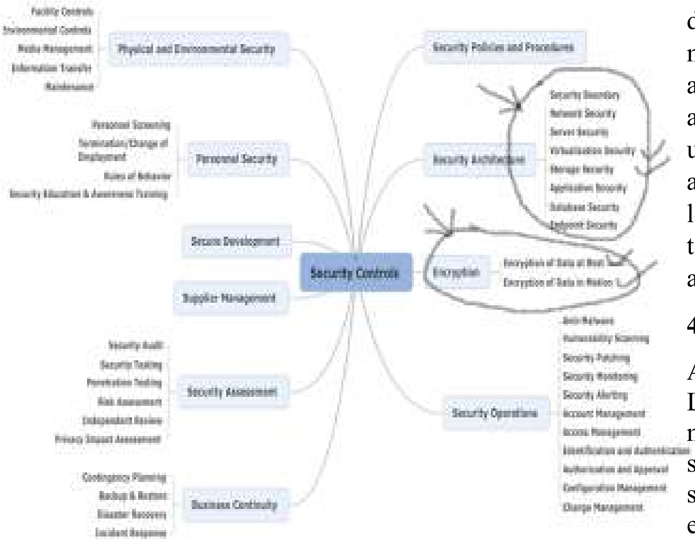
3.1 Jay Heiser Cloud Security Analyses:

In the Gartner’s report according to Jay Heiser analysis he says “through 2020, 95% of cloud security failures will be the customer's fault.” The major customer faults would be key management so strengthening key should be the primary focus for providing more security on data.

Reports says First Keeping the importance of cloud in mind by the Year 2016, 40% of enterprises with more than 1,000 employees, and 80% of organizations with over 10,000 employees, will have policies and practices in place to approve and track the use of SaaS. Second the number of enterprises with policies against placing any sensitive data in the public cloud will drop to 5% by 2017. Third By the Year 2017, 95% of cloud service providers with annual revenue over $500 million will have at least one formal security evaluation by 2020 it will be minimum one. Fourth Through the Year 2018, the number of public disclosures of in-house security failures will grow every year, but only one or two incidents a year will be attributed to poor cloud service provider technologies or practices. Lastly 50% of enterprises with more than 5,000 users will deploy products from cloud access security brokers to control their use of cloud services by the end of 2018. [14]

IV.My Emphasizes on Data Security:

As there is a much need for a good method that can solve the major problems associated with the protection of the sensitive Data in the public, private and Hybrid cloud. In an Academic System generally the cloud established will be a private cloud, so the Method of encryption implemented must incorporate robust key management, where a special key encryption algorithm likes “Unique Key



4.1 Cloud Computing Security chart:

In the above chart the highlighted part is the area where more logical security is required.

According to the Cloud Security Alliance(CSA) in the RSA conference 2016 still Data security aspects remain in the first place from the most Notorious Nine security elements (1.Data Breaches 2.Data loss 3.Account Hijacking 4. Insecure Interfaces and API’s 5.Denail of Service 6.malacious insiders 7.Abuse of Cloud Services 8. Insufficient Due Diligence 9.Shared technologies vulnerabilities)

To address all these security issues in Cloud Computing, we need to explore the nature of Cloud Computing security problems and answer the following questions: Which objects are we going to protect? Who can be the potential attackers and how would they attack? What kind of security services should we provide? Which security mechanisms should we use? [50]

4.1 Maintaining Data Security in Cloud

Irrespective of the specific cloud service chosen, there are a number of important security considerations that users should remain mindful of how to reduce the probability of unauthorised individuals gaining access to their data.

While many organizations have implemented encryption for data security, they often overlook inherent weaknesses in key management, access control, and monitoring of data access. If encryption keys are not sufficiently protected, they are vulnerable to theft by malicious hackers. Vulnerability also lies in the access control model;

“It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility. Here we emphasizes that an effective cloud security solution should incorporate three key capabilities: First is Make sure that data is not readable and that the solution offers strong key management (Data Lockdown). Second is Implement access policies that ensure only authorized users can gain access to sensitive information, so that even privileged users such as root user cannot view sensitive information and third is incorporate security intelligence that generates log information, which can be used for behavioural analysis to provide alerts that trigger when users are performing actions outside of the norm.

