International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Literature Survey on Obliterate of Secure Data using Universal Validation

Anvitha P Raj[1] and Sunil B N[2]

[1]*Student,MTech, Dept of CS&E ,Sahyadri College of Engineering and Management, Adyar,Mangalore,India*

[2]*Assistant Professor, Dept of CS&E ,Sahyadri College of Engineering and Management, Adyar,Mangalore,India*

Abstract - *The ability to securely delete sensitive data from storage is becoming important. Cloud computing is an emerging computing technology that uses the internet and central remote serves to maintain data and applications. With the cloud computing, data security becomes more and more important in cloud computing. In this method some important security services including authentication, encryption and decryption are provided in cloud computing. Existing software based data erasure program can be summarized as following the same one-bit-return protocol: the deletion program performs data erasure and returns either success or failure. However, such a one bit-return protocol turns the data deletion into black box-the user has to trust the outcome but cannot easily verify it. In order to make the data deletion more transparent and verifiable cryptographic solution is used.*

Key Words: **Secure Deletion, Data Security, Storage, TPM, Encryption.**

INTRODUCTION

With the development of cloud computing data security becomes more and more important in computing. Securely deleting data from storage system has become difficult today. Common deletion operations simply mark the occupied space as free and remove an entry from the directory, but some of the stored data may remain accessible for much longer.

Explores the use of encryption and key management for securely deleting data [1].When data is stored encrypted, only the corresponding key has to be destroyed for erasing the data. Deleting data becomes a problem of managing and deleting keys. A cryptographic solution is presented for deletion that makes the data deletion process more transparent and verifiable. Here introduce an assumption that sits in between namely "trust-but verify". Generally users assumes that when they delete a file, all the blocks that store the file are physically erased. However, traditional file deletion simply removes the metadata of the file, but leaves the file data intact [1].This may violate user privacy, because the deleted file can be easily recovered.

Another general misconception is that if a file was overwritten, the previous version of the file cannot be restored. In case of magnetic media such as a hard disk, the file can still be recovered, even if the file data was overwritten. There are two types of secure deletion schemes, overwriting and encryption [2].TPM communicates with host, following a secure storage and erasure (SSE) protocol. This is the central element in the entire system design.

LITERATURE SURVEY

In this section, we are presenting the research work of some prominent authors in the same arena and explaining a short report of various methods used for secure data in cloud computing.

Akli Fundo, Aitenka Hysi Igli Tafa ,[2] In this paper author analysed same techniques of erasing data from the disk from hard drives can also be used on SSD's. For erasing a file from hard drive from SSD's cannot use a same technique, in order to make this possible, some charges are required in file layer, file layer is used for mapping between physical address and logical address .Here author tried to analyse different methods to erase data from SSD's and to see which method gives the best result .Four levels of clearing data from storage media: First level is Logical Clearing: By over writing uses can delete single file or enter disk logically. Second level is Digital Clearing: Here, it is impossible to recover the data in a digital way .Third level is Analog Clearing: Signal which encodes the data is damaged in this level it is impossible to rebuild the signal. Alternative way to hide the bits Cryptographic Clearing: This level uses a key, in order to encrypt and decrypt the data which enter and exit .From

physical media someone can extract the key and can avoid the encryption. By comparing these methods author realized that first method ,had a half success , second method is more successful than first method .It has some fails in it, third method ,is of no use because it does not guarantee the deletion .

For secure deletion ,Z.N.J. Peterson, R.Burns, J.Herring, A.Stubblefield, A.D.Rubin these authors here compares two methods that uses a combination of authenticated encryption: Encrypting a file with key and securely disposing of the key to make the data unrecoverable .The files that encrypt data on disk ,data maybe securely deleted by the corresponding encrypt without a key ,data may never be decrypted and read again and secure overwriting: Original data cannot be recovered .secure overwriting has performance concern in versioning systems[3]. For the research and commercial applications versioning storage system are important .Secure deletion is the act of remaining digital information from a storage so that it can never be recovered . Here say that, a data is encrypted and converted into a cipher text block and a small slab. Securely overwriting the slab makes the corresponding block is recoverable. Here they present an two algorithms. First algorithm employs the all-or nothing transform so that securely overwriting a slab or any 128 bit block of a cipher text securely deletes the corresponding disk block .second algorithm generates a random key per block in order to make encryption no repeatable [3].

J.Reardon, D.Basin, S.Capkun, [4] Here in this paper present a taxonomy of adversaries differing in their capabilities as well as a systematization for the characteristics of secure deletion approaches .Characteristics includes environmental assumptions , such as the deletion latency and physical ware. Here in this paper say in detail by organizing the approaches in terms of interfaces to the physical medium. Here they organize secure deletion approaches into the layers through which key address the physical medium. Once secure deletion is implemented at one layer, then the higher layer, interfaces can explicitly offers this functionality. There are two common use level approaches. First, Environmental Assumption: include the expected behaviours of the system underlying the interface. Second, Behavioural Assumption: includes the deletion latency and the wear on the physical medium.

