The Security Challenges and an Assorted Approach in Cloud Computing

Rabindra Nath Ray
Student, Final Semister, Master of Technology (CSE)
THE NORTHCAP UNIVERSITY
Sector 23A, Gurgaon, Haryana, India.

Abstract - Cloud Computing [1,2,4] continues to evolve in the new era of internet based technology with reliable, ubiquitous and on demand services. The enterprises are combining private and public cloud servers due to virtualization and global storage of data and hence security for storage of data and computation stole the spotlight. The storage of containers at server and moving them between multiple cloud environments needs a greater security on data at rest and as well as moving stages. This paper proposes a hardware based Security Key Token (SKT) model which gives a double standard security of data access along with the cryptographic encryption and decryption strategies . The proposed SKT model keeps away the Cloud Service Providers (CSPs) and intruders for unauthorized access of data and hence proved to be a robust and reliable model for Cloud Users (CUs).

Keywords- Cloud Service Providers, Private Cloud, Public Cloud, Container, Cloud Security, Cloud Computing, Cloud Users, Threat 11, Mirage.

I. INTRODUCTION

Computing, in terms of cloud, is presently a well known versatile and admired technology which enables pay per use as per demand and access to network servers which form computing resources, application storages and other services on sharing basis. Rather than managing data and running software on the desktop computers, Laptops, mobile devices or server , the cloud users are able to execute applications and get access to shared data in the cloud from anywhere in the world on 24x7 basis without any implications. Cloud Computing being a distributed architecture, it enhances collaborations, availability, ability to adopt fluctuating demands, agility, scalability and provide cost optimization and adept computing. Cloud computing is combination of Service Oriented Architecture (SOA) [7], virtualization and advanced technologies with strong dependency on internet based applications. Google has introduce the MapReduce framework [6,45] along with Apache's Distributed File System (HDFS) [9] which is processing large amount of shared data and processing them with a little time over the internet based applications. Due to dependency on vulnerable internet and involvement of heterogeneous architectures with different CSPs, the security paradigm has changed to a new dimension. The so called security concepts like authorization, authentication, and identification are no longer stand strong to prevent valuable data stored in the server of CSPs by a cloud user and its safe transaction within network from possible threats. This paper discusses on various security issues and challenges in cloud computing, literature reviews on proposed security models of different authors published in journals and finally it explains the proposed SKT model followed by discussion and future works.

II. SECURITY ISSUES CHALLENGES IN CLOUD COMPUTING.

The aims of cloud computing is to faster the computing power to execute millions of instructions per second. Cloud computing consists of user end and cloud end. The user end contains the user's devices such as computer, laptop, mobile or any access device and application software that requires accessing the cloud network. The cloud end consists of high speed computing devices, servers and distributed data base system which provide the required access to the clients and hence form a cloud environment. See fig 1.

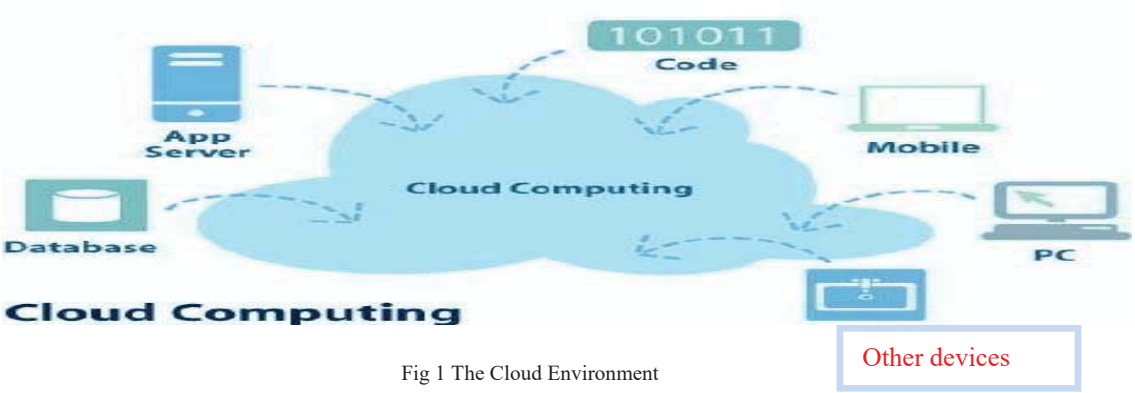

Fig 1 The Cloud Environment

The user end needs to connect his accessing devices like PC, Laptop or mobile to the cloud to access his data stored in a server in the cloud through an interface software using internet. The cloud being a distributed architecture, the user data is stored in CSP's server and the location of the server is unknown to the users or clients. The CSP's servers are managed by administrative groups to whom users need to depend upon for safeguarding data and maintaining privacy. The administrative group members, who are trading with user's data, can prove to be an insider threat violating data secrecy and privacy. The privacy along with confidentiality of user's data must be taken care. A threat management policy ensures that the cloud does not discover any information about the user's data. The followings are the security challenges which need immense concentration.

