ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

An Efficient Survey on Cloud Security Assessment

K.Balaji [1], Assistant Professor,
Vimal Sidhartha. [2], PG Scholar-MCA
Priyadharshini [3], PG Scholar-MCA
Hemalatha [4], PG Scholar-MCA
Department of Computer Applications, Srinivasan College of Arts and Science, Perambalur.

ABSTRACT

A cloud storing process, consisting of a gathering of storage servers, gives storage services larger than the Internet. Storing information in a third party's cloud system makes severe anxiety over information privacy but they have a chance to retrieve the data from the cloud. General encryption techniques look after information confidentiality, but also boundary the functionality of the storage space system because a few operations are favoured over encrypted data. Constructing a protected storage scheme that wires several functions is difficult when the storage space system is scattered and has no middle ability. In future, entry of proxy re-encryption (RSA is an algorithm used by encrypting and decrypt messages) technique and put together it with a decentralized removal code such that a protected circulated storage system is defined. ECC is used to generate the keys data confidentiality.ECC makes keys via the properties of the elliptic bend equation instead of the conventional functionality. The major technological donation is that the third party encryption method supports encryption operations over the encrypted text as well as forwarding actions more than encryption and encrypted text. Here, the process fully combines encryption, encoding, and forwarding. Examine and use appropriate parameters for the text dispatched to storage servers and the storing servers accessed by a key server. Extra flexible alteration between the number of storage servers and strength.

Keywords: Cloud computing, cybersecurity, advanced persistent threats, security metrics, and virtual machine (VM)

I. INTRODUCTION

It basically by patter into additional obscure they can expand quick contact to best industry applications or severely boost their communications possessions, all at a small cost. Gartner defines cloud computing as ''a style of computing anywhere particularly scalable Information Technology are released as service to outside clients using Internet technologies''. Cloud providers at present benefit from a thoughtful occasion in the marketplace. The providers must guarantee that they get the safety aspects right, for they are the ones who will take on the task if belongings go wrong. The cloud offers a number of payback like fast consumption, payment use, Minimum costs, scalability, quick provisioning, quick elasticity, everywhere system access, greater resiliency, hypervisor security against system attacks, low-cost calamity recovery and data storage space solutions, on-demand protection controls, real-time finding of system tampering and quick re-constitution of services.

web application vulnerabilities such SQL (Structured Query Language) insertion and cross-site scripting, material contact issues, privacy and manage issues arising from third parties having physical control of data, issues related to identity and documentation organization, issues interconnected to information confirmation, tampering, reliability, privacy, data loss and stealing, issues linked to verification of the respondent machine Though cloud computing is under attack to give well again operation of funds using virtualization techniques and to obtain up a lot of the job load from the client, it is filled with safety risks.

II. ISSUES AND CHALLENGES

The flexibility and scalability of CCSs can offer significant benefits to government and private industry. Whether cloud users can trust CSPs to protect cloud tenant data and whether CCSs can prevent the unauthorized disclosure of sensitive or private information. The literature is rife with studies of CCS security vulnerabilities. VMs run on computing hardware that may be shared by cloud tenants. This enables flexibility and elasticity but introduces security concerns. The security position of a CCS depends on a lot of factors, including safety applications organization

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

on the scheme, the hypervisor (HV) and connected protection events, the design patterns used to cut off the manage flat from cloud tenants, the level of shield provided by the CSP to cloud occupant user data and VM images, as well as additional factors.

III. SECURITY CHALLENGES

a) Proxy Re-Encryption

In a proxy re-encryption scheme, a substitute server can relocate a ciphertext under a public key PKA to a new one beneath an additional public key PK_B by using the re-encryption key $RK_{A->B}$. The server does not know the plaintext through alteration. In planned some proxy re-encryption schemes and functional them to the allocation occupation of sheltered storage systems. In their work, letters are first encrypted by the owner and then stored in a store attendant. When a user requests to divide his post, he sends a re-encryption key to the storage server. The storage server re-encrypts the encrypted messages for the official user. Therefore, their scheme has data carefulness and ropes the data forwardreason. Our work added integrates encryption, re-encryption, and indoctrination.

