THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

A Review of Security Algorithms in Cloud Computing

Virangna Pal
B.Tech. Student, Department of Computer Science,
Vellore Institute of Technology, Vellore, Tamil Nadu, India
Prasanth Chowdary
B.Tech. Student, Department of Computer Science,
Vellore Institute of Technology, Vellore, Tamil Nadu, India
Prabhakar Gaur
B.Tech. Student, Department of Computer Science,
Vellore Institute of Technology, Vellore, Tamil Nadu, India

Abstract:
Cloud Computing is method of computation that allows for storage and access to information over the web, as compared to the traditional use of hard drives. Due to its numerous benefits, the most important of which being access to the information from any place and time, the field of cloud computing has seen phenomenal growth amongst individual users and enterprises alike in the past few years. These administrations are conveyed by an outside supplier, in the form of Infrastructure, Platform, Software as services. The number of clients that store their information on the Cloud multiplies, the need for security the customer's information becomes pertinent. In this paper, we audit the algorithms that are currently used in providing security in all cloud based transactions in the premise of various constraints, for example, mechanism, features, and so on.

Keywords: *Security algorithms, Cloud, Data security*

1. Introduction

The cloud storage model allows for data to be kept in virtualized pools of different capacities, which are generally determined by the 3rd party provider. This method allows for far more flexibility in access, as compared to the traditional approach of simply storing in a singular location, such as the client's personal device. Cloud administrations gives programming and/or equipment to people and organizations from some remote areas which are overseen by an outsider.

In this system of great advantage, there is a considerable change in the workload [1]. Nearby PCs do not need to do all the work with regard to running applications, as it is taken care of by the cloud. On the client's side, the request of the product and equipment has been decreased. The main prerequisite for the client's framework is to bolster the essential design to run the distributed computing framework environment.

A complete rundown of advantages that distributed computing gives is given below:

- For companies with the objective of cutting costs: They can control their consumptions and make use of operational features for expanding their capacity to process. This reduces the amount of internal IT infrastructure required, without hindering the expected processing throughput.
- For companies interested in Scalability and flexibility: Such companies can begin with a minimal arrangement model and scale up into a large organization's infrastructure within no time. If needed, scaling back can also be done, depending on the resources and processing capability required. The benefit of a Distributed computing system permits the company to make use of additional assets at peak times and free these assets when not required, empowering them to fulfill customer requests without squandering any assets.
- For companies seeking Reliability: Services utilizing various excess stockpiling places bolster business progression and recuperation in case of a crisis.
- For companies looking to maintain systems: Cloud admins keep up the framework. Access to such systems is through Application program interfaces. These API's have the benefit of no installation requirements. In this way, we reduce the requirement for support.
- For companies that need Mobile Accessibility: People can get to their information from practically anyplace, which thus builds profitability.

1.1. Data Storage and Security

Organizations providing such facilities have huge servers, and individuals in need such administrations can buy or rent such services from the organizations. Based on the specification of the client, the administrators virtualize assets and then make these assets available in the form of storage pools. In order to maximize redundancy as a data security measure, data often traverses through multiple servers. The security of these documents will depend on the site of the data storage [2].

Security of information on the storage facility takes care of recuperation data, in the case of an accident. Redundancy is the most fundamental strategy to improve information storing security, however the dynamic way of the cloud implies client information may regularly change, so1 the requirement for measures to guarantee information consistency. As client information for various clients is put away on the same stage, Isolation ensures freedom between them, which implies client can just get to their own information, and information changes of different clients won't influence the present client [3].

1.2. Concerns

Below are some issues connected with distributed computing:

- Security and Privacy- These two issues are maybe the most correlated. For instance, we can address this concern by keeping the data closest to the association, yet allowing it to be a used in the cloud. To be exactly as mentioned above, the security components amongst association and the cloud should be better and hence rises the requirement for hybrid cloud.
- Improper Standards: There are no standards as of now depicting the interoperability amongst various cloud systems. The open grid forum is building on evolving Open cloud interface for the same.
- Continuous Evolution: The needs of the user are never constant, just like the essential conditions for capacity, interfaces and so on. This implies the cloud as well, anytime, does not stay static, particularly an open cloud.

2. Data Security Issues

Extensive usage of virtualization in the cloud brings about its own implications in terms of security. It concerns primarily the clients of an open cloud service [4]. Virtualization creates a new layer that must be properly created and managed. This drastically transforms the association amongst the basic equipment and the operating system [5].

