International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 05
April 2017

Necessity of Security for IoT based Hybrid Cloud for Authorized Deduplication

Shirisha Getty
Department of CSE

ABSTRACT: *Cloud computing is altering the customs software is developed and managedin enterprises, which is altering the way of doing business in that dynamically scalableand virtualized resources are regarded as services over the Internet.The main objective of this paper isData Deduplication, which is an efficient datacompression technique for removing theduplication copies. This work recuperates the two main problems one is Storage issue and other Security issue in cloudcomputing. We have proposed a new technique forduplication check by giving different privileges tousers. And new Convergent Encryption isintroduced to preserve efficient security level whendata is outsourced. The concept of tag and tokenswere introduced. All these procedure is carried inHybrid clouds which includes both the public andprivate cloud.*

KEYWORDS-Cloud,Security, Hybrid, Deduplication, Encryption

I. INTRODUCTION

Cloud computing is receiving a great deal ofattention, both in publications and from individualsto researchers. Cloud computing is a Internet basedcomputing where virtual shared servers providessoftware, infrastructure, platform devices and otherresources to customers on pay-as-you-use basis.The cloud makes it possible to access theinformation from anywhere and at any time acrossthe world unlike a computer which needs a physicallocation to access the information. This computingtechnology is mainly implemented where largeamount of data are being processed which requires ahuge storage space and high security standards. Themain criteria are to have a proper Internetconnection for the computing technique. There aremany definitions today which attempt to addresscloud from the perspective of academicians,architects, engineers, developers, managers, andconsumers. This document focuses on a definitionthat is specifically tailored to the uniqueperspectives of IT network and securityprofessionals. The keys to understanding how cloudarchitecture impacts security architecture are acommon and concise lexicon, coupled with aconsistent taxonomy of offerings by which cloudservices and architecture can be deconstructed,mapped to a model of compensating security andoperational controls, risk assessment andmanagement frameworks, and in turn to compliancestandards.

The Internet of Things (IoT), also called the Internet of Everything or the IndustrialInternet, is a new technology paradigm envisioned as a global network of machines anddevices capable of interacting with each other. The IoT is recognized as one of the mostimportant areas of future technology and is gaining vast attention from a wide range ofindustries. The true value of the IoT for enterprises can be fully realized when connecteddevices are able to communicate with each other and integrate with vendor-managedinventory systems, customer support systems, business intelligence applications, and businessanalytics [1].In this paper, we focus our attention on the integration of Cloud and IoT, which is what wecall the CloudIoT paradigm. The Internet of Things (IoT) paradigm is based on intelligent andself-configuring nodes (things) interconnected in a dynamic and global network infrastructure[2].

II. RELATED WORKS

Laili et al. [6] Proposed a computing resource allocation cloud manufacturing framework (CMfg) anddesigned a highly intelligent algorithm for optimal allocation of computing resources inCMfg. The research provides a new model which can enhance the inefficiencies inservice-oriented manufacturing.

Tao et al. [7] Described the relationship between cloud computing and CMfg. A computing andservice-oriented model with a detailed description and model is proposed in this researchusing the support of IoT, and advanced computing virtualization and service-orientedtechnologies are proposed.

Tao et al. [8] A parallel algorithm for solving large-scale software and hardware cloud services isproposed. Compared with traditional serial intelligent algorithms and classical parallelintelligent algorithms, the results are remarkable and can be applied to other large-scalecomposition service networks.

Xu [9] This research discusses some of the essential features of cloud computing and two types ofcloud computing adoptions in manufacturing and cloud manufacturing. An interoperableand flexible cloud manufacturing system (ICMS) is proposed to provide users with a bigrange of flexible manufacturing capabilities.

Zhang et al. [10] A CMfg prototype and the existing related works conducted by the authors' group on CMfg are briefly presented. Through taking virtual machine mappings as the accessingcarrier, distributed resources are mapped into virtual resources (virtual machine). Severalfunction modules are mainly achieved through related technologies.

Wu et al. [11] A unique strategic vision for cloud manufacturing is documented. Comparison of thestrategy vision and current state leads to suggestions for future work. Some potentialimpacts and future concepts for research are also discussed in this review.

Putnik [12] An introduction to the development concept of ubiquitous and cloud manufacturing ispresented. Architecture through an informal and conceptual presentation of cloudmanufacturing is also discussed, which enables development of an advanced manufacturingsystem or enterprise on different complexity levels.

Chen et al. [13] An innovative technology of virtual COM port technology is proposed in this research. A prototype system is addressed in this paper to implement the concept ofservice-as-a-software cloud computing concept.

Giriraj et al. [14] This paper establishes the value of realizing cloud connects and usage state of affairs in thecloud manufacturing environment. It offers monitoring vision and control and a case studywith the help of a manufacturing execution assembly system. The purpose of the theorypart of the study is to first introduce the concept of cloud connect in the respective field ofa manufacturing execution assembly system.