S.Garfinkel, A.Shelat, in this paper, say that there are many ways to assure privacy information. One of the oldest and most common techniques is Physical Isolation: keeping confidential data on computers that only authorized individual can access [5].Cryptography is an another tool that can assure information privacy. User can encrypt data as it is sent and decrypt it at the intended destination using for eg : Secure Socket Layer (SSL)encryption protocol . In absent of cryptographic file system, confidential information is readily accessible when owners improperly retire these disk drives.

D.Boneh, R.Lipton, [6] here in this paper, presents an system which enablesa user to remove a file from both the file system and all backup topics on which the file is stored. Here in this papers, new way of cryptography is applied, here cryptography is used to erase information rather than protect it . the backed up files are stored for extending periods of time it is desirable that the block cipher used to encrypt the files be extremely secure .Here also say about standard UNIX backup utilities ,user enable to specify a collection of files that should not be backed up.

M.Abdalla, M. Bellare and P. Rogaway, This paper provides security analysis for the public key encryption scheme DHIES and is now in several draft standards[7].DHIES is a Diffie Hellman based scheme that combine a symmetric encryption method authentication code , and a hash function ,in addition to number –theoretic operations, in a way which is intended to provided security against chosen – cipher text attacks .this paper also introduce about natural assumptions under which DHIES achieves security under chosen cipher text attack .those assumptions are hash DH assumption (HDH),oracle DH assumption (ODH) and , the strong DH (SDH) [7].

Sarah Diesburg, Christopher Meyers, Mark Stanovich, Michael Mitchell, Justin Marshall, Julia Gould, and An-I Andy Wang [8]. This paper introduces True erase, a holistic secure deletion framework. True erase shows that it is possible to build a legacy-compatible full storage data path framework that performs. Perfile secure deletion and works with common file systems and solid state storage while handling common system failures. In addition, framework can secure as a building block for encryption and tainting based secure deletion system. Here say that may opportunities exists to increase true erase performance on NAND flash.

Mohammed Achemlal, Said Gharout and Chrystel Gaber [9] This paper say about the possibility of using TCG(Trusted Computing Group) specifications to establish trust in cloud computing especially between the provider of cloud computing infrastructure and his customers and also describes the context and the motivations that lead to TCG

specification and also describes the functions and properties of TPM(Trusted Platform Module) which is the root of trust in TCG and also say that several approaches to adopt TPM in order to build trust in cloud computing.

CONCLUSIONS

In this paper, say about an investigation on how to apply the "trust-but-verify" paradigm in order to make data deletion process more transparent and verifiable. Here presents a cryptographic solution, called Secure Storage and Erasure (SSE), which enables a user to verify the correct implementation of cryptographic operations inside a TPM without having to access its internal source code. For secure random number generator future work includes extending the "trustbut verify" paradigm to other crypto primitives. While the "trust-but-verify" paradigm has been well studied and established in some fields (e.g., e-voting), it has been almost entirely neglected in the field of secure data deletion.

REFERENCES

[1] Feng Hao,Member, IEEE, Dylan Clarke, and Avelino Francisco Zorzo, "Deleting Secret Data with Public Verifiability", IEEE Transaction on Dependable and Secure computing, VOL. 13, NO. 6,

NOVEMBER/DECEMBER 2016.

[2] Akli Fundo, Aitenka Hysi,Igli Tafa Polytechnic University of Tirana, "Secure Deletion of Data from SSD" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No.8, 2014.

[3] Z.N.J. Peterson, R. Burns, J. Herring, A. Stubblefield, A.D.Rubin, "Secure Deletion for a Versioning File System," Proceedings of the 4th Conference on USENIX Conference on File and Storage Technologies (FAST), Vol. 4, pp. 143-154, 2005.

[4] J. Reardon, D. Basin, S. Capkun, "SoK: Secure Data Deletion," Proceedings of the 2013 IEEE Symposium on Security and Privacy, pp. 301-315, 2013.

[5] S. Garfinkel, A. Shelat, "Remembrance of

[6] Data Passed: A Study of Disk Sanitization Practices," IEEE Security & Privacy, Vol. 1, No. 1, pp. 17-27, 2003.

[7] D. Boneh, R. Lipton, "A Revocable Backup System," Proceedings 6th USENIX Security

Conference, pp. 91-96, 1996.

[8] M. Abdalla, M. Bellare and P. Rogaway, "The Oracle Diffie- Hellman Assumptions and an Analysis of DHIES," Topics in Cryptology - CT-RSA'01, LNCS Vol. 2020, 2001.

[9] S. Diesburg, C. Meyers, M. Stanovich, A. Wang and G. Kuenning, " TrueErase: Per-File Secure Deletion for the Storage Data Path ", ACM Transactions on Storage, vol. 12, no. 4, pp. 1-37, 2016.

[10] M Achemlal, S.Gharout,C.Gaber, "Trusted Platform Module as an Enabler for Security in Cloud Computing",Proc.Conf. on network and information system security(SAR-SSI),2011.