Essential security concerns are highlighted in an exploration by K.S. Suresh [27] as takes after:

- Data – The area of the information is vital on grounds that as the information is a part of the cloud, the supplier ought to give security, as a part of its services to the client’s information.
- Retrieving information- Who is allowed to access to this information is another essential feature.
- Data Classification-As various clients store information in the same area, it is essential this information does not get blended.
- Service level assention (SLA)- The SLA serves as an agreement that determines the ensured benefit between the supplier of the service and the end user. It determines what level of services will be provided to the user.
- Measures of safety - In the event that a security occurrence happens, what support will the cloud supplier give in incorporated by this point.

3. Security Algorithms

To give secure correspondence between the cloud service and the client over the system, encryption algorithm has a critical part. Encryption algorithm alters the data into a jumbled frame by with the aid of keys and only client has the means to decode this mixed data. Such algorithms can be grouped into two sorts: Symmetric, in which a public key is used to encode and decode and Asymmetric, where we have a private as well as a public key.

3.1. Symmetric Algorithms

These include what is a common singular secret key to encode and in addition decode information and are equipped for preparing vast measure of information. Symmetric algorithms encode plaintexts as Stream cipher codes, one bit after bit at once or as a block comprising of 64 bit units.

The accompanying are major symmetric calculations utilized for encoding information:

<u>3.1.1. Advanced Encryption Standard (AES)</u>

It depends on the Rijndael cipher. AES [28] is regularly utilized for encoding as well as decoding of information. It runs using the mechanism of substitution-change at the product and equipment levels. The sizes of the blocks utilized can be one twenty-eight, one ninety-two or two fifty-six; and utilizes a 4×4 matrix. The size of the key determines quantity of cycles or adjustments to be made on information to ensure it is encoded. Normally ten, twelve or fourteen cycles are utilized for changing usual content to scrambled content. An arrangement of reverse rounds is connected to decode the content.

3.1.1.1. Operation of AES

AES performs all its calculations on bytes. Henceforth, it considers one twenty-eight bits as sixteen bytes in it calculations. The aforementioned sixteen bytes are distributed in 4 sections and 4 columns to be handled like a network. Quantity of rounds varies, relying on individual key lengths. It utilizes ten rounds for 128-piece key, twelve rounds for 192-piece keys, fourteen rounds for the 256-piece key. These rounds utilize an alternate round key of 128-piece, that the 1st AES key is used to derive.

Encrypting:

We adhere to the description of a general round of encrypting in AES. Four sub forms make up every round. The first-round process is given below.

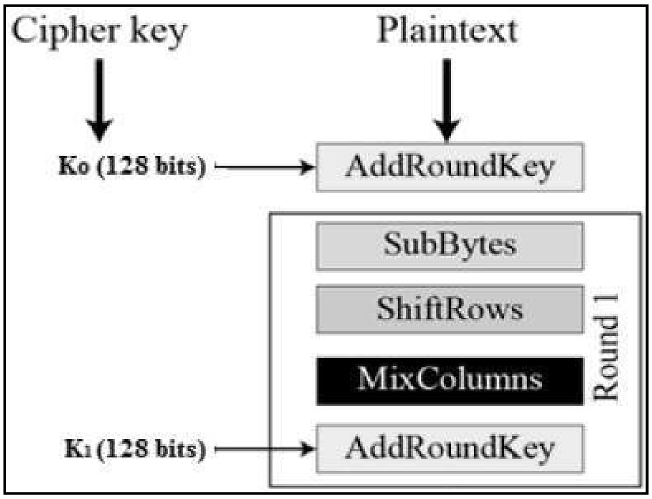


Figure 1: First round of AES

3.1.1.2. Byte Substitution
The sixteen input bytes will be replaced by checking the S box in the plan. Outcome is a matrix of 4x4.

3.1.1.3. Shifting Rows
All 4 rows from the matrix are moved to left side. The entries that tumble are embedded towards the right half of the line. Shifting is done as follows:

- 1st row isn't moved.
- 2nd row is moved 1 position to the left side.
- 3rd row is moved 2 positions left side.
- 4th row is moved 3 positions left side.
- Result is a matrix including the same sixteen bytes.