III. PROPOSED SYSTEM

We have to focus on security aspects also because this is the anothermajor issue in cloud service. So, in this paper wehave compared two standard encryption algorithms,1.SHA-1(Secure Hash algorithm) and 2. HMAC-(Hash based message authentication code)

SHA-1 (Secure Hash Algorithm): It is a most commonly used from SHA series of cryptographic hash functions, designed by the National Security Agency of USA and published as their government standard.SHA-1 produce the 160-bit hash value. Original SHA (or SHA-0) also produce 160-bit hash value, but SHA-0 has been withdrawn by the NSA shortly after publication and was superseded by the revised version commonly referred to as SHA-1. The other functions of SHA series produce 224-, 256-, 384- and 512-bit hash values.

The mainentities in the proposed algorithm are cloud users,cloud storage server, cloud manager, key splitterservers, share holder servers, security servers, logeditor which are defined in detail as follows:

1. User: The user can create, update and deletehis/her profile, store and retrieve the data.

2. Cloud Storage Server: It is a model of datastorage on virtualized storage pools or serverslocated remotely. Cloud storage can be used byusers to store their data. Users can buy storagecapacity from the

cloud hosting companies. Themain responsibilities of cloud storage server arestoring the encrypted document, storing the splitedencryption key values for the purpose of keyManagement.

3. Key Management Server: Key splitter serversplits the encryption keys into different shares andstore the splited keys in different share holderservers.

4. Share Holder Server: These servers store theshares for the different keys for different users.Share holders can be of two types. Primary shareholder directly receives the shares from the cloudmanager. Secondary share holders are the shareholders at the leaf level and these share holdersreceive their shares through primary share holders.

5. Log editor: It checks the share holder serverstimely to see if the shares are getting modified

6. Security server: It has the encryption decryption algorithm.

Encryption process

Step 1- Split the letter of modified plaintext.
Step 2- Assign the position (i) of the letter.
Step 3- Generate the ASCII value of plaintext letter.
Step 4- E=(p+k+i) p-plaintext, k-shared key, iposition
Step 5- Generate the ASCII character of thecorresponding decimal value in the resultfrom the above given formula.
This wouldbe the cipher text.

Decryption process

Step 1- Generate the ASCII value of the cipher text character.
Step 2- Same encryption key is used.
Step 3- Assign the position i of the cipher text.
Step 4- D=((c-k-i)+256) p-plaintext, k-shared key, i-position.
Step 5- Generate the ASCII character of thecorresponding decimal value in the result from theabove given formula. This would be the originalplain text.
File is "padded" with a 1 and as many 0's asnecessary to bring the content length to 64 bitsfewer than an even multiple of 512.
Append Length64 bits are appended to the end of the paddedcontents. These bits hold the binary format of 64bits indicating the length of the original filePrepare Processing FunctionsSHA1 requires 80 processing functions definedas:
f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 <= t <= 19)
f(t;B,C,D) = B XOR C XOR D (20 <= t <= 39)
f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 <= t <=59)
f(t;B,C,D) = B XOR C XOR D (60 <= t <= 79)
Main loop
for i from 0 to 79
if 0 ≤ i ≤ 19 then
if = (b and c) or ((not b) and d)
k = 0x5A827999
else if 20 ≤ i ≤ 39
f = b xor c xor d
k = 0x6ED9EBA1
else if 40 ≤ i ≤ 59
f = (b and c) or (b and d) or (c and d)
k = 0x8F1BBCDC
else if 60 ≤ i ≤ 79
f = b xor c xor d
k = 0xCA62C1D6
temp = (a leftrotate 5) + f + e + k + w[i]
e = d
d = c
c = b leftrotate 30
b = aa = temp

HMAC: Hash-based message authentication code (HMAC)is a mechanism for calculating a messageauthentication code involving a hash function. This
can be used to verify the integrity and authenticity of a message. HMAC depends upon thecryptographic strength of the underlying hashfunction, the size of its hash output, and on the size
and quality of the key

Scenario of Secure Communication

Putting these concepts together, here is how secure communication can be established:
Alice and Bob each generate asymmetric key pairs. They take a hash of their public key and encrypt it with their private key. They then attach the result to the public key itself. This is called self-signing their

public key.Alice and Bob share their public keys with each other. One of them generates a random session key and encrypts it with their private key. They take the result and encrypt it with the public key of the recipient.The receiver uses their private key to decrypt the message, and use the sender's public key to decrypt the result to obtain the random session key. The sender is assured that only the intended receiver is able to obtain the key, and the receiver is assured that only the expected sender could have sent it. From here, they can establish a secure channel using symmetric encryption with the session key. Any eavesdropper on the exchange would not be able to gain access to the session key, and thus could not listen in on the secure channel.

