© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

DECIMAL ATTRIBUTE BASED ENCRYPTION IN CLOUD SERVER

1AkshitaSaxena, Research Scholar, KIST Bhopal,M.P.
2NitinChaudhary , HOD Department of CS , KIST Bhopal,M.P.

ABSTRACT: This Research presents a comparative study of DECIMAL ATTRIBUTE BASED ENCRYPTION in cloud server and the security issues associated with those systems. In today's networked world, computers rarely work in isolation. They collaborate with each other for the purpose of communication, processing, data transfer, storage etc., when systems work in this collaborative fashion with other systems that are geographically scattered over wide distance it is commonly known as a distributed system. In literature, researchers have used diverse definitions to outline what a distributed system is Inspired by the cloud computing characteristics like pay per use, rapid elasticity, scalable, on demand self service, secure and economical. The motivation for cloud computing was initially driven by large scale resource intensive government application, that require more computational, network and storage resources then a single computer, cloud provides in a single administrative domain. Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage at low cost.

[1] Introduction

Cloud computing system has various advantages over traditional client server architecture of the government information system. Governments around the world have started using cloud computing models instead of traditional client server architecture due to advantages of cloud computing. In many cases government is the leader in deployment of cloud computing model across the wide economy [1]. The government contains general data and information for citizens but it also contains critical data which needs high security.

Security of critical government data is big concern when shifting government data and information on the cloud, so governments are hesitating to adopt cloud computing models and shift their data on them, another reason is the cloud computing is a new concept of the computing and still to get popularity among the governments, but its advantages attracts the governments. As per *Lockheed Martin cyber security alliance survey*: The cloud's non popularity, trust and security concerns have restricted the adoption of cloud computing by the governments which appear to be more perceptual than prohibitive [2]. But now cloud computing is gaining popularity among the people and governments through out the world, so governments are using cloud computing models to provide services to the citizens.

Some of the cloud providers have started providing cloud computing solutions to the government customers and address their specific requirements which includes security, cost saving, reliability etc. *Terremark Worldwide* provides cloud services to U.S. government; it offers high security to the sensitive data of the government [3]. Cloud computing provides infrastructure, platform and software as a service as per requirement of the client, through internet. Advantages of cloud computing solution attract both the private sector and government sector. The main advantage of cloud computing is, it reduces the infrastructure cost by

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

virtualizing the infrastructure like servers, storage devices etc.

Cloud Computing offers scalable services as per requirement of the client. These services include infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), based on off-premises, pay per use, operational model. The companies can get benefit from cloud computing in many ways, by adopting cloud computing model companies can build cloud ready data centers, companies can use resource as a service model and pay for the services they have used [5]. By using resource as services, governments can concentrate on their core services for public without worrying about the maintenance and upgradation of the infrastructure. Governments can reduce the expenses, increase productivity of their current information technology services by using cloud computing model. Government can also provide more efficient services to their citizens by using cloud computing [6].

Cloud computing service provider offers four basic deployment models, the client can choose any of these models as per their requirement. The four models include: (1) Private cloud: - for high security, in clients control and single company, (2) Community cloud: - used by multiple similar companies, (3) Public cloud: - control remains with the provider, any one can use it, for multiple companies (4) Hybrid Cloud: - combination of tow or more of above discussed models, sharing of data and utility [7]. Hybrid cloud combines both public and private cloud models. Agencies are adopting hybrid cloud computing model, where they can use benefits of public cloud and security of private cloud. With hybrid cloud, customers can avail services of 3rd party cloud provider which increases computing flexibility. Hybrid cloud environment can provide as per need and scalable services to the client agencies. In hybrid cloud model, if necessary the resources of private cloud can be increased from the public cloud, so the resources can be easily managed as per the increase or decrease in workload [8].The main advantage of using private cloud as a part of the hybrid cloud is security. Private cloud is more secure as compared to the public cloud. The advantage of using public cloud as a part of hybrid cloud is its public nature and many other advantages like pay per use and low cost etc.

Community cloud can also be used in the hybrid cloud model. Some agencies are concentrating on government efforts in adoption of cloud computing and providing service where other government agencies can obtain these services. The General Services Agency (GSA) is one of the agencies which provide such services. In the beginning GSA is planning to create and provide public cloud resources to the public cloud providers. In the next step private and hybrid cloud resources are proposed to be created to provide necessary services to the various government agencies [9].

[2] Motivation and Problem statement

Problem statement

Cloud server security is sometimes more than what people always thought it to be,malware, virus, Trojan, hackers. Cloud server security could be caused by unintentional human error and it could be compromised by human nature as well.