b) Research Objectives

- This research will provide new techniques to ensure security in Cloud Computing data. The objectives of proposed work are formulated as below:
- Cloud-Trust is based on CCS unique attack paths that cover the essential elements of IaaS cloud architecture.
- It is base on a Bayesian system model of the CCS, the group of students of APT attack path spanning the CCS assault space, and the APT attack steps necessary to implement each assault path.
- It provides two key far above the ground-level safety metrics,tosum up, CCS safety status quantitatively: The first security metric estimate whether elevated value information.
- The next metric assesses whether the CSP provideblurtenant sufficient CCS network monitoring, file access, and situation awareness data to detect intrusion into a tenant's cloud system and whether the tenant's safety and monitoring systems add to the intrusion uncovering.

IV. RELATED WORKS

[1] Obtainableconsentmechanismfails to provide influential and healthy tools for handling security at the levelessential for today's Internet. These mechanisms are future below increasing strain from the progress and consumption of systems that augment the programmability of the Internet. Moreover, this enlarged suppleness from side to side programmability trend seems to be accelerating with the coming of proposals such as Active Networking and movable Agents. The trust-management advance to distributed-system protection was urbanized as a response to the insufficiency of traditional agreement mechanisms. Trust-management engines shun the want to resolve "identities" in an authorization decision. in its place, thestate rights and limits in a encoding verbal communication. This allows for augmented elasticity and impressibility, as well as the consistency of modern, scalable refuge mechanisms. Further advantages of the trust-management advance comprise proofs that requested dealings comply with local policies and system architectures that support developers and administrators to believe an application's security policy carefully and specify it clearly. In this paper, to inspect existing authorization mechanisms and their inadequacies. To introduce the concept of trust management, explain its basic principles, and describe some existing trust-management engines, including PoHcy Maker and Key Note. To also report on our knowledge using trust-management engines in numerous distributed-system applications.

[2] Software as a Service (SaaS) is a rapidly growing model of software licensing. In contrast to traditional software where users buy a perpetual-use permit, SaaS users buy a donation from the publisher. Whereas conventional software publishers characteristically free new creation skin as part of new versions of software once in a few years, publishers using SaaS have an

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

enticement to discharge new features as soon as they are completed. To show that this property of the SaaS licensing model leads to greater speculation in product increase under most conditions. This increased outlay leads to higher software superiority in equilibrium under SaaS compared to perpetual licensing. The software publisher earns superior profits beneath SaaS while a social interest is also higher.

[3] Cloud computing allows delivering information knowledge power on order. Be it either the hosting of a convinced web request or the outsourcing of a whole server or data center by earnings of virtualization. Applying these techniques however goes along with handing over the final manage of statistics to a third party. This paper investigate the purpose of corona as a blurset aside and show an instancecomprehension for retain data run to the user based on nearmechanismimages encrypted on the client side. This means that the measures involved for verifying validity and accessing the virtual machine have to be completely provided by the user. To provide a sample completion of a secure virtual mechanism consisting of an encrypted divider, containing the data to be hosted, and a boot system, containing the logic to verify and admission the encrypted partition. Further facts of the execution are described and applied on a cloud resource available inside the Austrian Grid project. The methods presented in this paper form the basis for subsequent investigate on solitary point of admission lattice resp. cloud resources. The results will be applied in the Austrian Grid Phase 2 review ripeness "Grid-supported Breath Gas examination of Molecular leaning Diseases".

[4] blurcomputes systems basicallygiveright of entry to large pools of figures and computational property during a variety of interfaces like in strength to existing grid and HPC resource management and indoctrinationscheme. These types of systems offer a new indoctrination aim for scalable request developers and have gained popularity over the history few years. though most blurscomputesystem in procedure today are proprietary, rely upon communications that are unseen to the explore culture, or are not clearly intended to be instrumented and customized by systems researchers. In this work, to their CLOUDME – an open source software scaffold for cloud computing that apparatus what is commonly referred to as communications as a Service (IaaS); systems that give users the capacity to run and control entire virtual contraption instances deployed across a variety physical resources. To outline the basic doctrine of the CLOUDME design, detail important prepared aspects of the system, and discuss architectural trade-offs that made in order to tolerate CLOUDME to be portable, modular and easy to employ on infrastructure commonly found within academic settings. Finally, to provide evidence that CLOUDME enables users recognizable with existing Grid and HPC systems to discover new cloud computing functionality while maintaining entrée to existing, familiar application development software and Grid middleware.