3.1.1.4. Mixing Columns
Every column of quadruple bytes is presently altered applying a unique mathematical capacity. The capacity inputs 4 bytes of a section and produces 4 new bytes. Output is fresh matrix encompassing 16 fresh bytes. It must to be noted, this progression is not to be carried out in the final round.

3.1.1.5. Include Round Key
The sixteen bytes in the matrix are considered to be one twenty-eight bits, also XOR to one twenty-eight bits round key. In the event that happens to be the last round, the yield is the cipher content. Or else, subsequent one twenty-eight bits will be deciphered as sixteen bytes. We start a new comparable iteration.

3.1.1.6. Decoding Process
Decoding of an AES figure content is similar to the encryption done backwards. Every iteration comprises of 4 procedures in reverse order.

3.1.2. Data Encryption Standard
It functions [13] using blocks of sixty-four bits; applying secret key which is of fifty-six bits. The primary premise applied a secret key of sixty-four bits' length. Encrypting [12] a part of communication takes about sixteen phases. Utilizing the information key, 16 forty-eight bit keys are formed. In each round, 8 S boxes are operated. Utilizing the S boxes, congregations of 6 bits are plotted with meetings of the 4 bits. Contents of the boxes are controlled by NSA.

Each piece of the communication is broken into 2 parts. Right half ranges from 30 to forty-eight bits utilizing a different settled table. Outcome is combined by a sub-key for the round utilizing XOR operator. Using these S boxes, the forty-eight outcoming bits then modified again to thirty-two bits, that are in this way permutated employing yet additional settled table. This entirely rearranged right part is now consolidated with left part employing XOR process. In the subsequent round, this grouping is utilized as fresh left half.

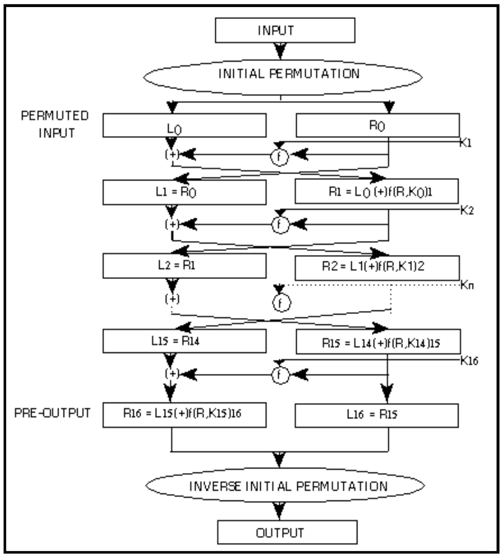


Figure 2: Left and right parts means as L_0, R_0. and the resultant adjusts as L_1, R_1, L_2, R_2 etc. Function f is in charge of the considerable number of connections depicted in the diagram.

The Triple-DES [7] variant was created subsequently it turns out to be obvious, i.e. DES lacking anybody else's involvement was too easy to break. It operates 3 fifty-six bit DES key, providing a combined key length of one sixty-eight bits. Encryption applying Triple DES:

i. encryption utilizing DES by the initial fifty-six-bit key
ii. decryption utilizing DES by the second fifty-six-bit key
iii. encryption utilizing DES by the third fifty-six-bit key

3.1.3. Blowfish Algorithm

It's another well-known algorithm that's utilized in cloud computing. This utilizes key depending S Boxes, more compound key plans. It utilizes a sixty-four-bit size and adjustable key length that can run from thirty-two bits to four forty-eight bits. Sixteen rounds are made and the structure looks like CAST-128. Unscrambling is done using starting converse rounds.

3.1.3.1. Portrayal of Blowfish

Blowfish [11] symmetric cipher algorithm encodes block information of 64-bits at once. This algo is isolated into 2 sections:

- key extension
- information Encryption

3.1.3.2. Key Extension

This would change over a key of max four forty-eight bits to a few sub key clusters accumulating four thousand one sixty-eight bytes. It utilizes substantial no of sub keys. The keys are created for information encrypting or decoding. The P exhibit comprises of eighteen, thirty-two-bit Sub-keys:

$$P_1, P_2, \ldots, P_{18}$$

Four hundred and thirty-two-bit S boxes contains two hundred and fifty-six entries:

$$S_1,0,S_1,1\ldots\ldots\ldots.S_1,255$$
$$S_2,0,S_2,1\ldots\ldots\ldots.S_2,255$$
$$S_3,0,S_3,1\ldots\ldots\ldots.S_3,255$$
$$S_4,0,S_4,1\ldots\ldots\ldots.S_4,255$$

