An Efficient Enhanced Algorithm to Diminish the Cyber Security Threats in Multi-Tenancy Cloud Computing

[1]SHEELA RINI.A, [2]Dr.MEENA.C

[1] Research Scholar, Avinashilingam Institute for Home Science & Higher Education for Women ,
[2] Head, Computer Center, Avinashilingam Institute for Home Science & Higher Education for Women
[1]sheelarini.a@gmail.com , [2] cccmeena@gmail.com

Abstract*— Cloud computing is considered as the hopeful standard for distributing IT facilities as computing benefits. Several industries like banking, healthcare and education are moving towards the cloud due to the effectiveness of services provided by the pay-per-use pattern based on the resources equivalent to process power used, transactions administered, bandwidth consumed, knowledge transferred, or storage space occupied etc. Cloud computing is totally in web dependent technology wherever client data is kept and maintained within the cloud provider's data center like Google, Amazon, Microsoft, Akamai, etc. Inadequate control over the data may procure several security concerns and threats which include data leakage, insecure interface, sharing of resources, data availability and insider attacks, which leads to cyber crimes in cloud environment. On the off chance that the organizations and clients are given web get to, they can get to their own records specifically from any side of the world. This innovation supports fruitful computing by coordinating information storage, processing and transfer speed.. In Cloud, security of information isn't ensured and even the information can likewise be gotten to by the third party. There is a need to Consequently, we have planned a protected document stockpiling framework with effortlessness, legitimacy and security. Nearly it is connected in everything which required giving consent to just affirmed approvals Consequently, we have planned a protected document stockpiling framework with effortlessness, legitimacy and security. Nearly it is connected in everything which required giving consent to just affirmed approvals on averting information release, warning for security mischance and security occurrence reviews. Cloud security needs to be enriched with the conventional methods like firewalls, Virtual Private Networks (VPN) and Security policies to get a carefully designed ripe administration from it. In any case, Cloud computing brings new difficulties, issues and dangers to the business. From many research it is observed that security is the main problem of cloud adoption. The dread of losing control of corporate information and the danger of data breaches in the cloud can possibly disturb the adoption of cloud services. Security issues must be addressed and new technologies must be produced in order to open cloud computing benefits. For retrieving the data in the cloud, clients need more security for guarding their data. Encryption and Hashing technique is being used in the cloud environment by carrying a key exchange process done with key encryption key and data encryption key to provide security. Also SHA3 hashing function is used for accomplishing data integrity and security in the cloud. This Proposed method looks in to an attack model based on threat model to overcome the Multi-tenancy situation. Additionally, resource allotment method will accomplish the balance between both the advantages gained from Multi-Tenancy and Security. To minimize the security threats and preserve the privacy, reliability and authenticity of data which is stored in cloud, Encryption and hashing techniques will be used.

Consequently, we have designed a protected file storage system with effortlessness, legitimacy and security. Nearly it is connected in everything which required giving permission to just certified authorizations. In the database, the password is stored as a message digest. This sort of storing password should be carefully designed. The encryption procedure makes the data secure and it prevents clarity by unauthorized persons and furthermore it sets up a system to remove imposture. This system has been designed in such a way, if the one-way hash function gets cracked, it will lead to get the encrypted data alone. The usage of hash function makes impossible for any overlooked changes on data. After the deployment of RSA and SHA3 (Keccak) before Storage, the data becomes impervious to access or changes by any third party and to the capacity framework.

In this manner by creating a two factor security verification of data which is stored in cloud will be a protected environment for the multitenant users to protect their data from cyber crimes. This will help the clients information to be more secured in the cloud platform.

Index Terms — *Cloud Computing, Cyber Security, Multitenancy, RSA, SHA-3, Keccak*

I. INTRODUCTION

Cloud Server is the framework which is supporting Web Service. The meaning of cloud server can have different view point, the most prevalent one are arranged by Infrastructure as a service (IAAS), Platform as a Service (PAAS), Software as a Service (SAAS) proposed by US NIST[X] and public cloud, private cloud, hyper cloud and some different categories, additionally computing, networking, storage capacity of a system viewpoint or utilizing, archiving and transmission from a data viewpoint (Chan et al., 2014).