However, there is still one thing missing which makes this communication vulnerable to a man in the middle attack. If Eve is able to tamper with the initial handshake, where the public keys are exchanged, she could pass fake public keys to each side. Alice would think that she received Bob's public key, when in fact she received Eve's public key. Her entire communication would be with Eve directly, who is impersonating Bob, but is also passing the messages to Bob after reading them. Neither is aware that this is happening.

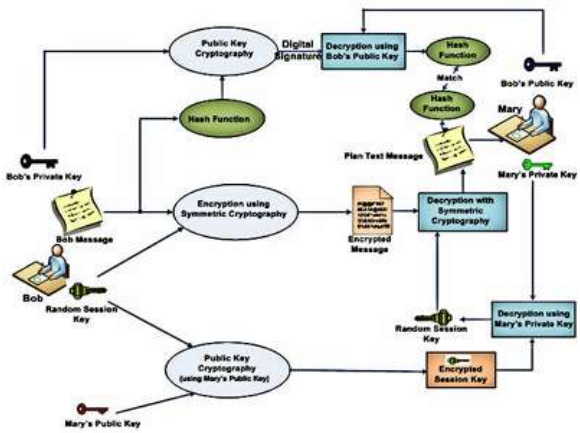

Fig.1Secure Communication

In other words, we can securely communicate with someone and be assured that no one else can eavesdrop, but you cannot be certain about who we are actually communicating with.

IV. CONCLUSION

In this paper proposedtechnique provides improved data security and keymanagement in cloud systems. This technique alsooffers better security against byzantine failure,server concluding and data modification attacks.The cryptographic methods always play a chiefrole in the design of each stage of the keymanagement. The art of the design can be betterevaluated from the conceptual level to theimplementation of the simulation study.

REFERENCES

[1]. In Lee, Kyoochun Lee, (2015) "The Internet of Things (IoT): Applications, investments,and challenges for enterprises", Business Horizons 58, 431—440, Elsevier.

[2]. A. Bott, W.Donato, V. Persico, A. Pescapé, (2016) "Integration of Cloud computing andInternet of Things: A survey", Future Generation Computer Systems 56, 684–700,Elsevier.

[3] P. Huss, N. Wigertz, J. Zhang, A. Huynh, Q. Ye and S. Gong, "Flexible Architecture for Internet ofThings Utilizing an Local Manager", International Journal of Future Generation Communication andNetworking vol. 7, no. 1 , (2014), pp. 235-248.

[4] C. Liu and J. Qiu, "Study on a Secure Wireless Data Communication in Internet of ThingsApplications", International Journal of Computer Science and Network Security, vol. 15 no. 2, (2015),pp. 18-23

[5] R. Fantacci, T. Pecorella, R. Viti and C. Carlini, "Short Paper: Overcoming IoT Fragmentation throughStandard Gateway Architecture", 2014 IEEE World Forum on Internet of Things, (2014), pp. 181-182

[6]. Laili, Y.; Tao, F.; Zhang, L.; Sarker, B.R. A study of optimal allocation of computing resources incloud manufacturing systems. Int. J. Adv. Manuf. Technol. 2012, 63, 671–690.

[7]. Tao, F.; Zhang, L.; Venkatesh, V.C.; Luo, Y.; Cheng, Y. Cloud manufacturing: A computing

andservice-oriented manufacturing model. J. Eng. Manuf. 2011, 225, 1969–1976.

[8]. Tao, F.; LaiLi, Y.; Xu, L.; Zhang, L. FC-PACO-RM: A parallel method for service compositionoptimal-selection in cloud manufacturing system. IEEE Trans. Ind. Inform. 2013, 9, 2023–2033.

[9]. Xu, X. Cloud manufacturing: A new paradigm for manufacturing businesses. Aust. J.Multi-Discip. Eng. 2013, 9, 105–116.

[10]. Zhang, L.; Luo, Y.; Tao, F.; Li, B.H.; Ren, L.; Zhang, X.; Guo, H.; Cheng, Y.; Hu, A.; Liu, Y.Cloud manufacturing: A new manufacturing paradigm. Enterp. Inf. Syst. 2014, 8, 167–187.

[11]. Wu, D.; Greer, M.J.; Rosen, D.W.; Schaefer, D. Cloud manufacturing: Strategic vision andstate-of-the-art. J. Manuf. Syst. 2013, 32, 564–579.

[12]. Putnik, G. Advanced manufacturing systems and enterprises: Cloud and ubiquitous manufacturingand an architecture. J. Appl. Eng. Sci. 2012, 229, 127–134.

[13]. Chen, S.-L.; Wang, H.P.; Chen, Y.Y. Development of software-as-a-service cloud computingarchitecture for manufacturing management systems based on virtual COM port drivertechnology. Appl. Mech. Mater. 2013, 1023, 479–480.

[14]. Giriraj, M.; Muthu, S. A cloud computing methodology for industrial automation andmanufacturing execution system. J. Theor. Appl. Inf. Technol. 2013, 52, 301–307.