4.2 Data Security and Integrity issues:

As cloud computing encompasses many technologies like Load Balancing, concurrency control, memory management, transaction management, resource scheduling, virtualization (cloud paradigm results in many security issues), operating systems, databases, networks so every technology has its own securities, so we can imagine that there numerous security issues associated with it. Data Security involves encrypting the personal data as well as ensuring that appropriate policies are enforced for data sharing. Today, with virtualization and the cloud, data may be under the organization’s logical control, but physically reside in infrastructure owned and managed by another entity. [4]

Such issues give rise to tremendous anxiety about security risks in the cloud. Enterprises worry whether they can trust their employees or need to implement additional internal controls in the private cloud, and whether third-party providers can provide adequate protection in multitenant environments that may also store competitor data. There’s also ongoing concern about the safety of moving data between the enterprise and the cloud, as well as how to ensure that no residual data remnants remain upon moving to another cloud service provider.[4]

Unquestionably, virtualized environments and the private cloud involve new challenges in securing data, mixed trust levels, and the potential weakening of separation of duties and data governance. The public cloud compounds these challenges with data that is readily portable, accessible to anyone connecting with the cloud server, and replicated for availability. And with the hybrid cloud, the challenge is to protect data as it moves back and forth from the enterprise to a public cloud.[4]

Here the primary focus is needed on the area of storing the Data on the Foreign Machine, secondly to query encrypted data as much of data on the cloud can be encrypted.

Generally a cloud system should support efficient storage of encrypted sensitive data, store ,manage and query massive amounts of data, support fine-grained access control and should definitely support a strong authentication

4.3 Data Security and its Challenges:

Before potential cloud users are able to safely move their applications/data to the cloud, a suit of security services would be in place which we can identify as follows 1.Data Confidentiality assurance 2.Data integrity protection 3.Gurantee of data availability 4.Secure Data Access 5.Regulations and Compliances and 6.service audition[50]

A data security framework for cloud computing networks is proposed [6]. The authors mainly discussed the security issues related to cloud data storage. There are also some patents about the data storage security techniques [7]. Younis and Kifayat give a survey on secure cloud computing for critical infrastructure [8]. A security and privacy framework for RFID in cloud computing was proposed for RFID technology integrated to the cloud computing [9], which will combine the cloud computing with the Internet of Things.

In short, the foremost issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. The security challenges in the cloud include threats, data loss, service disruption, outside malicious attacks, and multitenancy issues [9]. Chen and Zhao [10] analyzed privacy and data security issues in the cloud computing by focusing on privacy protection, data segregation, and cloud security. Data security issues are primarily at SPI (SaaS, PaaS, and IaaS) level and the major

Challenge in cloud computing is data sharing.[5]

There are complex data security challenges in the cloud: [4] . First is the need to protect confidential business, government, or regulatory data

Second are Cloud service models with multiple tenants sharing the same infrastructure? Third is Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive. Fourth is Lack of standards about how cloud service providers securely recycle disk space and erase existing data, fifth is Auditing, reporting, and compliance concerns, sixth is Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management and lastly A new type of insider who does not even work for your company, but may have control and visibility into your data

V Data Storage and its issues

5.1 Data storage Encryption:

It is very important that sensitive data be in strongly encrypted form, because in the cloud data can be place anywhere. There is a need to use a secure Co- Processor infrastructure to enable efficient encrypted storage of sensitive data; this will help in system to handle encrypted data efficiently. The security Requirement implies that the software running on the secure co-processor should be kept as simple as possible. When the question of hardware comes, we can encrypt the sensitive datasets using random private keys and to alleviate the risks key disclosure we can use tamper-resistant hardware to store some of the encrypted/Decrypted keys (A master key which encrypts all other keys). An attacker cannot learn the keys by simply taking the snapshot of the system as they will not reside in the memory unencrypted at any time.[2]