Cloud computing which is the following phase of internet development guarantees adaptability and elasticity of the framework. The barrier or anxiety for adopting Cloud Computing in enterprises demonstrates that security and accessibility which is one of the data security standards are concerns. Such problems are solved by Multi-Tenancy and Cloud nature of shared assets. The threat of information bargain increments in the Cloud, because of the expanded number of parties accessing the data in a particular platform with the separation of use/data by bucket system. Various concerns emerge regarding the issues of Multi-Tenancy and data in the cloud. Multi-Tenancy refers to resource sharing in cloud where any resource object is reusable in the cloud this itself describes that multi-tenancy is a basic dispute of cloud computing and its related risks, where privacy and/or reliability could be violated. Yet, there are more risk exists for the data, since it is utilized by several tenants.

The mixture of encryption and hashing algorithms are utilized to limit the security dangers. Encryption is an exciting piece of technology that work by mix up data so it is unreadable by unintended gathering. RSA is a public key encryption algorithm and the standard for encoding data sent over the internet.

Hash values are used to make sure that the data values are unmodified which results to a secured system The sender makes the hash an incentive for the message, encodes it, and sends it alongside the message. The receiver at that point decodes both the message and the hash and delivers another hash from the unscrambled message. In the event that both the hashes are the same, at that point it displays that the information isn't changed at the period of transmission. Hash makes a 128-bit process for the message verbalized as content. The SHA3 approach is projected for the same. As cyber attacks are constantly emerging, it is a need for launching many cryptographic techniques to ensure the email communication or stored data and also to limit the security risks in a cost efficient way.

II. LITERATURE REVIEW

This research work focus on multi-tenancy in cloud computing with security features. In particular, enhanced access control technique is used to minimize the security risks in cloud computing.

Brown et al.,(2012) proposed an architecture where Multi-tenancy introduces unique security risks to cloud computing as a result of more than one tenant utilizing the same physical computer hardware and sharing the same software and data. This paper proposed to explore the specific risk in cloud computing due to multi-tenancy and the measure can be taken to mitigate those risks. These paper shows that the security risks that have surfaced in the cloud computing model, as a result of multi-tenant Architecture (MTA), and as a result of MTA being implemented by cloud Service provider (CSPs). The multi-tenant systems allow the service provider to pass savings on to the user thus reducing their overall operating costs and indeed their total cost of ownership. The user must be aware of the risks and intentional in their efforts to take appropriate counter measures such as Governance, Control and Auditing configuration, Design and change management, logical Security, Access control and Encryption.

Aijahdah et al. (2014) proposed a model in cloud computing, in which security is considered as one of the most critical concerns for the large customers of cloud. Such valid concern is mainly driven by the multi-tenancy situation which refers to resource sharing in cloud computing and its associated risks when confidentially and/or integrity could be violated. This paper presents the uniqueness about multi-tenancy in cloud computing in which both the attackers and the victim are sharing the same server. Such step cannot be mitigated by traditional security techniques and measures because it is not designed to penetrate inside servers and their monitoring techniques. It also proposes a system model and a resource allocation techniques that will achieve the balance between both security and the benefits gained from multi-tenancy.

Zhan Chan et al. (2014) presented that cloud computing is rapidly changing the face of web Internet service infrastructure, enabling even small organization to quickly create web and mobile application for millions of users by taking advantage of the scalability and flexibility of the shared physical infrastructure provided by cloud providers. In this scenario, multiple tenants saved their data and application in the same data centers making the network boundaries between each tenant become blurred. This paper presents the physical gateway have been replaced by virtual logical boundaries between tenants, it repairs a firewall, IDS/IPS and other devices to collaborate with the traffic controller, to adapt the performance and safety requirements of each tenant or security domain, security boundary dynamics caused by virtual machine migration, as well as the dynamic security requirements of virtual machines on the demand. It uses VCNSMS for flexibility and scalability to protect multiple tenants with different security policy and security requirements.

Pansotra et al. (2015) quoted that every third person is using cloud computing directly or indirectly for eg. Email, most commonly used application of cloud computing, you can access your mail anytime anywhere. So it is very important for the company to secure that data which makes confidentiality, availability and integrity. This paper shows the symmetric key algorithms in which a single key is used for encryption and decryption where as RSA, Diffie-Hellman Key exchange and homographic equations are asymmetric, in which two different keys are used for encryption and decryption. These algorithms are not secure; there is a need to enhance the security algorithms. So the security of cloud make very strong.

Chidambaram et al. (2016) observed that the data is stored in the cloud can be sensitive and at times needs a proper file storage system with a tough security algorithm. This paper proposed a secure storage system for a cloud which is an open shareable elastic environment. The files stored in the cloud are encrypted with RSA algorithm and digital fingerprint for the same has been generated through SHA3 message digest before storage. The RSA provides unreadability of data and SHA3 makes it impossible for any changes of data. After the application, data is secured by of RSA and SHA3 before storage, the data becomes resistant to access or modifications by any third party and the intruders of cloud storage system. The system has been designed in such a way that this one way hash function, if even cracked, will lead to getting encrypted data only.