A. Vulnerabilities

Software as a service (SaaS) applications like Gmail, Yahoo or Facebook are provided to user via internet browser. Attackers are penetrating into client's computer or application by using the web browser. Customary security solutions do not efficiently protect data from attacks. Consequently new approaches are required to be enforced. In virtualization technique, varied instances running on the same corporeal machine needs to be secluded. A Virtual Machine Monitor (VMM) software that abstracts the substantial resources from the multiple virtual machines. Vulnerability in Microsoft Virtual PCs or Microsoft Virtual Servers can allow a casual visitor to run programmed code on the host or on another operating system. Two virtual machines using covert channel can communicate with each other bypassing all the rules defined by the VMMs. Another cloud threat called **Threat 11 [46]** where an attacker creates malicious VM image containing malware or virus and publish it on the providers storage area where other user can retrieve them and infect the whole cloud environment. To counter this attack, **Mirage [19],** an image management system was proposed which focuses on the access control mechanism, image filtrations, derivation tracking system and warehouse maintenance services. VMMs should be root locked so that no right within the virtualized guest environment grants interface with the host systems.

B. Attacks in Networks

(i) Sniffer attacks:

Data in a network travels from one node to another as a packet. Capturing of these packets by intruders in a network is termed as sniffer attack. If the data packets are not encrypted, the data may be accessed and modified by the unauthorized guests and hence vital data packets may lost its identity. A sniffer programme through the Network Interface Card (NIC) guarantee the data linked to other systems in the network also gets recorded so that its identity remains intact. The Address Resolution Protocol (ARP) and Round Trip Time (RTT) [20] are used in a sniffing detection platform to detect a sniffing in networks.

(ii) A spoofing attack:

When a malicious party launches attacks against network hosts, steal data, spread malware or bypasses access controls by imitating another user's device. Some of the common spoofing attacks are IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks. An attacker sends IP packets from a false (or 'spoofed')

source address in order to camouflage itself. ARP is used to resolve IP addresses to MAC (Media Access Control) addresses for transmitting data. In ARP Spoofing attacks, a malicious party sends spoofed ARP messages across a local area network in order to link the attacker's MAC address with the IP address of a genuine member of the network. Here the data which is meant for original user are sent to attacker and the attacker steal the information and modify data, this type of data also included in session hijacking and man in middle attacks.
A Domain Name Server (DNS) associate domain name to an IP address. DNS resolves URLs, email addresses and other human readable domain names into their respective IP addresses. In DNS spoofing attacks attackers modify the server to redirect the domain name to a different IP addresses and infect the data with malware. Using packet filtering, using spoofing detection software and cryptographic network protocol (TLS, SSH and HTTPs) spoofing attack can be avoided.

(iii) Reused IP address:

This is a big security issue in terms of network security. When an old user is migrating from the current network and the old IP address is re-assigned to a new user. There is a cache log for IP addresses of the departing users in the DNS server, which remain active for certain time and the time lag between the re-assigned IP address and the cache log in DNS server [21] creates a big security issue. Hence the attackers may use the cache log of the DNS and modify the DNS with malware which would violate the originality of the data of new users.

(iv) Relationship with third party

Platform as a Service (PaaS) provider offer third party web services components along with its own programming language. Cloud provider sometime subcontracts a third party for data backup in order to recovery of data in case of adversity. So the use of multi tenant architecture and flaw in either one may affect the other and the interconnection complexities raise many security issues. There must be some mechanism or agreed upon policies among the cloud service providers, subcontracted parties and cloud users to counteract those issues which can be security threat for stored data.

C. Cryptography:

Cryptography is meant as the infeasibility of breaking the encryption system and unable to compute the information about exchanged messages. The main aim of cryptography is to secure communication over an insecure channel. Suppose, party M wants to send a secret message to party N which should not be intercepted by a third party. The traditional solution to this problem was Private Key Encryption [47]. In this encryption system, the two party (M and N) hold a meeting and the message passing takes place by agreed upon a pair of encryption and decryption algorithm 'E' and 'D' and additional information 'S' to be kept secret. The intruder may know the 'E' and 'D' algorithm but does not know the secret key 'S'. when M wants to send a message 'm' over communication channel, M encrypts the plaintext message 'm' by computing the cipher text c=E(S, m) and sends c to N. After receiving c, N decrypt the c by computing m= D(S, c). The intruder does not know S and hence don't able decrypt c to get the message m. This mechanism is useful for a small amount of data or message and if the data is handled by two users only. Now a day's data is not handled by users alone. A big amount of data needs to be shared among millions of different users. Hence a cryptographic key needs to be flexible enough to handle such big data. A cryptographic algorithm needs to be strong enough to protect the data. Data in modern days is encrypted via AES (Advanced Encryption Standard) and the SSL (Secured Socket Layer) technology to protect while it is on transit in the network nodes. Although those techniques seem to be secured but a muster key can be developed by the intruder (insider threat) to access the data and hence the threat prevails in the cloud environment.