5.2 Key management on data in the cloud

Data encryption before outsourcing to the cloud is a common and simple way to protect data privacy. Although the encryption algorithms are public, information encrypted under the algorithms is secure because the key used to encrypt the data remains the secret. As a result, key management is a critical element in the cloud computing .it is the ability to correctly assign, secure and monitor keys that defines the level of operational security provided by any encryption implementation [3]

5.3 Remote integrity Check on the data:

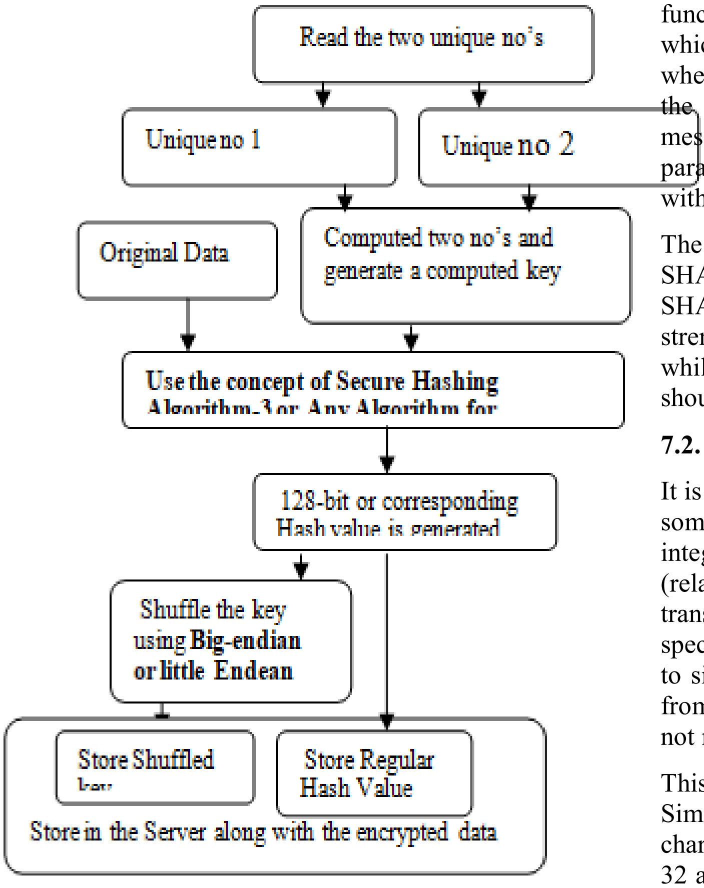
It is very common that store data in the remote cloud server. As the clients store their important data in the remote cloud server without a local copy, it is important to check remote data integrity. While it is easy to check data integrity after completely downloading the data it is large waste of communication bandwidth.[3]

VI Cryptographic algorithms for data Security:

A cryptographic algorithm named Diffie-Hellman is proposed for secure communication [11], which is quite dissimilar to the key distribution management mechanism. For more flexibility and enhanced security, a hybrid technique that combines multiple encryption algorithms such as RSA, 3DES, and random number generator has been proposed [11]. RSA is useful for establishing secure communication connection through digital signature based authentication while 3DES is particularly useful for encryption of block data. Besides, several encryption algorithms for ensuring the security of user data in the cloud computing are

discussed [12] and various other include Identity based authentication, RSA algorithm, Dynamic Intrusion detection system, Multi tenancy based access control model, TLS Handshake, Public key homomorphic, Third party auditor, probabilistic sampling technique, Diffle – Hellman key exchange, Private face recognition, MACs, Data coloring and water marking, A novel Cloud dependability model, KP-ABE, RBAC, ARVTM, Security assertion markup language, TPM, Proof of irretrievability, Fair MPNR protocol, Sobol sequence, Redundant array of independent Net storages, Handoop distributed file system, self cleansing intrusion tolerance, searchable symmetric encryption, Provable data possession, Privacy manager, Time bound ticket based mutual authentication other algorithms [27].