c) System Setup

The algorithm SetUp (1) generates the arrangement parameters. A customer uses KeyGen to create his community and secret key pair and ShareKeyGen to divide his secret key to a set of m key servers with a threshold t, where k < =t <= m. The user nearby provisions the third constituent of his covert key.

d) Data Storage

When user A desires to hoard a memo of k blocks m1,m2, .;mk with the identifier ID, he computes the uniqueness voucher and performs the encryption algorithm Enc k blocks to get k original ciphertexts C1,C2, . . . ; Ck. An original ciphertext is indicated by a foremost bit b ¼ 0. User A sends each code text Ci to v erratically selected storage servers. A storage server receives a set of novel symbols texts with the same self-coin _ from A. When a ciphertext Ci is not acknowledged, the storage server inserts Ci to the set. The singular format of is a mark for the absence of Ci. The storage attendant performs Encode on the set of k ciphertexts and provisions the encoded result (codeword symbol) Encryption. Encoding is a main part of the data storeroom.

e) Data Forwarding

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

Requirements to forward a memo to a new user B. He requests the first constituent a1 of his furtive key. If A does not hold a1, he queries key servers for key shares. What time at slightest t key servers react, arecover the first division a1 of the secret key SK_A via the Key pick upthe algorithm. Let the identifier of the meaning be ID. User A computes the re-encryption key $RK^{ID}_{A->B}$ via the Re KeyGen algorithm and steadily sends the re-encryption key to each storeroom server. By $RK^{ID}_{A->B}$a storage spacewine waiter re-encrypts the sole password sign C0with the identifier ID into a re-encrypted codeword sign C'' via the ReEnc Þ algorithm such that C'' is decrypted clever by using B's secret key. A re-encrypted codeword sign is indicated by the foremost bit b ¼ 1. Let the public key PK_B of user B be $(g^{b1}; h^{b2}.)$.

f) Data Retrieval

There are two cases for the data recovery stage. The first container is that a user A retrieves his own communication. When usinga needs to recover the significance with the identifier ID, he informs all key servers with the identity token A key server first retrieves unique key cryptogram from u arbitrarily chosen storeroom servers and then performs partial decryption split Dec on each retrieved unique password character C0. The result of partial decryption is called a partially decrypted codeword symbol. The key server sends the somewhat decrypted codeword symbols _ and the coefficients to user A. After customer A collect replies from at least t key servers and at smallest quantity k of them are originally from distinct storage servers, he executes unite on the t somewhat decrypted codeword symbols to recover the blocksm1;m2; .;mk. The next case is that a user B retrieves a communication forwarded to him. User B informs all key servers directly. The get-together and combinepart are the equal as the first case except that key servers get back re-encrypted password symbols and do fractional decryption Share-Decrypted on re-encrypted passwordcipher.

g) Data Storage Phase

In the data storeroom stage, user A encrypts his communication M and dispatches it to storage servers. A message M is decaying addicted to k blocks m1; m2; .;mk and has an identifier ID. User A encrypts each block mi into a ciphertext Ci and sends it to v erratically select storage servers. ahead getting secret message texts from a client every storage server linearly combines them with arbitrarily chosen coefficients into an underground sound symbol and stores it. Note that a storage space server might receive less than k import blocks and to assume that all storage servers know the worth k in progress.

h) Symmetric (Secret) Key Cryptography

This cryptographic method uses two different algorithms for encryption and decryption respectively, and the same key is used both the sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt that data

i) AES

AES (Advanced Encryption Standard) is a symmetric block encryption normaloptional by NIST (National organizationof principles and Technology) second-hand for securein order. It uses the same key for both encryption and decryption. It has a variable key length of 128, 192, or 256 bits; default 256 [2][8]. It encrypts factsblock of 128 bits in 10, 12 and 14 around depending on the input size

j) DES

DES (Data Encryption Standard) is a symmetric block encryption standard to be recommended by NIST. The DES algorithm is the most broadly used encryption algorithm in the world. The same algorithm and key are used for encryption and decryption, with minor differences. DES accepts an input of 64- bit long plaintext and 56-bitkey (8 bits of parity) and producesan output of 64-bit block.

