JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

An Efficient Survey on Cloud Security Algorithms

M. Subhashini[1*], P. Srivaramangai[2]

[1*] Dept. of Computer Science, Maruthu pandiyar college of Arts & Science, Thanjavur

[2] Dept. of Computer Science, Maruthu pandiyar college of Arts & Science , Thanjavur..

Available online at: www.ijcseonline.org

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 favored 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 encrypt 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 technical participation is that the proxy re-encryption technique supports encryption operations over encrypted text as well as forwarding actions over 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, cyber security, 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 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.

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 status of a CCS depends on many factors, including security applications running on the system, the hypervisor (HV) and associated protection measures, the design patterns used to isolate the control plane from cloud tenants, the level of protection provided by the CSP to cloud tenant user data and VM images, as well as other factors.

SECURITY PROXY RE-ENCRYPTION

In a proxy re-encryption scheme, a substitute server can relocate a cipher text 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 storage 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. Thus, their system has data discretion and supports the data forwarding purpose. Our work additional integrates encryption, re-encryption, and encoding.

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 based on a Bayesian network model of the CCS, the class of APT attack paths spanning the CCS attack space, and the APT attack steps required to implement each attack path.
- ❖ It provides two key high-level security metrics to summarize CCS security status quantitatively: The first security metric estimates whether high value Data.
- ❖ The second metric assesses whether the CSP provides cloud tenants sufficient CCS network monitoring, file access, and situation awareness data to detect intrusions into a tenant’s cloud network, and whether the tenant’s security and monitoring systems contribute to the intrusion detection.
- ❖ The second metric assesses whether the CSP provides cloud tenants sufficient CCS network monitoring, file access, and situation awareness data to detect intrusions into a tenant’s cloud network, and whether the tenant’s security and monitoring systems contribute to the intrusion detection.

II. RELATED WORKS

[1] Existing permission mechanisms fail to provide powerful and robust tools for handling safety at the scale necessary 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 "increased flexibility through programmability" trend seems to be accelerating with the arrival of proposals such as Active Networking and Mobile Agents. The trust-management advance to distributed-system protection was urbanized as an respond to the insufficiency of traditional agreement mechanisms. Trust-management engines shun the want to resolve "identities” in an authorization decision. Instead, they express rights and restrictions in a encoding language. This allows for augmented elasticity and impressibility, as well as 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 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 investigates the function of Nimbus as a cloud reserve and shows an example realization for retaining data manage to the user based on virtual machine descriptions 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] Cloud computing systems fundamentally provide access to large pools of statistics and computational possessions

during a assortment of interfaces like in spirit to existing grid and HPC resource management and programming system. These types of systems offer a new indoctrination aim for scalable request developers and have gained popularity over the history few years. However, most cloud computing systems in process today are proprietary, rely upon infrastructure that is unseen to the explore culture, or are not clearly calculated to be instrumented and modified 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 middle-ware.

II. METHODOLOGY

EXISTING ALGORIHM

RSA

The enhanced conclusion of this paper is RSA and ECC perception. **RSA** is an algorithm used by current computers to encrypt and decrypt mail.

ASYMMETRIC CRYPTOGRAPHIC ALGORITHM

It is an asymmetric cryptographic algorithm. Asymmetric income that there are two diverse keys. This is also called community key cryptography; since one of them can be given to each individual the other key should be kept confidential. Elliptic curve cryptography (ECC) is a draw near to public-key cryptography base on the algebraic structure of elliptic curves above finite fields.

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.

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 cipher texts C1,C2, . . . ; Ck. An original cipher text 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 cipher text 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 cipher texts and provisions the encoded result (codeword symbol) Encryption. Encoding is main part in the data storeroom.

DATA FORWARDING

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. When at least t key servers respond, A recovers the first section a1 of the secret key SK_A via the Key Recover 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 using $RK^{ID}_{A->B}$ a storage server re-encrypts the unique password symbol C0with the identifier ID into a re-encrypted codeword symbol C'' via the ReEnc Þ algorithm such that C'' is decrypt 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}.).

DATA RETRIEVAL

There are two cases for the data recovery stage. The first container is that a user A retrieves his own communication. When user a 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 gathering and combining parts are the equal as the first case except that key servers retrieve re-encrypted codeword symbols and perform fractional decryption Share-Decrypted on re-encrypted codeword symbols.