A common Distributed network security problem (Employees) most organizations are facing sometimes has to do with the company's employees and their various errors they make.

According to Dr. Michael E. Whitman, CISM, CISSP, and the author of the textbook "Principals of Information Security, "Humans make mistakes; sometimes that is due to inexperience or improper training, and sometimes it because an incorrect assumption was reached. But

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

regardless of the reason and the lack of malicious intent—something as simple as a keyboarding error has the potential to cause a worldwide Internet outage". (Whitman and Mattord 2012) The problem of piracy is another common network problemPiracy is a situation where intellectual properties are compromised although there are technical mechanisms that aid in enforcing copyright laws to tackle this problem.However it is not only human errors that can cause problem to network security, problems can also be caused by natural forces like fire breakouts, earthquakes, floods lightning etc.

The ways network administrators think about securing networks has been changed by an increasingly dynamic and technically challenging risk environment

Security of Distributed network

During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. While cryptography is necessary for secure communications, it is not sufficient. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense.The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

[3] Survey of earlier work

In December 2012 Network Security Using Cryptographic Techniques by SumedhaKaushik, AnkurSinghal :

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions,

characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Only one particular element underlies many of the security mechanisms in use:

Cryptographic techniques; hence our focus is on this area Cryptography. Cryptography is an emerging technology, which is important for network security. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured communication.

C. Sanchez-Avila et.al analyzed the structure and design of Rijndael cipher (new AES), remarking its main advantages and limitations, as well as its similarities and dissimilarities with DES and T-DES. Finally, a performance comparison among new AES, DES and T-DES for different microcontrollers has been carried out, showing that new AES have a computer cost of the same order than the one needed by T-DES [4]. A. Murat Fiskiran et.al showed some cryptographic

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

algorithms that have properties that make them suitable for use in constrained environments like mobile information appliances, where computing resources and power availability are limited characterization of the instructions executed by these algorithms, and demonstration that a simple processor is sufficient.

Susan et.al concluded that the Security field is a new, fast moving career. A focus on security stabilizes course material, reduces worry about student hacking, and helps to provide students the skills necessary to become security analysts. It also defines the set of skills required by Network Security analysts as network Security skills emphasize business practices, legal foundations, attack recognition, network optimization and describes active learning exercises that assist the students in learning these important skills. This actually summarized all the skills relating to network security, and discussed active learning exercises that assist students in learning these important skills. Main focus was on security information skills that are to be used in securing the network

NeetuSettiaet. al discussed the security and attack aspects of cryptographic techniques and also discussed the dominant issues of security and various attacks. Finally, bench marked some well-known modern cryptographic algorithms in search for the best compromise in security. In this paper,CrypTool was used as a simulator to conduct the experiments and to get the result.

PunitaMeelu et.al presented the fundamental mathematics behind the AES algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security since AES provides better security and has less implementation complexity and has emerged as one of the strongest and most efficient algorithms in existence today.

Zhang et.al focused on application level attacks and explores how the packet payload can be used for identifying application level attacks. It also discusses the current status of network anomaly detection, and emphasized the importance of payload based detection research using existing problems, and proposed an efficient method to detect payload related attacks. The method is divided into a training phase and a detection phase

[4] Tools and technology used

HARDWARE

- CPU 1Ghz or more
- HARDDISK (5GB Free space)
- DVD ROM
- MONITOR (HIGH RESOLUTION)
- KEYBOARD/MOUSE

SOFTWARE

- WINDOWS 7/8
- MATLAB
- JDK 1.5
- NETBEANS

Attribute based encryption

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is possible only if

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 06 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

the set of attributes of the user key matches the attributes of the ciphertext.[1] A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

The concept of **attribute-based encryption** was first proposed by AmitSahai and Brent Waters [2] and later by VipulGoyal, OmkantPandey, AmitSahai and Brent Waters.[3]Recently, several researchers have further proposed Attribute-based encryption with multiple authorities who jointly generate users' private keys

Usage of Attribute based encryption

Attribute-based encryption (ABE) can be used for log encryption.[10] Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys usedAlthough ABE concept is very powerful and a promising mechanism, ABE systems suffer mainly from two drawbacks: non-efficiency and non-existence of attribute revocation mechanism Other main challenges are:

- Key coordination
- Key escrow
- key revocation

Efficiency

Attribute revocation mechanism

Revocation of users in cryptosystems is a well studied but nontrivial problem. Revocation is even more challenging in attribute-based systems, given that each attribute possibly belongs to multiple different users, whereas in traditional PKI systems public/private key pairs are uniquely associated with a single user. In principle, in an ABE system, attributes, not users or keys, are revoked. Now discuss how the revocation feature can be incorporated. A simple but constrained solution is to include a time attribute. This solution would require each message to be encrypted with a modified access tree T0, which is constructed by augmenting the original access tree T with an additional time attribute.