k) 3DES

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

Triple Data Encryption Algorithm (TDEA or Triple DEA) is a symmetric-key block cipher standard which is similar to DES method but increases encryption level 3 times than DES. As a result, this is slower than other block cipher methods. The block size of 3DES is 64 bit with 192 bits key size[2]

l) Blowfish

Blowfish is a symmetric key cryptographic algorithm that encrypts 64-bit blocks with a variable length key of 128-448 bits. Blowfish is the better than other algorithms in throughput and power consumption

m) RC4

The RC4 (Rivest Cipher 4) is an encryption algorithm that is a communal key brookcipher algorithm require a safeswap of a shared input. The RC4 encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) using 40 and 128-bit keys. To make the key brook, the nonentity makes use of a clandestineinterior state which consists of two parts: 1. A permutation of all 256 possible bytes. 2. Two 8-bit index-pointers. The permutation is initialized with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA).

n) International Data Encryption Algorithm (IDEA)

inclusive Data Encryption Algorithm (IDEA), at firstcallbetterprospect Encryption usual (IPES), is a symmetric-key chunkcode designed by James Massey of ETH Zurich and Xuejia Lai and beprimaryexplain in 1991. The algorithm was intended as a replacement for the Data Encryption Standard (DES). International Data Encryption Algorithm (IDEA) is a symmetric key encryption technique that uses the same key for both encryption and decryption. This key is of length 128-bit which secures 64-bit data. Also, it runs eight and a half rounds for encrypting and decrypting the data

o) SEED

A massnonentity uses 128-bit block and 128-bit keys. It was urbanized by the Koreain order Security group (KISA) and adopt as a nationwidenormal encryption algorithm in South Korea

p) ARIA

A 128-bit block cipher employs 128-, 192- and 256-bit keys. It was developed by a large group of researchers from academic institutions, research institutes and federal agencies in South Korea in 2003 and subsequently named a national standard

q) TEA

TEA is to a Feistel prearranged symmetric key algorithm. TEA is a chunkcode that uses a 64-bitsimple text with 64 round and a Key distance end to end of 128-bit with changeable (recommended 64 Feistel rounds) roundhave 32 cycles. It does not contain S-boxes and the similar algorithm is used in upturned for decryption

r) CAST

CAST is symmetric solution algorithm base on the backconception of Feistel constitution. The CAST is a building block code that uses a 64-bit plain text with 12 or 16 rounds and a variable Key Length of 40 to128-bit. It also contains 4 S- boxes and the similar algorithm is used in upturned for decryption

s) Two Fish

Bruce Schneier is the person who composed Blowfish and its successor Two fish. The Keys used in this algorithm may be up to 256 bits in length.Two fish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Two fish is also freely available to anyone who wants to use it. As a result, we'll find it bundled in encryption programs such as Photo Encrypt, GPG, and the popular open source software TrueCrypt

t) Triple DES

Triple DES is same as the DES operation. It uses three 64-bit keys and overall key length of 192 bits. We simply type in the entire 192-bit (24 characters) key rather than entering each of the invidiously three keys.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

The procedure for encryption is exactly the same as DES, but this process is repeated three times. It is encrypted with the first key then decrypted with the second key, and finally encrypted again with the third key. This procedure for decrypting something is the same as the procedure for encryption, except it is accepted same as the reverse process

u) Two fish algorithm

Two fish is also a symmetric block cipher having Feistel structure. It is also developed and explained by BruceSchneier in 1998. Two fish also uses block ciphering like Blowfish. It is efficient for software that runs ona smaller processor (smart cards) and embedding in hardware. It allows implementers to customize encryption speed, key setup time, and code size to balance performance. Two fish is license-free, unpatented and freely available for use. In two fish encryption, it uses key sizes of 128, 192 and 256 bits. It uses the block size of 128 bits and there are 16 rounds of encryption in this encryption algorithm.