When moving workloads to the cloud, enterprises need to extend their security management into the cloud and maintain control of their data in order to protect intellectual property, sensitive information and brands, while continuing to pass security audits. Government agencies are also modifying regulations and policies to cover the cloud and virtualization environments, in general. The data in a virtualized cloud environment are also subject to regulatory compliance requirements such as PCI (Payment Card Industry) and HIPAA (Health Insurance portability and Accountability Act). Several new government cloud computing recommendations clearly state that cloud service consumers are responsible for compliance with these regulations. For example, US NIST states that “when data or processing is moved to a cloud, the consumer retains the ultimate responsibility for compliance”. UK ICO states in its Guidance on the use of cloud computing” that cloud service consuming organizations will continue to be data controllers and will be required to meet their obligations under the Data Protection Act. Failing to protect data in the cloud will result in damage to the enterprise’s brand, loss of intellectual property and competitive advantage, and significant financial cost related to litigation and penalties. According to

Ponemon, the average cost of a data breach event was $ US5.5 million in 2011.

Therefore, the first challenge of cloud security is how to protect cloud consumers' data in a multi-tenant environment from other side attacks launched by other malicious tenants and from "insider" attacks launched by the malicious cloud administrators, and to provide a mechanism for cloud consumers to control their data and meet compliance requirements.

III. SCOPE AND METHODOLOGY

This paper focuses on security issues and new cloud security techniques to be developed to unlock cloud computing benefits for multi-tenant clouds and virtualization environment.

Virtualization Infrastructure: Workloads typically ran on a virtualized infrastructure consisting of virtual server, virtual networks and virtual storage.

Multi-tenancy: Multiple cloud service can share the same hyper visor, the same physical server, network storage.

Protecting data and maintaining control in multi-tenant cloud Enterprises have spent many years building solid processes, scalable procedures and internal systems expertise to make their data centers secure, reliable and manageable in order to be compliant with business and regulatory requirements.

A. Existing System

This framework is to enhance the cloud information security by joining different cryptographic strategies. To give sealed confidentiality, encryption and decoding modules are included. Moreover integrity of information is additionally checked utilizing message process. And the data is protected by hashing technique and stored in the DB. The algorithm used here for encryption can't be broken effortlessly including the mainstream dictionary attack. Brute force attack is additionally hard to perform. This algorithm contains self-satisfaction and to guarantee security for the customers of the cloud. Despite the fact that cloud isn't reliable utilizing the proposed encryption of information and by hashing it can be put away in the cloud solidly. The proposed architecture is shown below.

Public Key Cryptography is being used, with asymmetric key RSA algorithm. In Public Key Cryptography the key for both the encryption and decryption process will be using different keys. Here encryption is done with the public key and by decryption is done with private key (Fig.1). So this can be an appropriate RSA encryption technique for the cloud environment.

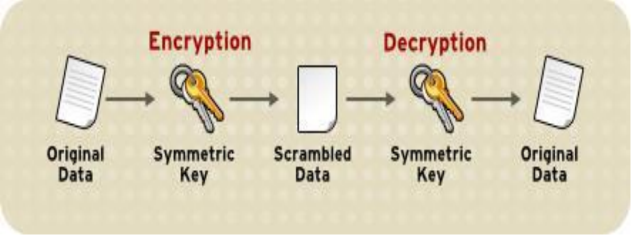


Fig.1: Encryption and Decryption

RSA: Key Generation technique

1) Select two random prime numbers which ought to be unique. Assign values to the variables (a and b) both should have similar bit length.

2) Calculate n=ab, where 'n' is the number usedutilized as the modulus for private and public keys. Key length is equivalent to 'n' length.

3) Now calculate. $\psi(n)=(a-1)(b-1)$

4) Select an integer Ke It should satisfy 1< Ke < $\psi(n)$. GCD of p and $\psi(n)$ should be equal to 1; that is Ke and $\psi(n)$ are coprime. Now is the public key component.

5) Compute Kd. Ke is proportionate 1(mod. $\psi(n)$).Kd. Is the private key component and it should be kept secret.

6) Ke and n are broadcasted to the community for encryption.

7) Cipher text, and modulus are used, for decryption,. With q and $\psi(n)$ decryption key is calculated called private key Kd and must be kept secret.