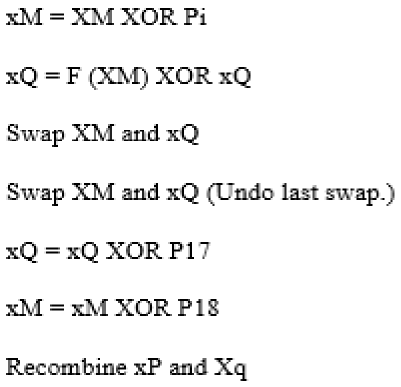
3.1.3.3. Creating Sub-Keys

Sub-Keys are computed utilizing Blowfish calculation:

1.Set the P exhibit 1st and after that the 4 S boxes, all together, using a settled string. It comprises of hexa-decimal digits of PI: P_1 = 0x243f6a8, P_2 = 0x85a308d, P_3 = 0x13198a2, P_4 = 0x0370734, and so forth.
2. XOR P_1 by initial thirty-two-bits of the key, XOR P_2 by the 2nd thirty-two bits of key, thus for every bit of the key. Over and again burn through key bits till whole P exhibit is XOR ed with main bits.
3. Convert all the 0th string using Blowfish calculation, applying sub keys represented as a part of steps 1,2.
4. change P_1, P_2 using yield of 3rd step.
5. Encode yield of 3rd step utilizing Blowfish calculation with altered subkeys.
6. Substitute P_3, P_4 with yield of 5th step.

7. Do this procedure, supplanting every section of P cluster, afterwards each of the four S-confines arrange, with yield of constantly altering Blowfish algo. Altogether, five twenty-one cycles are needed to produce the required sub-keys. Apps can stockpile the sub-keys as opposed to implement this determination procedure various times.

3.1.3.4. Information Encryption:
This is having capacity to repeat sixteen times of a system. Every round comprises of key ward change and information subordinate replacement. every processes are XORs and increases on thirty-two bit words. The main extra processes are 4 recorded cluster information query tables for each round.
Isolate x to 2 thirty-two bit parts: xM, xQ
For i = 1 to 16:



```
xM = XM XOR Pi
xQ = F (XM) XOR xQ
Swap XM and xQ
Swap XM and xQ (Undo last swap.)
xQ = xQ XOR P17
xM = xM XOR P18
Recombine xP and Xq
```

3.2. Asymmetric Algorithms

The accompanying are the major Asymmetric encryption algorithms [19] utilized for scrambling or digitally marking information:

3.2.1. RSA
Rivest, Shamir, and Adleman discharged the Rivest-Shamir-Adleman (RSA) open key calculation in 1978. It is the most widely recognized calculation utilized for encryption [15]. This calculation can be utilized for scrambling and marking information. The encryption and marking procedures are performed through a progression of particular duplications. It could produce open and private keys [16].so the cloud supplier will create an open key known to all, and it is decoded just utilizing the comparing private key.
The RSA [8] calculation could be clarified as beneath.
ciphertxt = (plaintxt)^c mod x
plaintxt = (ciphertxt)^b mod x
secret Key = {b, x}
Open Key = {c, x}
The calculation for validation would be:
ciphertxt = (plaintxt)^b mod x
plaintxt = (ciphertxt)^c mod x
secret key = {b, x}
open key = {c, x}

3.2.2. Digital Signature Algorithm (DSA)
It was designed by the US government for computerized marks. DSA could be utilized just to sign information, and it can't be utilized to encrypt. The process for marking [20] is made by a progression of figurings in light of a chose prime number.

The initial segment of this algorithm is people in public key and secret key era, that is shown below:

- Choose any prime m, it shall be designated as the prime divisor.
- Choose another groundwork number n, with the end goal that n-1 mod m = 0. We know n is prime modulus here.
- Choose a number t, with the end goal that 1 < t < n, t**m mod n = 1 and t = h**((n–1)/m) mod n. m is likewise called t's multiplicative modulo n.
- Choose a whole number, such that 0 < z < m.
- Compute e as t**z mod n.
- Set the general key as {n, m, t, e}.
- Set the private key as {n, m, t, z}.