v) Three Fish

Three fish is a symmetric key block cipher designed by BruceSchneier, Niels Ferguson, Stefan Lucks, Doug Whiting, MihirBellare, JesseWalker. It was first published in the year 2008. Three fish block cipher is directly related to Blowfish and Two fish. Three fish algorithm is tweaked able block cipher. A tweakable block ciphertakes three inputs, a key, a tweak and block of massage. A unique tweak value is used to encrypt every block of massage. The tweak value is 128 bits for all block sizes. Three fish encryption uses three type of keys 256 bits, 512 bits or 1024 bits

w) RC5

RC5 is a symmetric-key block cipher. It is designed by Ronald Rivest in 1994. RC stands for “Rivest Cipher” or it is also called “Ron’s Code”. AES (Advanced Encryption Standard) is directly based on RC5. It uses key sizes 0 to 2040 bits but suggested count is 128 bits. RC5 uses block sizes of 32, 64 or 128 bits but 64 bits are suggested. It is fiestellikea network. It has 1 to 255 encryption rounds but 12 rounds are suggested originally. It is suitable for hardware and software implementation because it uses only those operations which are available in the typical microprocessor

x) Skipjack algorithm

Asymmetric cryptographic algorithm developed by the U.S. National Security Agency (NSA). It is used in the Department of Commerce's Escrowed Encryption Standard (EES), which was embodied in the CLIPPER chip.The key to the encrypted message is itself encrypted with a key combined from two escrowed keys. The encrypted key and an identifier of the chip that sent it is encrypted again with a "family key." In this way, a law enforcement agency can use the family key to decrypt the outer layer and glean the chip ID, which is used to obtain the two escrowed keys that are combined to decrypt the key that decrypts the message. Skipjack uses an 80-bit key to encrypt 64-bit blocks, but algorithm details are classified.

y) Tiny Encryption Algorithm (TEA)

TEA is used for constrained environments like sensor networks or smart things. It is written in very few lines of code. It does not use a complex program but requires simpleoperations of XOR, adding and shifting. It uses a block size of 64 bits and 128-bit keys and does not make use of existing tables or any predefined computations18. A number of variants exist for TEA like extended TEA19, Block TEA and so on. These extensions try to resolve the problems in original TEA like equivalent keys. But still, due to its simple operations TEA and its variant are susceptible to a number of attacks.

z) Present

It is based on SPN and is used as an ultra lightweight algorithm for security. It works on substitution layer uses 4-bit input and output S-boxes for hardware optimization. It has a key size of 80 or 128 bits and operates on 64-bit blocks20. PRESENT has been presented as a lightweight cryptography solution in ISO/IEC 29192-2:2012 “Lightweight Cryptography”21. PRESENT is vulnerable to differential attack on 26 out of the 31 rounds

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

aa) High security and lightweight (HIGHT)

Hight uses very basic operations like addition mod 28 or XOR to work for Feistel network. It has a block size of 64 bits; work in 32 rounds on128 bit keys16. Its keys are generated while encryption and decryption phase. A parallel implementation of high was proposed in17 that require less power, mentioned in few lines of code, and improves speed for RFID systems. High is vulnerable to saturation attack.

bb) Serpent

The serpent is an Advanced Encryption Standard (AES) competition, stood 2nd to Rijndael, is a symmetric key block cipher, designed by Eli Biham, Ross Anderson, and Lars Knudsen. The serpent is a symmetric key algorithm that is based on substitution-permutation network Structure. It consists of a 128-bit plain text with 32 rounds and a variable Key Length of 128, 192 and 256 bit. It also contains 8 S- boxes and same algorithm is used in reverse for decryption. Security presented by Serpent was based on more conventional approaches than the other AES finalists. The Serpent is open in the public sphere and not yet patented.