III. LITERATURE REVIEWS

A. The "SeDaSC" Model:

In IEEE System Journal 1[18,25], Mazhar Ali, Student Member IEEE, REvathi Dhamotharan, Eraj Khan,Samee U. Senior member IEEE, Athanasios V, VAsilakos, Senior Member, IEEE, Kegin Li, Fellow IEEE and Albert Y. Zomaya, Fellow IEEE proposed a model on Secure Data Sharing on Cloud (SeDaSC) titled " **SeDaSC: Secure Data Sharing in Clouds".** In their model the user file is encrypted by a single encryption key called **master key.** After encryption of the file, the master key is then divided into two different key shares for each of the users. One

key part is possessed by the user, which keeps away the intruder (insider threat) from the user data and other key part is stored by the trusted third party, which is called the Cryptographic **Server (CS)**. The master key is deleted permanently. The key part alone cannot decrypt the user data. It needs to again generate the Master key again with the help of the two key parts to decrypt the user's file. See Fig 2.

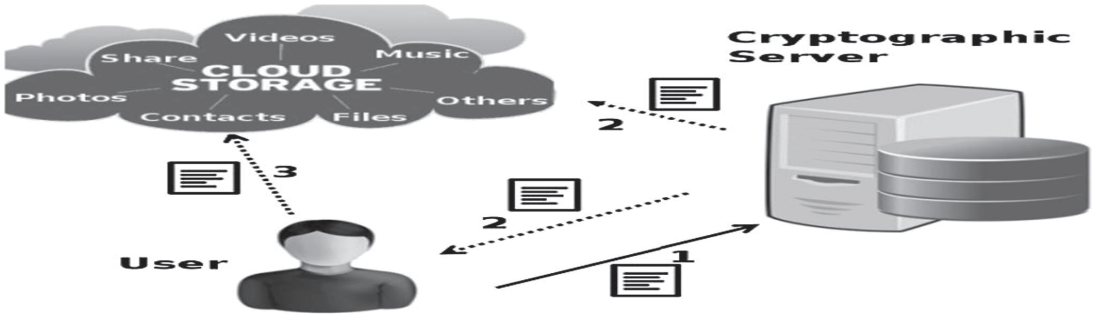

Fig 2 Basic idea for the SeDaSC methodology.

(i) The working of the "SeDaSC" Model:

There are three entities namely (a) Users, (b) a Cryptographic Server (CS) and (c) the cloud in the "SeDaSC' model. In the primary phase the user/data owner load the data, lists of users who all are going to use the data and the parameters to generate an Access Control List (ACL) to the Cryptographic Server (CS). The CS then, being a trusted third party take all the responsibility of access control, key management, encryption and decryption for the data/file. The CS generates a symmetric master key and encrypt the data with the generated master key. The master key is then divided into two parts such that a single part of the key cannot generate the original master key. The original master key is deleted via a secure overwriting. The one part of the key is passed to the users in the circle and the other portion of the key is retained by the CS in the maintained ACL list related to the data file. The encrypted file is stored by the CS in the cloud storage which is maintained by cloud service provider. The user , when wishes to access the data, sends a access request to the CS. The CS upon receiving the request, it downloads the required user's file and asks for the user's portion of the key. After authentication, the CS reconstructs the master key with the help of user's key and CS maintained portion of the key for that particular user. The user's file is then decrypted with the master key newly generated and sent back to the user. If a new member joins to the group, the new user is added to the ACL and two portion of the key is again generated. For the member who is leaving the group, his identification is deleted from the ACL. The departing member cannot access the data as he is remaining with user portion key only. The SedaSc model suggests that no frequent encryption and decryption are needed in case of changes in the group membership.
The SeDaSC claims to be used in mobile cloud computing environment in addition to existing conventional cloud computing due to the reason that compute intensive operations are performed by the Cryptographic Server.

(ii). Discussions on 'SeDaSC Model:

Though the SeDaSC model seems to be a muscular in terms of safety and privacy of data, lacks in addressing so many issues. The model itself is a complex one. The computational burdens in this model makes it unhealthy for handling millions of data and keeping user's data separate form others user in the network. The following issues needs to have a greater attention to upgrade the security issues for the data.

(a) The Cryptographic Server (CS) :

(i) To maintain a CS in the cloud environment is a huge task and two steps generation of user key will impose an intensive computation cost and an overburden increase in pay per use definitely would discourage the cloud users to store their data.

(ii) The administrators of the CS may not be trustworthy. The user's portion of the key may be retained by the tainted administrators and the data security and privacy may be violated.

(iii) A duplicate ACL list for the outgoing members of the group may exists in the server as a mirror image and can be used by the departing members as they are already holding the user portion key

(iv) The CS may not response due to un-reachability /withdrawal/denial of service at any point of time then whole data will be lost. There is no mechanism to recover the data as the user alone cannot recover the data without the CS portion of the key. Moreover, the encryption and decryption of data is done by the CS only. So the users have no control over their own data.

(b) The Cloud Service Provider (CSP) needs to maintain user's records along with the CS records and an extra network link with the CS, which makes the cloud environment a critical mesh.