VII Proposed Unique keys Computed key Encryption Algorithm:


Read the two unique no's
Unique no 1
Unique no 2
Original Data
Computed two no's and generate a computed key
Use the concept of Secure Hashing Algorithm-3 or Any Algorithm for
128-bit or corresponding Hash value is generated
Shuffle the key using Big-endian or little Endean
Store Shuffled key
Store Regular Hash Value
Store in the Server along with the encrypted data

Flow Chart of the Proposed Algorithm

In this Algorithm we worked on the idea of taking two unique keys and working on them to generate a new key. With the use of these two different unique keys and on the computation of the unique keys we generate a new key(unknown to the user and others as well), the generated key along with the original data will be again computed using a algorithm(which is a kind of SHA algorithm) generates a 128 or corresponding bit hash value , upon the generated key we will apply a concept of Big-endian or Little-endian to shuffle the 128 bit generated key and store the regular generated 128-bit value as well as the shuffled key value in the server so as to provide data integrity to the users.

7.1 Secure hashing Algorithm

The process of SHA-3 standardization by NIST was completed in August 2015 and includes four hash functions with output lengths of 224, 256, 384 and 512 bits. In all these cases, the width is 1600 (i.e., the underlying permutation is Keccak-f[1600]) and the capacity is twice the output length. The capacity works as a security parameter, so that security is increased with higher capacities, but there is a security-efficiency trade-off and speed may be increased by using lower capacities. The function of SHA3 is implementation of the four hash functions in the SHA-3 standard. It is an indexed function which should be called in the form: SHA3 [n](message) where n is the output length in bits (which must be one of the following values: 224, 256, 384, 512), message is the message and there is an additional (optional) input parameter to specify the type of message (text, hex or file) with text the default.

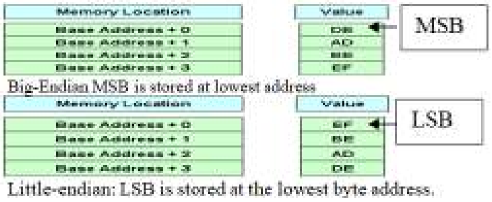
The next procedure implements the XOFs SHAKE128 and SHAKE256. These functions should be called in the form: SHAKE[n](message, d) where n is now the "security strength" of the function which must be either 128 or 256, while d represents the bit-length of the output, which should be a multiple of 8.

7.2. Mix Endianess:

It is a process of byte ordering in memory used to represent some king of data. Typical cases are the order in which integer values are stored as bytes in the computer memory (relatively to a given memory addressing scheme) and the transmission order over a network or other medium. When specifically talking about bytes, endianness is also referred to simply as byte order. Endianness is nothing but writing from left to right, right to left. However endianness does not matter in dealing with a sequence of single bytes.

This is the case with the strings encoded in the ASCII and Similar codes, where one byte corresponds to one character. Strings encoded with Unicode UTF-16 or UTF-32 are affected by endianness because in those a set of two or four bytes represents one character .Aarchitectures such as PowerPC, MIPS, and Intel's 64 IA-64 are Big-Endian, i.e. they are capable of operating in either Big-Endian or Little-Endian mode [13].

For a 32-bit number, 0xDEADBEEF.



Big-Endian MSB is stored at lowest address

Little-endian: LSB is stored at the lowest byte address.

VIII Conclusion:

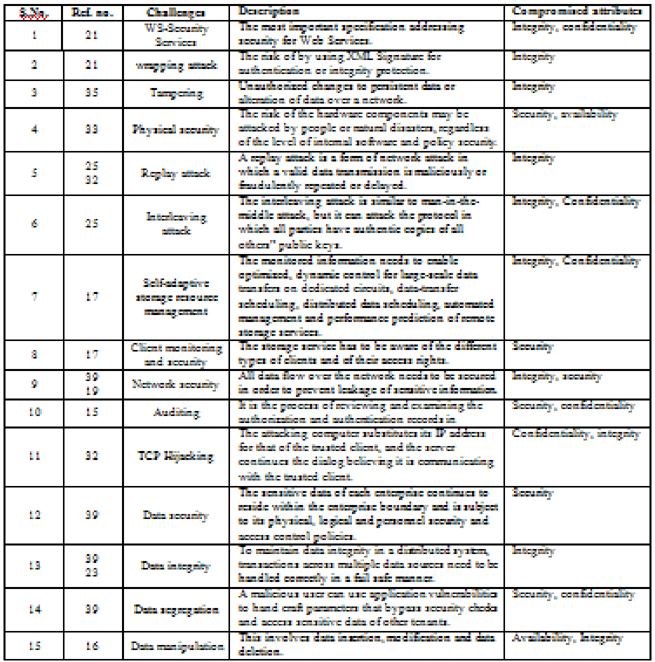
The above explained unique key (here unique mean every individual has a unique number and is secure), algorithm will provide and extra security feature for the cloud data, if we add one more unique key and compute them this will become more strong key and will help to encrypt our data and provide more security.