cc) Asymmetric (public) Key Cryptography

This cryptographic method makes use of two different algorithms for encryption and decryption respectively, a public key for encryption and a private key for decryption. The public key of the sender is used to encrypt the message by the sender. The receiver decrypts the ciphertext with the help of a private key. The description of some widely used Asymmetric key cryptographic algorithms is given below

dd) RSA

RSA (Rivest-Shamir-Adleman) is generallysecond-hand an asymmetric encryption /decryption algorithm which involves a communityinput and a confidential key. The community key can be informed to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. It secured user data assimilate encryption before to storage, user authentication procedures prior to storage or retrieval, and making secure channels for data transmission. 4096-bit key size is used for execution of RSA algorithm. RSA algorithm involves these steps: 1. Key Generation 2. Encryption 3. Decryption

ee) DIFFIE-HELLMAN

The scheme was first revealed by Whitfield Diffie and Martin Hellman in 1976. Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It permits two parties that have no prior knowledge of each other to jointly make a shared secret key over an insecure communications channel. This key can then be used to encrypt posterior communications using a symmetric key cipher.

ff) PAILLIER

The Paillier cryptosystem is an asymmetric algorithm. It has homomorphic property permits this scheme to do normal addition operations on several encrypted values and achieving the encrypted sum, the encrypted sum can be decrypted later without even knowing the values ever that made up the sum

gg) ElGamal

El-Gamal is the asymmetric key cryptography. It is a public key cryptography which is based on Diffie Hellman key exchange. It was introduced by Taher El-Gamal in 1985. It is consist of signature, encryption algorithms as well as discrete logarithm problems. ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm

hh) Elliptic Curve Cryptography (ECC)

PKC algorithm is based upon elliptic curves. ECC can presentlevel of safety with little keys similar to RSA and additional PKC method. It was designed for devices with limited computing power and/or memory, such as smart cards and PDAs

ii) DSA

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

The digital name Algorithm (DSA) is a centerin order Processing normal for Digital signature. It was proposed by National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard. The key generation in DSA has two phases. Aprimarystage is anoption of algorithm parameter which may be communallyflanked bydissimilar users of the scheme. The second phase computes the public and private keys for a single user.

jj) OAEP (OPTIMAL ASYMMETRIC ENCRYPTION PADDING)

OAEP was introduced by Bellare and Rogaway. Optimal Asymmetric Encryption Padding (OAEP) is a padding scheme often used together with RSA encryption. The OAEP algorithm is a form of Feistel network which uses a pair of random oracles G and H to process the plaintext prior to asymmetric encryption. When combined with any secure trapdoor one-way permutation, this processing is proved in the random oracle model to result in a combined scheme which is semantically secure under chosen plaintext attack. When implemented with certain trapdoor permutations (e.g., RSA), OAEP is also proved secure against chosen ciphertext attack. OAEP can be used to build an all-or-nothing transform.

IV. COMPARISON

S.No	Name Of The Techniques	Author name	Algorithm	Confidentiality or security	Key sizes	Focus area
1.	*AES*	Md. AlamHossain, Md. BiddutHossain	Symmetric algorithm	High secure	128,192,256 bits	AES cipher is noted as a number of repetitions of the transformation of rounds which converts the plaintext input into the text output which cannot be able to read by a human.
2	*DES*	Vineet Kumar Singh	Symmetric algorithm	Proven Inadequate	56 bits	DES is a symmetric cryptographic algorithm used for encryption and decryption of the message
3.	*3DES*	RandeepKaur, SupriyaKinger	Symmetric algorithm	Considered Secure	112, 168 bits	3DES requires always moretime than DES because of its triple phaseencryption characteristics.
4.	*BLOWFISH*	Md. AlamHossain, Md. BiddutHossain	Symmetric algorithm	Considered Secure	32-448 bits	It is only suitable for application where there is no change in key, often like communications link or an automatic file encryption.
5.	*RC4*	B.Nithya, Dr.P.Sripriya	Symmetric algorithm	No longer considered secure.	Variable size	The algorithm is serial as it requires successive exchanges of state entries based on the key sequence