(c) The sharing of keys within multitenant cloud environment is not recommended.

B. The 'SecCloud' Model

There is a paper named "Security and privacy for storage and computation in cloud computing" [48] by Lifei, Haojin Jhu, Zhenfu Cao, Xiaoleo Dong and team published in a journal named 'ELSEVIER'. In this paper they proposed a privacy cheating discouragement and secure computation auditing protocol which is named as 'SecCloud'. They claimed that the proposed 'SecCloud' is the first protocol that bridges between secure storage and secure computation auditing in cloud. It achieves the privacy cheating discouragement by designated verifier signature, batch verification and probabilistic sampling techniques.

They also tried to build a "practical secure-aware cloud computing experimental environment" which is named as 'SecHDFS', a test bed to implement 'SecCloud'

(i) The Working of " SecCloud" Model

The model considers a general cloud computing model which is having number of cloud servers S1 to SN. The servers are under the control of one or multiple cloud service providers (**CSP**). A mobile phone or a laptop (called as cloud users or **CU**) which is having lesser storage is connected to CSP to avail the resources (computation and storage) of the cloud. It is also assume that there are verification agencies or **VA**s trusted by CUs and responsible for auditing the storages and computing of the CSPs. VAs are assumed to be having more powerful computing capability than CUs.

As per their claim, the protocol is able to achieve the following goals:

(a) Data storage security by the effective auditing of CU and VA.
(b) Data computation security by VAs verification and auditing by CU and VA.
(c) Privacy cheating discouragement because of verification by a designated party and discouraging CSPs for revealing privacy of CUs data even if the servers are attacked by the attackers.

(ii) Discussion on "SecCloud" Model

The proposed protocol performs the following four steps:-

(a) The proposed protocol request for a storage space to the CSPs and the CSP allocates a space by returning a space index *i*, for the message to be stored.
(b) The CUs need to sign each transmitted message block to enable the VAs for auditing.
(c) Data encapsulation is carried out by CUs for pre computing a session key by using Bilinear Diffie-Hellman (BDH) method. The CUs then send the data encrypted by the session key and corresponding signature pairs to the cloud for storage.

When the data is need to be received, then the CSP decrypt the packet by using it own session key to recover data signature pairs and check the signature for data authenticity by VAs using it secret key. The authority for checking the signatures are held by the CSP and VA only and hence it is claimed that the data is secured and protected.

Though the 'SecCloud' protocol claims to be robust and reliable, its shortcomings can be found as bellow:

(a) The computing and transmission overhead is the main concern here. The computing and transmission of encrypted data is very much complex and takes a lot of time which may cause a time out for access to the servers.

(b) Here in this proposed model we are again going to be dependent on a third party i.e. Verification Auditors (VAs) which may reveal the valuable user's data and cause a threat. VAs are need to convinced that the cloud servers use the data on the correct position so that cloud server's cheating behave should not be detected.

(c) In some cases the users may face a denial of service due to the fact that VAs may unresponsive due to connection loss with the users or servers.

IV THE PROPOSED APPROACH: SECURE KEY TOKEN (SKT) MODEL

In the proposed Security Key Token (SKT) approach Cryptographic Server (CS) is avoided for the issues arise so far in the discussions of the SeDaSC model in para 3.2 above. Here a simple and robust model is proposed circumventing the CS. The huge computational cost is avoided and trustworthy on security of data is enabled at a mammoth level. In this SKT model, all the controls for securing and accessing data remain on the hand of users only.

The SKT is hardware based key generation device which generates SKT id for a particular user by applying a special algorithm inside the key. The SKT device is kept and maintained by the user to work in the cloud environment. The SKT model uses two steps to secure the data/files. In the first step, it encrypts the data using RSA or Public Key Encryption. In the second step, it binds the encrypted data with the SKT id which is generated with Symmetric Key Generation algorithm using Hash function and then the encrypted data with SKT id termed as a packet is uploaded to cloud for secure data storage.

Generally, the CSP maintains a user id and password to establish the connection and access the cloud for the registered users. A registered user after establishing the connection with the cloud, requests for his data, the CSP authenticates the user and permits downloading of data packets. After downloading of the data packets, the user needs to match SKT id bounded in the packet with the SKT id available within the SKT device held by the user. If the matching is successful then SKT id is separated from the packet and data is allowed for further decryption process, otherwise it returns a key error and discards the user. In the second stage, after matching and separation of SKT id from the packet, the encrypted data is decrypted through a private key which is available with authorized user only. After accessing the data user may do some modification on data /files i.e read or write operations and again follow the same procedures to upload the data and a new SKT id is bounded with the encrypted data. A copy of the SKT id is kept in the SKT device for the data/files uploaded in the cloud. If data packets go into the hands of unauthorized users, the packets are useless for them as they cannot access the data contents because of not having SKT id and the private key. In this scenario the SKT model approaches to secure data with the double standards, less computations and cost effective manner as well. Cloud users need not to rely on third party i. e. CSPs or Cryptographic Server (CS) for their data security. See Fig 3.