[5] Conclusion

cipot xelpmoc yrev a si ytiruceS. ot tnatropmi yrev si tI eht taht yaw a hcus ni skrowten dna smetsys duolc dliub metsys ytiruces eht fo dedniamer yltnstsnoc ton si resu mih dnuora. ytiruces dnif ohw sresUpolicies and systems too restrictive will find waysaround them. The proposed system is implemented ti os stpecnoc gnidaerht no desab emit eht secuder ti ecneh noitazilitu UPC eht secuder noitpyrced dna noitpyrcne eht rof deriuqer. desoporp ehT txet no detset yllufsseccus si metsys. fo elacs eht sA worg ot seunitnoc gnitupmoc etubirtsid, fo ytilbailer eht noitciderp eruliaf dna laicurc erom semoceb metsys eht metsys ni elor rojam a yalp smsinacem noitcerroc dna ytilbailer. yb elbixelf yrev si gnitupmoc duolc ehT namuh ecnahne hcihw evitacinummoc daolkrow gnicuder noitacinummoc namuh ot. yb eussi ytilbailer sserdda eW rof metsys tnemeganam tluaf tneiciffe na gnipoleved metsys detubirtsid. neeb evah seuqinhcet suoiraV gnitupmoc duolc ni stluaf gnitceted rof desoporp. Attribute-based encryption (ABE) can be used for log encryption.[10] Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes.

From all the available distributed and centralized systems, four most commonly used distributed systems were discussed in depth and then the security issues faced by these systems and the solutions proposed by various researchers were discussed in depth. Finally the security

issues and solutions proposed for different systems were summarized and compared with each other. eht erutuf nI evititepmoc dna wen eht poleved ot neek era srohtua detubirtsid eruces fo tnempoleved eht rif sehcaorppa smetsys.

References

]1[.leenerP traB , ASR eht ta kcarT 'srehpargotpyrC ehT" "ecnerefnoc, 2005, retupmoc ni seton erutceL ecneicS3376 ,springer-Verlag ,pp .29-43 ,extended version :http//:eprint .iacr.org/2004/222 ./

]2 .[Ilango Sriram ,"Distributed ,Parallel and Cluster computin"g, 2009, aSimulation Tool Exploring Cloud-Scale Data Centres, In: CloudCom 2009, LNCS 5931, pp. 381-392, 2009

]3 .[S ,esevoneG erotava"Akamai Introduces Cloud-Based Firewall Provides a scalable edge defense system for blocking Web application attacks in the cloud", 2009.

http://cloudcomputing.sys-con.com/node/1219023.

]4 ecnarg miT dna llim reteP .[, "The NIST Definition of Cloud Computing", 2011, National Institute of Standards and Technology ,Gaitherbsburg,MD 20899-8930, noitacilbuP laicepS TSIN800-145.

]5 remsseM nellE .[, "New security demands arising for virtualization, cloud computing", 2011, http://www.networkworld.com/article/2178628/virtualization/gartner--new-security-demands-arising-for-virtualization--cloud-computing.html

]6 .[SumedhaKaushik dnaAnkurSinghal ,"Network Security Using Cryptographic Techniques "2012 , volume 2, eussI12.

[7]. Charles Miers, Fernando Redigolo dna Marcos Simplicio ,"A quantitative analysis of current security concerns and solutions for cloud computing",2012 ,*Journal of Cloud Computing: Advances, Systems and Applications* doi:10.1186/2192-113X-1-11

The electronic version of this article is the complete one and can be found online at:http://www.journalofcloudcomputing.com/content/1/1/11

[8]. Rabi Prasad Padhay, "An Enterprise Cloud Model for Optimizing IT Infrastructure" ,2012 ,International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.3, pp. 123~133 ISSN: 2089-3337ttp://iaesjournal.com/online/index.php/IJ-CLOSER

[9]. Nelson Gonzalez, et. al. ,"A quantitative analysis of current security concerns and solutions for cloud computing",2012 ,*Journal of Cloud Computing: Advances, Systems and Applications* doi:10.1186/2192-113X-1-11The electronic version of this article is the completeone and can be found online at:http://www.journalofcloudcomputing.com/content/1/1/11

]10[. CSA "Security Guidance for Critical Areas of Focus in Cloud Computing", (2009), Tech. rep., Cloud Security Alliance.