V. CONCLUSION

In a cloud-based system, there are yet many practical dilemmas which have to be solved. Cloud computing is a difficult tool with reflective implications not only for Internet services but also for the Information Technology sector as a whole. Still, some wonderful issues continue living, mostly related to service-level agreements (SLA), safety and time alone, and power efficiency. As described, current protection has a lot of loose ends which scares away a lot of prospective users. In anticipation of a proper safety part is not in a position, possible users will not be capable to power the reward of this technology. This safety part should supply all the issues arising from all information of the cloud. Each part in the cloud must be analyzed at the worldwide and micro level and an incorporated result must be considered and deployed in the cloud to attract and captivate the possible consumers. Until then, cloud background will stay cloud.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

6.	*International Data Encryption Algorithm (IDEA)*	Zurich and Xuejia Lai	Symmetric algorithm	Inadequate	128 bits	The basic operations are modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied tosub-blocks.
7.	*SEED*	Saurabh Sindhu, Divya Sindhu	Symmetric algorithm	Considered Secure	128-bit	It has the Feistel structure with 16 rounds and is strongagainst differential cryptanalysis and linear cryptanalysis balanced with security/efficiency trade-off.
8.	*ARIA*	Saurabh Sindhu, Divya Sindhu	Symmetric algorithm	Considered Secure	128-, 192- and 256-bit	The algorithm uses a substitution-permutation network structure based on AES.
9	*TEA*	Wheeler, D.J., & Needham	Symmetric algorithm	Inadequate	128-bit with variable	It does not contain S- boxes and same algorithm is used in reverse for decryption
10	*CAST*	Heys, H.M.; Tavares, E	Symmetric algorithm	Considered secure	40 to128-bit	The CAST is a block cipher that uses a 64-bit plain text with 12 or 16 rounds and a variable Key Length of 40 to128-bit
11	*Triple DES*	AamerNadeem and Dr M. YounusJaved	Symmetric algorithm	Insecure	192-bit	Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block
12	*TWO FISH*	Bruce Schneier	Symmetric algorithm	Secure process	128, 192 and 256 bits	It is efficient for software that runs ona smaller processor (smart cards) and embedding in hardware
13	*THREE FISH*	Bruce schneier, Niels Ferguson, Stefan Lucks, Doug Whiting	Symmetric algorithm	Secure process	256, 512 or 1024 bits	Threefish-1024 one round of encryption having plaintextblock and sub-key with tweak value.
14	*RC5*	K. Abdullah	Symmetric algorithm	Secure process	0 to 2040 bits	It is suitable for hardware and software implementation because it uses only those operations which are available in the typical microprocessor
15	*Skipjack algorithm*	DiaaSalama, Abdul Minaam, Hatem M. Abdual-Kader	Symmetric algorithm	Less Secure process	80 bits	The key to the encrypted message is itself encrypted with a key combined from two escrowed keys.
16	*Tiny Encryption Algorithm (TEA)*	Wheeler DJ, Needham RM	Symmetric algorithm	Secure process	128 bits	TEA is used for constrained environments like sensor networks or smart things
17	*PRESENT ALGORITHM*	Derbez P, Fouque PA	Symmetric algorithm	Secure process	80 bits	It is based on SPN and is used as an ultra lightweight algorithm for security
18	*High security and lightweight (HIGHT)*	Devadiga K.	Symmetric algorithm	Secure process	128 bits	A parallel implementation of high was proposed in17 that require less power, mentioned in few lines of code, and improves speed for RFID systems

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 5, Special Issue 12, April 2018