A deep survey is made on many published papers and identified various challenges, the compromised attributes and its description is listed as **List-1**.

Similarly a deep survey is made on the papers published and identified some techniques used for providing data security and integrity of the cloud data is listed as **List-2**

IX. Future Work:

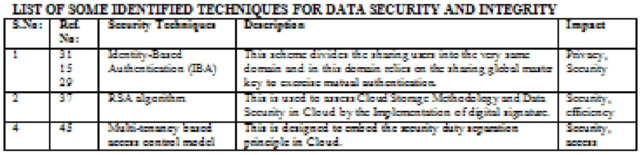
For the above explained algorithm the only problem is if anyone knows the unique keys and computation of those keys they can decrypt the data easily. If you can add the feature of facial recognition system are any iris recognition systems along with the unique keys for computation the encrypted data becomes more complex and if anyone want to decrypt the data it will become very difficult. More focus is needed on security challenges like Eaves dropping, Hypervisor viruses, Legal Interception point , Virtual machine security ,Trusted transaction , Risk of multiple Cloud tenants , Smart phone data slinging , Abuse and nefarious use of Cloud Computing ,Insecure application programming interfaces, Malicious insiders, Shared technology vulnerabilities, Service and traffic hijacking. These challenges need very high security algorithms.



S.No.	Ref. no.	Challenges	Description	Compromised attributes
1	21	WS-Security Services	The most important specification addressing security for Web Services.	Integrity, confidentiality
2	21	wrapping attack	The risk of by using XML Signature for authentication or integrity protection.	Integrity
3	35	Tampering	Unauthorized changes to persistent data or alteration of data over a network.	Integrity
4	33	Physical security	The risk of the hardware components may be attacked by people or natural disasters, regardless of the level of internal software and policy security.	Security, availability
5	25 32	Replay attack	A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.	Integrity
6	25	Interleaving attack	The interleaving attack is similar to man-in-the-middle attack, but it can attack the protocol in which all parties have authentic copies of all others" public keys.	Integrity, Confidentiality
7	17	Self-adaptive storage resource management	The monitored information needs to enable optimized, dynamic control for large-scale data transfers on dedicated circuits, data-transfer scheduling, distributed data scheduling, automated management and performance prediction of remote storage services.	Integrity, Confidentiality
8	17	Client monitoring and security	The storage service has to be aware of the different types of clients and of their access rights.	Security
9	39 19	Network security	All data flow over the network needs to be secured in order to prevent leakage of sensitive information.	Integrity, security
10	15	Auditing	It is the process of reviewing and examining the authorization and authentication records in.	Security, confidentiality
11	32	TCP Hijacking	The attacking computer substitutes its IP address for that of the trusted client, and the server continues the dialog believing it is communicating with the trusted client.	Confidentiality, integrity
12	39	Data security	The sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies.	Security
13	39 23	Data integrity	To maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner.	Integrity
14	39	Data segregation	A malicious user can use application vulnerabilities to hand craft parameters that bypass security checks and access sensitive data of other tenants.	Security, confidentiality
15	16	Data manipulation	This involves data insertion, modification and data deletion.	Availability, Integrity

List-2

LIST OF SOME IDENTIFIED TECHNIQUES FOR DATA SECURITY AND INTEGRITY



S.No:	Ref. No:	Security Techniques	Description	Impact
1	31 15 29	Identity-Based Authentication (IBA)	This scheme divides the sharing users into the very same domain and in this domain relies on the sharing global master key to exercise mutual authentication.	Privacy, Security
2	37	RSA algorithm	This is used to assess Cloud Storage Methodology and Data Security in Cloud by the Implementation of digital signature.	Security, efficiency
4	45	Multi-tenancy based access control model	This is designed to embed the security duty separation principle in Cloud.	Security, access