SHA3 hash work calculation has been utilized to generate the message process. The SHA3 message process calculation creates 16-byte hash an incentive in content arrangement as 32-digit hexadecimal number. SHA3 has been utilized in an assortment of zones, fundamentally used to check the information uprightness in the cryptographic area. Cryptographically solid process calculation creates an about exceptional advanced unique finger impression esteem from any source string. Little change in the message prompts the transcendently unique hash. SHA3 even delivers a hash for zero-length string.

Pseudo Code: Consider the following:

(1) The information message is separated into squares of 512 bits. In the event that the aggregate number of bits isn't the various of 512, at that point the cushioning of bits will be finished.

(2) Padding is done in the accompanying format: First, single piece "1" is added to the end and zeros are cushioned to make message length as 64 bits not exactly the various of 512.

(3) The last square speaks to the first message length.

(4) The SHA3 calculation uses 4 affixing factors of 32-bit length.

(5) There are four fundamental capacities which utilize the above state factors and info message to deliver the message process. The capacities are as per the following:F(B,C,D) = (B & C) | (~B &D),

G(B,C,D) = (B & D) |(C&~D),

H(B,C,D) = B^C^D,

I(B,C,D)=C^(B|~D),

Note: &,^ , | and ~ denotes bitwise AND, XOR, OR, and NOT operations, respectively. These four functions are connected to all the individual 512-piece bit blocks. At last, the process is stored in the factors A, B, C and D.

B. Proposed Architecture

In this proposed technique public key framework (RSA) is utilized where two distinctive keys are utilized one for encryption and the other for decoding. To break the framework factoring "n" is required, where n is the product of two prime numbers. RSA framework is hard to hack since speculating of two extensive prime numbers in the key space is complex.

With SHA3 calculation speedier avalanche effect is achievable; that is, little change in the message prompts the dominatingly extraordinary hash. SHA3 even creates a hash for zero-length string. Here the length of hash is 128 bits, along these lines, for birthday assault, 264 arbitrary records should be attempted. The main purpose of hash functions in Cryptography is to produce digital signatures, and they can be used to protect passwords in a user database. RSA algorithm is used for encryption which relies on the computational difficulty of factoring large integers. As computing power increases and more efficient factoring algorithms are discovered, the ability to factor larger and larger numbers also increases. Encryption strength is combined with the hash function SHA will be more powerful to reduce the security risks in cloud computing. It can be noted that some recent variants of RSA the encryption algorithm internally use hash function. Hash functions are good "randomization" and this makes them appropriate for building more elaborate cryptographic algorithms with good security features. Hash (SHA) is to ensure data integrity and encryptions (RSA) is for data confidentiality. They are used in conjunction to make sure the data is not being tempered with and only the authentic member is able to access it. So this way the confidentiality, Integrity and authenticity of the database are maintained in the multi-tenancy environment in cloud computing.

This way a threat model is identified with the combination of RSA and SHA algorithms will give the better accuracy and CIA (Confidentiality, Integrity, Authenticity) is maintained to reduce the security risks of multi-tenant environment in cloud computing. In this proposed approach both RSA and SHA3 highlights were joined together so complexity expanded towards hacking. Along these lines, contrasted and the accessible writing, the most extreme level of security with tamper resistance for document storage in the cloud will be accomplished.

The Keccak: The SHA-3 New Encryption Algorithm

The United States government has chosen the Keccak algorithm as a novel SHA-3 Encryption algorithm after passing through a number of long stretches of Testing and Analyzing.

Keccak Algorithm was adopted by the National Institute of Standards and Technology (NIST), in October 2012 as the new SHA-3 Encryption Standard. Keccak presents many advantages viz., better resistance and high performance behavior.

The research paper centers on a incisive look at Keccak's mechanism. It examines its engine and perceives how it furnishes the message content into a hash. It also makes a comparison of keccak with SHA-1 and SHA-2.

Limitations of SHA-1 and SHA-2

The SHA-1 and SHA-2 employ the same engine, called Merkle-Damgard, to manipulate message text which poses a major problem.

This implies that a competent attack on SHA-1 turns into a potential danger on SHA-2. For instance, in SHA-1, brute force attack mostly takes approximately 280 rounds to find a collision if a full-round SHA-1is used. In February 2005, Xiaoyun Wang and his peers employed a differential path attack to pull down a full-round SHA-1, and it took only 269 cycles to achieve success. The same attack was later justified by Martin Cochran in August 2008.