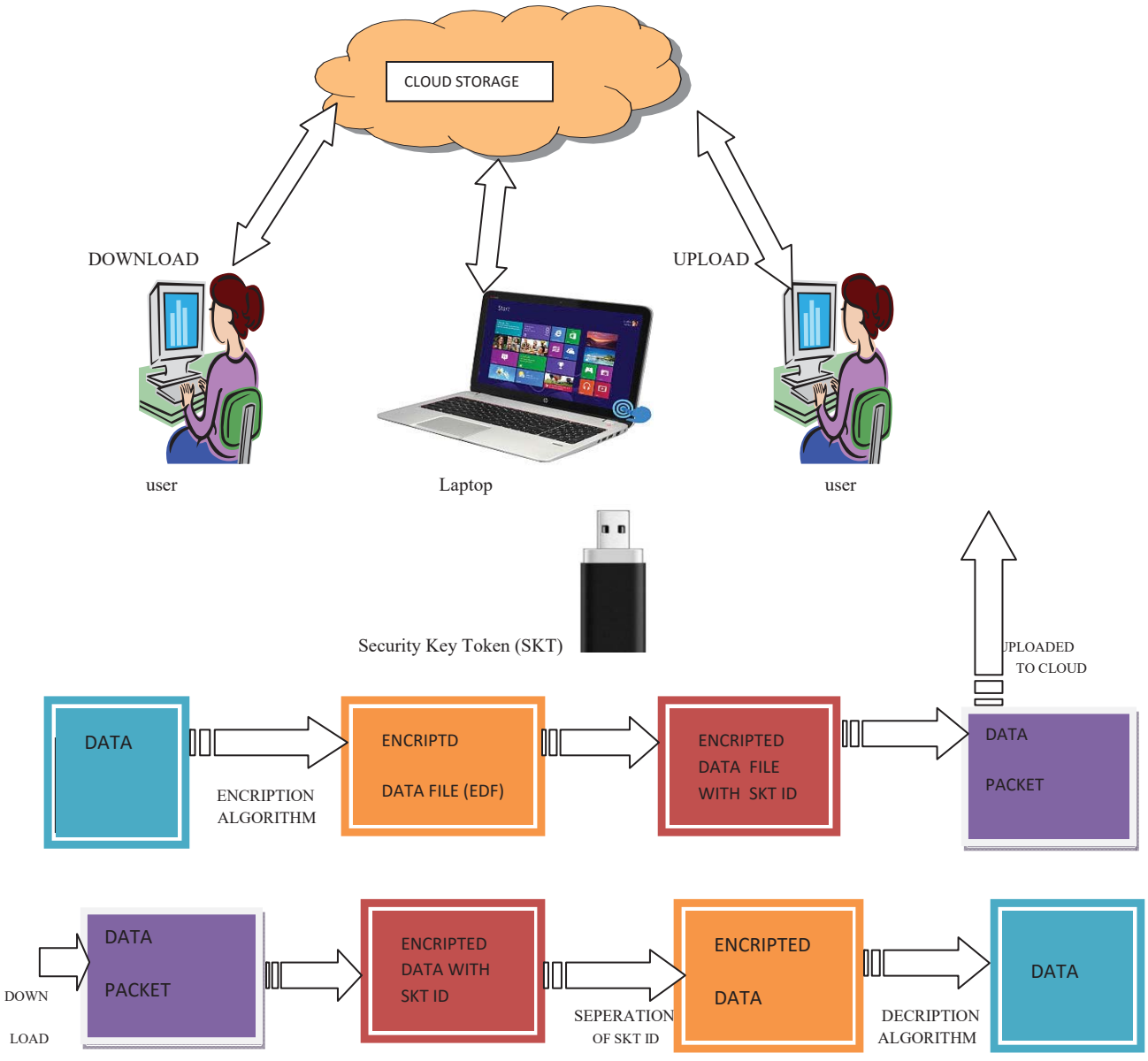

Fig 3 (The proposed approach-SKT model)

A. The RSA Algorithm:

The first public key cryptosystem and widely used for secure data transmission is the **RSA algorithm** [23]. In this cryptosystem the encryption key is public and it differs form the decryption key and the decryption key is kept secret called private key. The RSA is drawn from the initial letters of the surname **Ron Rivest**, **Adi Samir** and **Leonard Aldeman**, who first publicly described the algorithm in 1977. The RSA algorithm involves four steps namely (a) Key Generation (b) Key Distribution (c) Encryption and (d) Decryption. The principle of RSA algorithm is to deal with two keys a public key and a private key. The public key is used for encryption of messages and the private key is used for decryption of messages. It is practical to find three large positive integers a, p and d so that with modular exponentiation for all m:

$$(m^a)^p \bmod d = m$$

Even knowing a, d or even m it is very difficult to find p.

Key Distribution: To enable Tom to send his encrypted messages, Jerry transmits public key (d, a) to Tom via a reliable but may be non secret route. The private key is never shared.