List-1

List-2

LIST OF SOME IDENTIFIED TECHNIQUES FOR DATA SECURITY AND INTEGRITY

		(MTACM)		control
5	21 25	TLS Handshake	It is designed to exchange the evidence in the data transaction, which removes the ambiguities that lead to repudiations or disputations between the user and service provider.	security
8	30	Probabilistic sampling technique	This aims to consider secure data storage, computation and privacy preserving together.	Security, privacy
9	48 38	Diffie-Hellman key exchange	It describes protocol between Cloud service provider and the user for secretly sharing a symmetric key for secure data access.	Security, access control
13	27	Data coloring and software water marking techniques	This lets us segregate user access and insulate sensitive information from provider access.	Performanc e, security
14	17 25 43	A novel Cloud dependability model	This involves enhancing the security of heterogeneous Cloud environments. System-level virtualization techniques are used to enhance the dependability of Cloud environments.	QoS, security
16	36 22	Proxy Re-Encryption (PRE)	This is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under user1 public key into another cipher text that can be opened by user2 private key without seeing the Underlying plaintext.	Performanc e, security
18	46	Application-oriented Remote Verification Trust Model (ARVTM)	This model is capable of adjusting the user"s trust authorization verification contents according to the specific security requirements of different applications, and dynamically adjusting the user"s trust value with the trust feedback mechanism to determine whether or not the requested resource or service should be provided.	Qos, security
20	49 18 28	Trusted Platform Module (TPM).	This involves which Cloud Computing system is combined with Trusted Platform Support Service (TSS) to obtain authentication.	Qos, security
22	24	Fair MPNR protocol	This solves the problem of fair non-repudiation and roll back attack. Each message consists of specified data transmission information as evidence.	Security, performance
23	40	Sobol Sequence	This involves The numbers are generated sequentially to fill the larger "gaps" in the Pseudorandom Data to address data storage security in Cloud Computing.	Security, performance , efficiency
26	34	Self-Cleansing Intrusion Tolerance (C-SCIT)	This describes a recovery-based intrusion tolerance scheme leveraging Cloud Services from multiple vendors.	Security, privacy
27	44	searchable symmetric encryption (SSE)	This involves to allow the data owner to outsource his data in an encrypted manner while maintaining the selectively search Capability over the encrypted data.	Security, privacy, performance
28	31	Provable data possession(PDP)	This involves allowing a client that has stored data at a un trusted server to verify that the server possesses the original data without retrieving it.	Security, performance , efficiency
29	20	Time bound ticket based mutual authentication scheme	This involves achieving mutual authentication between the server and the client, this scheme reduces the server"s processing overhead efficiently.	Efficiency, security, performance
30	47	Security Access Control Service (SACS)	This includes Access Authorization, Security API and Cloud connection Security.	Security
32	26	Intrusion detection	Leads to effective	Efficiency,
34	41,42	Identity Management	users and services based on credentials and characteristics	Security

References:

1. Peter Mell. (2011) 'The NIST Definition of Cloud ', Reports on Computer Systems Technology, sept., p. 7.

2. Security Issues for cloud computing: Technical report UTDCS-02-10, University of Texas at Dallas.

3. Data Security and Integrity in the cloud computing by Miao Zhou, university of Wollongong,
4. Data Security in cloud ; Protecting business-critical information in private, public and hybrid cloud environment.
5. A. Pandey, R. M. Tugnayat, and A. K. Tiwari, "Data Security Framework for Cloud Computing Networks," International Journal of Computer Engineering & Technology, vol. 4, no. 1, pp. 178–181, 2013.
6. D. A. Klein, "Data security for digital data storage," U.S. Patent Application 14/022,095, 2013.