In the year 2012, Mark Stevens adopted an enhancement of cloud server in order to lay out a differential path attack on SHA-1. His attack resulted in a closer impact after 258.5 rounds. He also evaluated that altered attack can deal with a full impact after 261 cycles.

When we consider SHA-2, the major successful attacks were those that were incorporated against a restricted round SHA-2 hash. The best attack reported was against a 46-round SHA-2 (512-bit variant) and against a 41-round SHA-2 (256-bit variant). It took around 2253.6 cycles to crack the 256-bit variant and 2511.5 cycles for the 512-bit variant.

It is clear from the facts that, while no booming attacks against a full-round SHA-2 have been reported, there is almost certainly that attacking methods are being created in person. The above fact formed the motivation for NIST to support the SHA-3 competition, which in turn led to the development and ongoing adoption of Keccak.

High Level Description of Keccak

Clients have selected some parameters to be used in the keccak. NIST didn't made any official conclusion that which parameters will be used for the SHA-3 standard, at the time of creating the Keccak. A focal necessity by means of NIST meant for the SHA-3 hash function was the help of the following output lengths:

- 256 bits
- 384 bits
- 512 bits

Additionally Keccak permits the generation of many output bits randomly. Totally this is different as of the functionality of SHA-1 and SHA-2 that will produce fixed length bit block. In this viewpoint, sha-3 uses two principle modes:

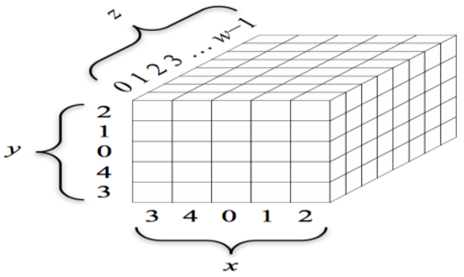
SHA-2 Replacement Mode

Here, SHA-3 creates a fixed -length yield of 224,256,384, or 512 bits.

Variable-length Output Mode

It permits to utilize SHA-3 for the creation of numerous output bits randomly. There are numerous applications in cryptography, For e.g., when utilizing Keccak as a stream cipher for producing pseudo-random bits.

SHA-3 is a family of sponge functions characterized by two parameters, the bitrate r and capacity c. The sum, r + c determine the width of the SHA-3 function permutation used in the sponge construction and is restricted to a maximum value of 1600. Selection of r and c depends on the desired hash output value. Ex.: for a 256-bit hash output r = 1088 and c = 512 and for 512-bit hash output r = 576 and c = 1024 is selected. The 1600-bit state of SHA-3 consists of a 5x5 matrix of 64-bit words. as shown in Fig. 2.



$0 \leq x, y \leq 4$

$0 \leq z \leq 63$

Fig.2: State Matrix of SHA-3

The Keccak-f Function (or the Keccak-f Permutation)

There are 24 rounds in the compression function (Core) of SHA-3 and each round consists of 5 steps, Theta (θ), Rho(ρ), Pi(π), Chi (χ) and Iota (i) as shown in the below in eq. (1) to (6).

Theta (θ) Step: ($0 \leq x,y \leq 4$)

$$C[x] = A[x,0]\oplus A[x,1]\oplus A[x,2]\oplus A[x,3]\oplus A[x,4]; \qquad \textbf{(1)}$$

$$D[x] = C[x-1]\oplus ROT(C[x+1],1) \ ; \qquad \textbf{(2)}$$

$$A[x, y] = A[x, y]\oplus D[x]; \qquad \textbf{(3)}$$

Rho (ρ) and Pi (π) Step: ($0 \leq x,y \leq 4$)

$$B\ [y, 2x+3y] = ROT\ (A[x,y], r[x, y]); \qquad \textbf{(4)}$$

Where r [x, y] is the Cyclic Shift Offset

Chi (χ) Step:(0 ≤x, y≤ 4)

$A[x, y] = B[x,y] \oplus ((NOT B[x+1,y]) AND B[x+2,y]);$ **(5)**

Iota (i): $A[0, 0] = A[0, 0] \oplus RC$; **(6)**

Keccak does not depend on Merkle-Damgard construction like SHA-1 and SHA-2. An incredible hash function relies upon what is known as a sponge construction. After the process of pre-processing which isolates the message into squares and creates padding , the sponge construction includes two phases:

Absorbing (Input) Phase

The message blocks Xi gets passed into the algorithm for calculation and handled.

Squeezing (Output) Phase

An output of adaptive length is processed.