Encryption: Suppose Tom wants to sends message M to Jerry. Firstly,Tom needs to turn the message M into an integer m, such that

0 <=m<d and gcd (m, d) = 1 by using an agreed upon reversible protocol known as padding scheme. Tom then computes the cipher text c using Jerry's public key a corresponding to **c=m^a mod d.** Even for 500 bit numbers, this can be done efficiently using modular exponentiation. Tom then sends c to Jerry.

Decryption: Jerry can recover m from c by using private key exponent p by computing

c^p ≡ (m^a)^p ≡ m mod d.

Jerry can finds the original message M, using m and reversing the padding scheme.

Key generation of RSA:

The keys generation is an imperative part for RSA algorithm. The keys are generated as follows:

(a) p and q are two prime numbers are chosen distinctly. The prime numbers p and q are chosen randomly and are similar in magnitude. They differ in length by a few digits for making the factoring harder.

(b) Now compute n=p.q
For both the private and public keys n is used as modulus and its length is expressed in bits which are termed as key length.

(c) Calculate $\varphi(n) = \varphi(p).\varphi(q) = (p-1)(q-1) = n-(p+q-1)$, the value of $\varphi(n)$ is the private key portion, which is called Euler's totient function and is kept secret .

(d) An integer d is chosen such that $1<d<\varphi(n)$ and GCD(d, $\varphi(n)$) =1; i.e, d and $\varphi(n)$ are co prime.

(e) Find out e as $e \equiv d\text{-}1 \pmod{\varphi(n)}$: i.e., e is modular multiplicative inverse of d(modulo $\varphi(n)$).

In a simple it can be stated that for given $d.e \equiv 1 \pmod{\varphi(n)}$ take out the solution for e. The length of e being a short and small Hamming weight it results in more efficient encryption.
Here e is released as the public key exponent and d is kept as private key exponent. The modulus n and the public exponent e together make the public key and the modulus n and the private exponent d (for decryption) form the private key which is kept secret. The prime numbers p and q and $\varphi(n)$ also kept secret because those are used for calculating d.

B. Key generation for SKT (SKT id)

Suppose, S is generated randomly by the SKT device for each of Encrypted Data File (EDF). At the first step a random number R having length 256 bits may be generated in such away that R= (0, 1) ^ 256. In the second step R be passed through a Hash function using secure Hash algorithm 256 (SHA-256). The second step is to randomize the initial user derived random number R. Now the output of the Hash function is S which is used in Symmetric Key Algorithm (SKA) for encryption in Advanced Encryption Standard (AES) for securing user's data. This S is used for generating the SKT id which is then added to the encrypted data and then called as packet which is stored in the cloud. The copy of SKT id is saved to the user SKT device for matching and recovering data after downloading the requested data.

C. Algorithm for SKT id generation

Input: The EDF, The SKA and the 256 bits Hash Function (Hf()).

i. Compute R = {0,1}^256 and S= Hf(R)
ii. SKT id = SKA (EDF, S)
iii. Add SKT id to EDF
iv. Return SKT id and save SKT id to SKT device of the owner.
v. Packet P ≡ (EDF+ SKT id)
vi. Upload the P into the Cloud.

D. Algorithm for SKT id separation

Input: The data packet (P), the SKA

After downloading the data packet (P)

Compute:

i. Get SKT id from the requesting user (Plug in SKT device into PC or Laptop)

ii Match the SKT id of user (the SKT id of user and the SKT id present in the data packet).

iii. If matching successful then go to step v else

iv. Return unauthorized user.

v. EDF = SKA (SKT id, P)

vi, Send EDF to the user

vii. Delete (SKT id)

vii. end if

E. Discussions on the proposed model

There are many research approach towards the security issues of the cloud computing. The related approaches focus on some complex architecture which tends to be difficult to implement on real cloud environment and impose a complex computation overhead. More over these researches are not that much well built to face all security challenges. The proposed SKT model uses RSA algorithm to encrypt user's data file. After encryption of data file it is named as Encrypted Data File (EDF) and it becomes difficult to decrypt the file by the unauthorized intruders as there is a secured private key to unlock the data file. The EDF again goes through a symmetric key generation algorithm (SHA-256) and generate the SKT id. The SKT id is added to the EDF and a copy of the EDF id is saved automatically in the SKT device for each file loaded to the cloud. When a download request is received by the CSP then the data file's SKT id is matched with the SKT id of user's SKT device. If the matching is found then only the data file is allowed to download for the authorized user and the authentication is established. The SKT id is then separated from the encrypted data using SKT separation algorithm and old SKT id is then deleted from the data file and as well as SKT device. The encrypted data is decrypted via reverse RSA algorithm. After accessing data, user may do some read/write operation and when he uploads the data to cloud again a SKT id is generated and the same procedure follows to secure the data. In this model every security aspect is maintained by the user himself. Users need not to rely on third party's trust which is the main threat for data storage.

The cloud storage only storing the packet containing the encrypted data along with SKT id, this data if is accessed by illicit users, the data is useless for them. The model is relatively simple and trustworthy in view of the security concerns for the cloud environment.