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 cipher text Ci and sends it to v erratically select storage servers. Upon receiving cipher texts from a user, each storage server linearly combines them with arbitrarily selected coefficients into a secret word symbol and stores it. Note that a storage server may receive less than k meaning blocks and to assume that all storage servers know the worth k in progress. elevant details should be given including experimental design and the technique (s) used along with appropriate statistical methods used clearly along with the year of experimentation (field and laboratory).

Table 1: A Comparative Performance Evaluation on Different Algorithms

S. NO	***NAME OF THE ALGORITHM***	***MERITS***	***DEMERITS***	***FOCUSING AREA***
1.	**RSA Algorithm**	1 To provide both secrecy and digital signature. 2. Resistance to noise and outliers.	1. Not Scalable process 2. Encryption and decryption process is slower 3. Brute Forced and Oracle attack occur	Public and private key
2.	**Asymmetric Cryptographic Algorithm**	elliptic curve cryptography (ecc) is a draw near to public-key cryptography base on the algebraic structure of elliptic curves above finite fields	The Other Key Should Not Be Kept Confidential.	It is an asymmetric cryptographic algorithm. Asymmetric income that there are two diverse keys
3.	**System Setup**	A customer uses KeyGen to create his community and secret key pair and ShareKeyGen to divide his secret key	No security of key process	The algorithm SetUp (1) generates the arrangement parameters. A customer uses KeyGen to create his community and secret key pair
4.	**Data Storage**	He Computes The Uniqueness Voucher And Performs The Encryption Algorithm Enc K Blocks To Get K Original Cipher Texts	Cipher text is not set	Encode on the set of k cipher texts and provisions the encoded result (codeword symbol) Encryption.
5.	**Data Forwarding**	The Secret Key SK_A Via The Key Recover Algorithm	Less Key Security	The Re KeyGen algorithm and steadily sends the re encryption key to each storeroom server.
6.	**Data Retrieval**	user needs to recover the significance with the identifier ID	Less quality	A key server first retrieves unique key cryptogram from u arbitrarily chosen storeroom servers
7.	**DATA STORAGE PHASE**	User A encrypts each block mi into a cipher text Ci and sends it to v erratically select storage servers	Less arbitrary storage	Receiving cipher texts from a user, each storage server.

III. CONCLUSION

I In a cloud-based system, there are yet many practical dilemmas which have to be solved. Cloud computing is a difficult tools 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 effectiveness. As described, currently protection has lot of loose ends which scares away a lot of prospective users. In anticipation of a proper safety part is not in position, possible users will not be capable to power the reward of this technology. This safety part should supply to 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 cloudy.

REFERENCES

[1] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," *NIST Spec. Publ.*, pp. 800–144, 2011.

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing." NIST, 2011.

[3] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud Migration Research: A Systematic Review," IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 142–157, 2013.

[4] L. Vaquero, L. Rodero-Merino, and D. Morán, "Locking the sky: a survey on IaaS cloud security," *Computing*, vol. 91, no. 1, pp. 93–118, Jan, 2011 **.**

[5] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in thirdparty compute clouds," in Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 199–212.

[6] Sakshi kathuria, "*A Survey on Security Provided by Multi-Clouds in Cloud Computing*", International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.1, pp.23-27, 2018.

[7] B. Krekel, "Capability of the People's Republic of China to conduct cyber warfare and computer network exploitation," U.S.-China Economic and Security REview Commission, Northrop Grumman Corp., DTIC Document, 2009.

[8] *FedRAMP Security Controls*, Federal Chief Information Officer's Council, [Online]. Available: http://cloud.cio.gov/document/fedramp-security-controls. [Accessed: 29-Oct-2014].

[9] S. Zevin, Standards for security categorization of federal information and information systems. DIANE Publishing, 2009.

[10] M. Walla, "Kerberos Explained," May, 2000. [Online]. Available: http://technet.microsoft.com/en-us/library/bb742516.aspx. [Accessed: 12-Jan-2014].

Authors Profile

Mr. C T Lin pursed Bachelor of Science from University of Taiwan, Taiwan in 2006 and Master of Science from Osmania University in year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computational Sciences, Department of Electronic and Communication, University of Taiwan, Taiwan since 2012. He is a member of IEEE & IEEE computer society since 2013, a life member of the ISROSET since 2013, ACM since 2011. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 5 years of teaching experience and 4 years of Research Experience.

Mr C H Lin pursed Bachelor of Science and Master of Science from University of New York, USA in year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Telecommunication, University of New York, USA since 2012. He is a member of IEEE & IEEE computer society since 2013, a life member of the ISROSET since 2013 and ACM since 2011. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 5 years of teaching experience and 4 years of Research Experience.