LIST OF SOME IDENTIFIED CHALLENGES FOR DATA SECURITY AND INTEGRIT

7. M. Y. A. Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: a survey," Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013.
8. S. Kardas¸, S. C¸elik, M. A. Bing¨ol, and A. Levi, "A new security and privacy framework for RFID in cloud computing," in Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom '13), Bristol , UK,
9. A. Behl, "Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation," in Proceedings of the World Congress on Information and Communication Technologies (WICT '11), pp. 217–222, IEEE, December 2011.
10. D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), vol. 1, pp. 647–651,Hangzhou, China,March 2012.
11. D. Boneh, "The decision Diffie-Hellman problem," in Algorithmic NumberTheory, vol. 1423, pp. 48–63, Springer, 1998. [p11] A. Kaur and M. Bhardwaj, "Hybrid encryption for cloud database security," Journal of Engineering Science Technology, vol. 2, pp. 737–741, 2012.
12. R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," International Journal of Engineering Research and Applications, vol. 3, no. 4, pp. 1922–1926, 2013.

13. Advanced Research on Electronic Commerce, Web Application, and Communication: International Conference, ECWAC 2011, Guangzhou, China, April 16-17, 2011. Proceedings,

14. Top Strategic Predictions for 2016 and Beyond: The Future Is a Digital Thing Published: 2 October 2015.

15. Almulla S, Chon Yeob Yeun. (March 2010) 'Cloud Computing Security management ', 2nd International Conference On Engineering Systems Management and Its Applications , 1-7.

16. B. lagesse. (Mar.2011) 'Challenges in Securing the Interface between the cloud and Pervasive Systems', 2011 IEEE International Conference on Pervasive Computing and Communications Workshops, 106-110.

17. Dawei Sun, Guiran Chang. (Sept.2010) 'A Dependability Model to Enhance Security of Cloud

Environment Using System-Level Virtualization Techniques', Pervasive Computing Signal Processing and Applications, 305-310.

18. Doelitzscher F, Reich C. (July 2010) 'Designing Cloud services adhering to Government privacy Laws ', IEEE 10th International Conf. on Computer and Information Technology, 930-935.

19. Ford R.B. (2011) 'Information Security in the Cloud', Network Security, vol. 2011, no. 4, April, pp. 15-17.

20. Hao Z, Zhong S. (June,2011) 'A Time-Bound Ticket-Base Mutual Authentication Scheme for Cloud Computing', International Journal of Computers, Communications and Control, vol. 6, no. 2, June, pp. 227-235.

21. Jensen M, Schwenk J. (Sept.2009) 'On Technical Security Issues in Cloud Computing', IEEE International Conference on Cloud Computing, 109-116.

22. Jia Weiwei Zhu, Haojin Cao. (10-15 April, 2011) 'A Secure data service mechanism in mobile Cloud Computing', Computer Communications Wrokshops (INFOCOMWKSHPS), IEEE Conference 2011, 1060 - 1065.

23. Jun Feng, Yu Chen. (Jan 2010) 'Bridging the Missing link of Cloud data storage security in AWS ', 7th IEEE conf. on Consumer Communications and Networking Conference (CCNC), 1-2.

24. Jun Feng, Yu Chen. (Jan 2011) 'Enhancing Cloud storage security against rool- back attacks with a new fais multi party non-repudation protocol', Consumer Communications and Networking Conference (CCNC), IEEE conference 2011, 521-522.

25. Jun Feng, Yu Chen. (Sept 2010) 'Analysis of Integrity Vulnerabillities and a Non repudation Protocol for Cloud Data Storage Platforms', 39th International Conf. on Parallel Processing Workshops (ICPPW), 251-258.

26. Jun-Ho Lee, Min-Woo Park. (feb. 2011) 'Multi level Intrusion Detection System and Log management in Cloud Computing', Advanced Communication Technology (ICACT), 13th International Conference 2011, 552-555.

27. Kai Hwang, Deyi Li. (2010) 'Trusted Cloud Computing with Secure Resources and Data coloring', Internet Computing, vol. 15, no. 05, October, pp. 14-22.

28. Kai Zhang, Ying Song. (july,2010) 'Trusted Connection System based on Virtual Machine Architecture', 3rd IEEE International Conference on Computer Science and Information Technology, 192-196.

29. Lifei wei, haojin Zhu. (June.2010) 'SecCloud: Bridging Secure Storage and Computation in Cloud', 30th International Conference on Distributed Computing Systems Workshop, 52-61.