V. CONCLUSION

The storage, virtualization as well as the various virtualization techniques and the network in use encompass a greater security concern in cloud computing environment. The security of user's data needs to be ensured at highest level. Due to the complex architecture of the cloud it is a big challenge to ensure security of data at all levels in the cloud environment. The cloud is still in a growing phase and the proposed SKT model approach can definitely address the existing security issues. In future work, it is intended to undertake detail computations for this SKT model and implementation on real cloud platform.

REFERENCES

[1] LordCrusAd3r,"ProblemsFacedbyCloudComputing",dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.
[2] https://en.wikipedia.org/wiki/Cloud_computing.
[3] R. Buyya, S. Pandey, and C. Vecchiola, Cloudbus toolkit for market-oriented cloud computing, in Proceedings 1st International Conference on Cloud Computing (CloudCom 09), Beijing, 2009, pp. 3_27.
[4] Lord CrusAd3r,"Problems Faced by Cloud Computing", , dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.
[5] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.
[6] Ren, Yulong, and Wen Tang. "A SERVICE INTEGRITY ASSURANCE FRAMEWORK FOR CLOUD COMPUTING BASED ON MAPREDUCE."*Proceedings of IEEE CCIS2012*. Hangzhou: 2012, pp 240 – 244, Oct. 30 2012-Nov. 1 2012.
[7] www.ibm.com/software/solutions/**soa**
[8] P.Mell, T. Grance, The NIST definition of cloud computing (draft), NIST Special Publ. 800 (145) (2011) 7.
[9] K, Chitharanjan, and Kala Karun A. "A review on hadoop — HDFS infrastructure extensions.". JeJu Island: 2013, pp. 132-137, 11-12 Apr. 2013.
[10] D. AB. Fernandes, L. FB. Soares, J.V. Gomes, M.M. Freire, P. RM Inácio, security issues in cloud environments: a survey, Int. J. Inform. Sec. 13 (2) (2014) 113–170.
[11] UNDERSTANDING The Cloud Computing Stack SaaS, Paas, IaaS, © Diversity Limited, 2011 Non-commercial reuse with attribution permitted.
[12] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA
[13] Keene C (2009) The Keene View on Cloud Computing. Online. Available:http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html.Accessed: 16-Jul-2011
[14] K. Hashizume, D.G. Rosado, E. Fernndez-Medina, E.B. Fernandez, An analysis of security issues for cloud computing, J. Internet Services Appl. 4 (1) (2013) 1–13.
[15] W.A. Jansen, Cloud hooks: Security and privacy issues in cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), 2011, pp. 1–10.
[16] F. Zhang, H. Chen, Security-preserving live migration of virtual machines in the cloud, J. Netw. Syst. Manage. 21 (4) (2013) 562–587.
[17] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (2011) 1–11.
[18] M. Ali, R. Dhamotharan, E. Khan, S.U. Khan, A.V. Vasilakos, K. Li, A.Y. Zomaya, SeDaSC: secure data sharing in clouds, IEEE Syst. J. (2015), http://dx.doi.org/10.1109/JSYST.2014.2379646.
[19] Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of virtual machine images in a Cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud Computing Security. ACM New York, NY, USA, pp 91–96
[20] Ohlman, B., Eriksson, A., Rembarz, R. (2009) What Networking of Information Can Do for Cloud Computing. The 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Groningen, The Netherlands, June 29 - July 1, 2009.
[21] L.J. Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture," ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009.
[22] Diaa Salama, Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", International Journal of Network Security, PP.78-87,Sept. 2010.
[23] Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public key cryptosystems. Commun. ACM **21**, 120–126 (1978).
[24] Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of virtual machine images in a Cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud Computing Security. ACM New York, NY, USA, pp 91–96
[25] IEEE SYSTEMS JOURNAL 1 SeDaSC: Secure Data Sharing in Clouds Mazhar Ali, Student Member, IEEE, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Senior Member, IEEE, Athanasios V. Vasilakos, Senior Member, IEEE, Keqin Li, Fellow, IEEE, and Albert Y. Zomaya, Fellow, IEEE.
[26] Security and privacy for storage and computation in cloud computing Lifei Wei a, Haojin Zhu a, Zhenfu Cao a,⇑, Xiaolei Dong a, Weiwei Jia a, Yunlu Chen a, Athanasios V. Vasilakos b.
[27] Cong Wang; Qian Wang; Kui Ren; Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," INFOCOM, 2010 Proceedings IEEE , vol., no., pp.1,9, 14-19 March 2010
[28] International Journal of Thesis Projects and Dissertations (IJTPD) Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013, Available At: www.researchpublish.com Page | 1 Research Publish Journals Security Issues in Cloud Computing - A Review Anitha Y1 1Department of Computer Science and Engineering, Punjab Technical University 1SSCET, Pathankot, India
[29] Ensuring Data Storage Security in Cloud Computing Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology. Wenjing Lou Department of ECE Worcester Polytechnic Institute.
[30] A Comparative Survey on Symmetric Key Encryption Techniques by Monika Agrawal , Department Of Computer Science Shri Shankara Charya Institute Of Technology & Management Bhilai, India. Pradeep Mishra Department of Computer Science Shri ShankaraCharya College of Engineering & Technology Bhilai, India.