Figure 3 shows the high-level diagram of Keccak. The same function is being utilized by both the phases. This function is named as keccak-f.

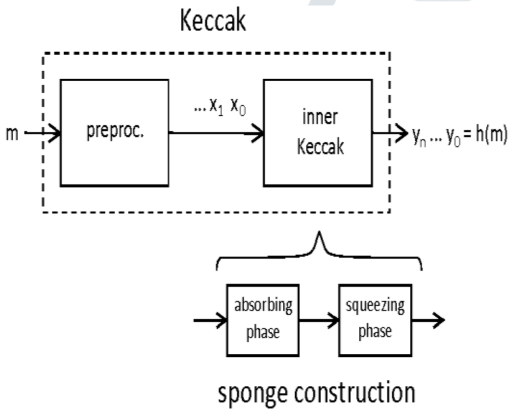


Fig.3: High level Depiction of Keccak

The figure 4 exhibits how the sponge construction peruses in the input blocks xi and how the output blocks yj are produced. The sponge construction licenses arbitrary length outputs y0….yn.

At the point when SHA-3 is utililzed as SHA-2 substitution simply the first bits of the first output square y0 are required.

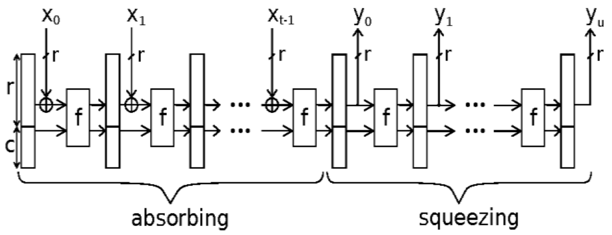


Fig.4: The sponge construction's Absorbing & Squeezing phases

The measure of input and output block and additionally the safety level of keccak can be designed by a few parameters. The comparing parameter b is the width of the state,

i.e., b = r+c.

b thus relies upon the exponent l and can take the accompanying qualities: b = 25 · 2 l , l = 0,1,...,6

b (State) [bits]	r [bits]	c [bits]	Security level [bits]	Hash output [bits]
1600	1344	256	128	224
1600	1344	256	128	256
1600	1088	512	256	384
1600	1088	512	256	512

Table 1: The Parameters of SHA-3 when utilized as SHA-2 substitution

IV. CONCLUSION

The combined usage of RSA and SHA-3 (Keccak) will reduce the cyber security risks in the cloud environment. As sharing of information is happened in multi-tenancy environment, there is more cyber security risks. So in order to avoid that, this powerful algorithm will prove the security and privacy and portability of the system. In this way confidentiality, Integrity and authenticity of the system will be maintained so that multi supplier and hybrid security, management and governance plus Business analytics for cloud will be improvised. creation a multi-tenancy application will upgrade the process becomes significantly more simple with a multi-tenant application the process for spinning up a new cloud application is incredibly easy and can be done very quickly. Also provision of additional layer to allow for customization while still maintaining is underlying code base remains constant for all users. The proposed output may give the result of minimized the security risks in a day to day activity. The speed and time schedule may increases.

REFERENCES

[1] Aljahdali, H., Albatli, A., Garraghan, P., Townend, P., Lau, L and Xu., J. (2014), Multitenancy in cloud computing, Service Oriented System Engineering (SOSE), IEEE, 8th International Symposium

[2] Brown, J., Anderson, V and Tan, Q. (2012), Multitenancy - Security Risks and Countermeasure, 7th International Conference on risks and security of Internet and systems (CRISIS) IEEE explore 2012

[3] Chan, Z., Dong, W., Li, H., Cao, J., Zhang, P and Chen., X. (2014), Collaborative network security in multi-tenancy data centre for cloud computing, IEEE Xplore Digital Library Tsingheea Science and Technology

[4] Chidambaram, N., Pethuru Raj, K. Thenmozhi, K and Amirtharajan, R. (2016), Enhancing the security of customer Data in cloud Environments using a Novel Digital Finger Printing Techniques, International Journal of Digital Multimedia Broadcasting,

[5] Lazorova, V (2012) Multi tenancy in Cloud Computing, International Conference on Application and Communication Technology and Statistics in Economics and Education (ICAICTSEE -2012)

[6] Pansotra, A and Singh, P (2015) Cloud Security Algorithms, International Journal of Security and its Application, 9, 10,2015,353-360

[7] Christof Paar and Jan Pelzl SHA-3 and The Hash Function Keccak An extension chapter for "Understanding Cryptography — A Textbook for Students and Practitioners"