30. Lin Weiwei, Chen Liang. (Juy 2011) 'A hadoop Based Efficient Economic Cloud storage system', Communications and Systems (PACCS), 3rd Pacific - Asia Conference on Circuits, 1-4.

31. Lishan Kang, Xuejie Zhang. (Nov.2010) 'Identity-Based Authentication in Cloud Storage Sharing', Multimedia Information networking and Security, 851-855.

32. L. Savu. (May.2011) 'Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges', International Conference on Computer and Management, 1-4.

33. Mathisen, Eystein. (may 31, 2011) 'Security challenges and solutions in Cloud Computing', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference, 208-212.

34. Nguyen Q, Sood A. (June 2011) 'Designing SCIT architecture pattern in a Cloud based Environment ', 41st International Conf. on Dependable Systems and Networks workshops, 123-128.

35. Saripalli P, Walters B. (July 2010) 'A Quantitative Impact and Risk Assessment Framwork for Cloud Security ', 3rd International Conference on Cloud Computing, 280-288.

36. Shucheng Yu, Cong Wang. (March 2010) 'Achieving secure Scalabe and Fine grained data access control in Cloud Computing ', IEEE Conference INFOCOM , 1-9.

37. Somani U, Lakhani K. (Oct 2010) 'Implementing Digital signature with RSA Encryption algorithm to enhance the data security of Cloud in Cloud Computing', 1st International Conference on Parallel Distributed and Grid Computing , 211-216.

38. Srinivasatava Prashant, Singh Satyam. (June 2011) 'An Architecture based n Proactive model for Securrity in Cloud Computing', International conference on recent Trends in Information Technology (ICRTIT), 661-666.

39. Subashini S, Kavitha V. (2011) 'A Survey in Security issues in service delivery models of Cloud Computing', Journal of Netwrok and Computer Applications, vol. 34, no. 1, Jan, pp. 1-11.

40. Syam kumar P, Subramanian R. (Oct 2010) 'Ensuring data storage security in Cloud Computing using Sobol sequence', 1st International Conference on Parallel Distributed and Grid Computing (PDGC), 217-222.

41. Takabi H, Joshi J. (2010) 'Security and Privacy challenges in Cloud Computing Environment', Security & Privacy, IEEE , vol. 8, no. 6, December, pp. 24-31.

42. Takabi H. (July.2010) 'Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments', IEEE 34th Annual Computer Software and Applications Conference Workshops, 393-398.

43. Tie Fang Wang, Baosheng Ye. (July 2010) 'Study on enhancing performance of cloud trust model with famiy gene technology', 3rd IEEE International conf. on Computer Science and Information Technology (ICCSIT), 122-126.

44. Wang Cong, Cao Ning. (June 2010) 'Secure Ranked keyword serch over Encrypted Cloud data ', IEEE 30th International conf. on Distributed Computing Systems (ICDCS), 253-262.

45. Xiao Yong Li, Yong shi. (Dec 2010) 'Multi Tenancy Based Access Control in Cloud', International Conf. on Computational Intelligence and Software Engineering (CiSE), 1-4.

46. Xiaofei Zhang, Hui Liu. (Nov 2010) 'Application Oriented Remote Verification Trust Model in Cloud Computing ', 2nd International Conf. on Cloud Computing Technology and Science, 405-408.

47. Xue Jing, Zhang Jian-jin. (Aug. 2010) 'A Brief Survey on the Security Model of Cloud Computing', 9th International Conf. on Distributed Computing and Applications to Business Engineering and Science (DCABES)l, 475 - 478.

48. Zhang Jianhong, Chen Hua. (Sept 2010) 'Security storage in the Cloud Computing: A RSA based assumption data integrity check without original data', International Conf. on Educational and Information technology (ICEIT), 143-147.

49. Zhidong Shen, Li Li. (May 2010) 'Cloud Computing System Based on Trusted Computing Platform', Intelligent Computation Technology and Automation (ICICTA), 942-945.

50. Data Security in cloud Computing: by Shucheng Yu1, Wenjing Lou2, and Kui Ren3

51.