[31] ISSN 2348-1196 (print) International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 3, Issue 2, pp: (1130-1134), Month: April - June 2015, Available at: www.researchpublish.com Page | 1130 Research Publish Journals Data Security and Privacy Protection Issues in Cloud Computing 1Ms. Rupali R. Kanthe, 2Ms. Rinkle C. Patel 1, 2 Department of MCA, IMCOST College, Thane (w), University of Mumbai, India.
[32] International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012 421 Cloud Computing: Different Approach & Security Challenge Maneesha Sharma, Himani Bansal, Amit Kumar Sharma.
[33] International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014 DOI : 10.5121/ijnsa.2014.6304 45 SECURITY ISSUES ASSOCIATED WITH BIG DATA IN CLOUD COMPUTING Venkata Narasimha Inukollu1 , Sailaja Arsi1 and Srinivasa Rao Ravuri3 1Department of Computer Engineering, Texas Tech University, USA 3Department of Banking and Financial Services,Cognizant Technology Solutions, India.
[34] IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011 Cloud Computing: Security Issues and Research Challenges Rabi Prasad Padhy1 Manas Ranjan Patra2 Suresh Chandra Satapathy3 Senior Software Engineer Associate Professor HOD & Professor Oracle India Pvt. ltd. Dept. of Computer Science Dept. of Computer Sc. & Engg. Bangalore, India Berhampur University, India ANITS, Sanivasala, India.
[35] International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014 DOI : 10.5121/ijnsa.2014.6304 45 SECURITY ISSUES ASSOCIATED WITH BIG DATA IN CLOUD COMPUTING Venkata Narasimha Inukollu1 , Sailaja Arsi1 and Srinivasa Rao Ravuri3 1Department of Computer Engineering, Texas Tech University, USA 3Department of Banking and Financial Services,Cognizant Technology Solutions, India.
[36] Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors Tiago Oliveira a,*, Manoj Thomas b, Mariana Espadanal a a ISEGI, Universidade Nova de Lisboa, 1070-312 Lisbon, Portugal b School of Business, Virginia Commonwealth University, 301 W. Main Street, Richmond, VA 23284-4000, USA.
[37] Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage by Yong Yu · Man Ho Au · Yi Mu · Shaohua Tang ·Jian Ren · Willy Susilo · Liju Dong.
[38] See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/259072387 Cloud Computing Security Issues and Challenges ARTICLE · JANUARY 2011.
[39] A. Abbas and S. U. Khan, "A review on the State-of-the-art privacy preserving approaches in e-health clouds," IEEE J. Biomed. Health Informat., vol. 18, no. 1, pp. 1431–1441, Jul. 2014.
[40] A Comparative Survey on Symmetric Key Encryption Techniques Monika Agrawal Department Of Computer Science Shri ShankaraCharya Institute Of Technology & Management Bhilai, India monika.agrawal1986@gmail.com Pradeep Mishra Department Of Computer Science Shri ShankaraCharya College Of Engineering & Technology Bhilai, India pradeepmishra4u@gmail.com.
[41] Nisioka, Mototsugu, " Public-Key cryptosystem with provable security, DSpace at WasedaUniversity, 2013.
[42] https://en.wikipedia.org/wiki/Cloud_computing_security.
[43] J. Dean, S. Ghemawat, MapReduce: simplified data processing on large clusters, Communications of The ACM 51 (1) (2008) 107–113.
[44] Himani Agrawal and Monisha Sharma, "Implementation and analysis of various symmetric cryptosystems", Indian Journal of Science and Technology Vol. 3 No. 12, December 2010.
[45] R. Buyya, S. Pandey, and C. Vecchiola, Cloudbus toolkit for market-oriented cloud computing, in Proceedings 1st International Conference on Cloud Computing (CloudCom 09), Beijing, 2009, pp. 3 27.
[46] https://**clouds**ecurityalliance.org/top**threats**/csa**threats**.v1.0.pdf.
[47] Lecture Notes on Cryptography Shafi Goldwasser1 Mihir Bellare2 July 2008 1 MIT Computer Science and Arti¯cial Intelligence Laboratory, The Stata Center, Building 32, 32 Vassar Street, Cambridge, MA 02139, USA. E-mail: shafi@theory.lcs.mit.edu ; Web page: http://theory.lcs.mit.edu/ shafi 2 Department of Computer Science and Engineering, Mail Code 0404, University of California at San Diego, 9500 Gilman Drive, La Jolla, CA 92093, USA. E-mail: mihir@cs.ucsd.edu ; Web page: http://www-cse.ucsd.edu/users/mihir.
[48] Security and privacy for storage and computation in cloud computing Lifei Wei a, Haojin Zhu a, Zhenfu Cao a,⇑, Xiaolei Dong a, Weiwei Jia a, Yunlu Chen a,Athanasios V. Vasilakos b.