19	*Serpent*	Eli Biham, Ross Anderson, and Lars Knudsen	Symmetric algorithm	Secure process	128, 192 and 256 bit	Security presented by Serpent was based on more conventional approaches than the other AES finalists.
20	*RSA*	B.Nithya, Dr.P.Sripriya	Asymmetric algorithm	Considered secure	Minimum 512 bits.	RSA is an asymmetric cryptographic algorithm which is also used forencryption and decryption of the message
21	*DIFFIE-HELLMAN*	Whitfield Diffie and Martin Hellman	Asymmetric algorithm	Not secure	--	It is a technique for securely exchanging cryptographic keys over a public network and was the primary specific example of public-key cryptography.
22	*PAILLIER*	Saurabh Sindhu, Divya Sindhu	Asymmetric algorithm	Inadequate	--	It has homomorphic property permits this scheme to do normal addition operations on several encrypted values and achieving the encrypted sum
23	*ElGamal*	Md. ShafinUddin, Shariar Md. Imtiaz	Asymmetric algorithm	Not secure	1024 bits	It is consist of signature, encryption algorithms as well as discrete logarithm problems
24	*Elliptic Curve Cryptography (ECC)*	B.Nithya, Dr.P.Sripriya	Asymmetric algorithm	Inadequate	Smaller but effective key	ECC can offer levels of security with small keys comparable to RSA and other PKC methods.
25	*DSA*	Uma Somani	Asymmetric algorithm	Not secure	192 bits	The secrecy and uniqueness of random key signature value are critical such that violating any of these requirements can reveal the original secret key to the hacker.
26	*OAEP (OPTIMAL ASYMMETRIC ENCRYPTION PADDING)*	Bellare and Rogaway	Asymmetric algorithm	Not secure	1024 bits	Optimal Asymmetric Encryption Padding (OAEP) is a padding scheme often used together with RSA encryption.

REFERENCES

[1] William Stallings, "Cryptography AndNetwork Security: Principles and Practice second edition", ISBN 0-13869017- 0, 1995 by Prentice- Hall, Inc. Simon & Schuster / A Viacom Company Upper Saddle River, New Jersey 07458.

[2] Md. AlamHossain, Md. BiddutHossain, Md. ShafinUddin, Shahriar Md. Imtiaz, "Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 3, March 2016.

[3] Swati Kashyap, Er.NeerajMadan "A Review on Network Security and Cryptographic Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, April 2015.

[4] B.Nithya, Dr.P.Sripriya, "A Review of Cryptographic Algorithms in Network Security" International Journal of Engineering and Technology (IJET) Vol 8 No 1 Feb-Mar 2016.

[5] Saurabh Sindhu, Divya Sindhu, "Cryptographic Algorithms: Applications in Network Security", International Journal of New Innovations in Engineering and Technology Volume 7 Issue 1– February 2017.

[6] PrernaMahajan&AbhishekSachdeva,"A study of Encryption Algorithms AES, DES and RSA for

Security", Global Journal of Computer Science and Technology, Vol.8,No.15, (2013) pp.15-22.

[7] Jitendra Singh Laser, Viny Jain, "A Comparative Survey of various Cryptographic Techniques" International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 03 | Mar-2016.

[8] PriyankaArora, Arun Singh, HimanshuTyagi " Evaluation and Comparison of Security Issues on Cloud Computing Environment" in World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221- 0741 Vol. 2, No. 5, 179-183, 2012.

[9] E. Thambiraja, G. Ramesh and Dr R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 226-233, July 2012.

[10] PushpendraVerma, DrJayantShekhar, Pretty,AmitAsthana, "A Survey for Performance Analysis Various Cryptography Techniques Digital Contents", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015, pg. 522-531

[11] SwetaK.Parnar,Prof. K.C.Dave,"A review on various most common symmetric encryption algorithm",InternationalJournal for scientific research and development, volume 1,issue 4,2013

[12]S.Artheeswari,Dr.RM.Chandrasekaran,"INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) FOR DATA SECURITY IN CLOUD", International Journal of Technology and Engineering System (IJTES)

[13] Vineet Kumar Singh, DrMaitreyeeDutta "ANALYZING CRYPTOGRAPHIC ALGORITHMS FOR SECURE CLOUD NETWORK" International Journal of advanced studies in Computer Science and Engineering IJASCSE Volume 3, Issue 6, 2014.

[14] S C Rachana, Dr H S Guruprasad, "Emerging Security Issues and Challenges in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, March 2014, and ISSN: 2319- 5967.

[15] RajdeepBhanot and Rahul Hans," A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306

[16] M. Kumar and E. G. Dharma, "A comparative analysis of symmetric key encryption algorithm", IJARCET, vol. 3, no. 2, (2014).

[17] RandeepKaur, SupriyaKinger "Analysis of Security Algorithms in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, March 2014, ISSN 2319 – 4847.

[18] Christopher Yale Crutchfield "Security Proofs for the MD6Hash Function Mode of Operation", Massachusetts Institute of Technology2008.