The secondary part of calculation is mark era and mark confirmation. It is given below:
To produce the message, sender can take after these means:

- Consider an irregular number g, with the end goal that 0 < g< m.
- Compute q as (t**g mod n) mod m. In the event that q = 0, choose an alternate g.
- calculate v, to an extent that g*v mod m = 1. v is known as the particular multiplicative opposite of g modulo m.
- Compute c = v*(h+r*z) mod m. In the event that c = 0, select an alternate g.
- Package the advanced signature as {q, c}.

At the point when DSA is utilized, the way toward making the computerized mark is speedier than approving it.
At the point when RSA is utilized, the way toward approving the computerized mark is quicker than making it.

3.2.3. Diffie-Hellman Key Agreement

Diffie-Hellman calculation [17] is not used for encrypting or decoding. It rather addresses a pair of gatherings that are included in correspondence for the creation of a mutual private key for trading data. This key can then be utilized to encode the next communication utilizing a symmetric key. Hellman key [18] can be understood as:
Consider a pair of gatherings who need to exchange information safely.

- M1 and M2 concede to 2 huge whole numbers x and y with the end goal that 1 < x < y.
- M1 then picks an irregular number e and registers E = x^e mod y. M1 sends I to M2.
- M2 then picks an irregular number f and processes F = x^f mod y. M2 sends J to M1.
- M1 figures N1 = J^e mod y.
- M2 figures N2 = I^f mod y.
- Here N1 = N2 = x^(ef) mod y and along these lines.

N1 and N2 are the secure keys for transmission.

4. Conclusions

Cloud services are revolutionizing the methods and ways in which IT divisions buy, utilize and oversee related assets. Organizations have an array of of approaches to utilize cloud administrations as a part of, inclusive of infrastructure, platform or applications.
Security is a noteworthy prerequisite for any distributed computing environment with regards to storing data. There is a plethora of algorithms which are already in use in the field of cloud computation.
In our paper, we discussed the two types of algorithms, their attributes, mechanisms, advantages and disadvantages. Future extension incorporates enhancing these algorithms and creating hybrid calculations that are productive, as well as wipe out the mishaps of individual calculations. As cloud security tradeoff has not been common until as of late, more research is required on the conceivable dangers and how algorithms like DES, 3DES, AES, RSA, Blowfish, and so on match up against them.

5. Acknowledgment

This research was supported by VIT University, Vellore. We would like to extend our gratitude to our peers from VIT University who provided great insight, which in turn, assisted our review immensely.
We thank Priya G., Professor for guidance with implementation of methodologies and comments that improved the overall quality of our work.

6. References

i. G. RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, “Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing.
ii. Cong Wang, Qian Wang, KuiRen and Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing”, In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.
iii. Cong Wang, Qian Wang, Kui Ren and Wenjing Lou “Ensuring Data Storage Security in Cloud Computing.” IEEE 2009.
iv. Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.
v. Hickey, Kathleen. "Dark Cloud: Study finds security risks in virtualization", Government Security News. Retrieved 12 February 2012.
vi. Pratap Chandra Mandal, ‘Superiority of Blowfish Algorithm’, International Journal of Advanced Research in Computer Science and Software Engineering. September (2012) ISSN: 2277-128X Vol. 2, Issue 7.
vii. Karthik,”Data Encryption and Decryption by UsingTripleDES and Performance Analysis of Crypto System”,ijser
viii. B.Persis Urbana Ivy, Purshotam Mandiwa and Mukesh Kumar, ‘A Modified RSA Cryptosystem Based on ‘n’ Prime Number’, International Journal of Engineering and Computer Science. Nov (2012) ISSN: 2319-7242 Volume 1 Issue 2.
ix. Ayan Mahalanobis, ‘Diffie-Hellman Key Exchange Protocol’, Its Gernalization and Nilpotent Groups. August (2005).
x. Alexa Huth and James Cebula ‘The Basics of Cloud Computing’, United States Computer Emergency Readiness Team. (2011).

xi. G. Devi and M. Pramod Kumar, ‘Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish Algorithm’, International Journal of Computer Trends and Technology. (2012) Vol. 3 Issue 4, ISSN: 2231-2803, pp.592-596

xii. Electronic Frontier Foundation, “DES challenge III broken in record 22 hours," January1999. (http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html)

xiii. Sombir Singh, “enhancing security of des algorithm”ijascrss ,volume 3 issue 6 ,2013

xiv. H. Bonnenberg, A. Curiger, N. Felber, H. Kaeslin, and X. Lai, “VLSI implementation of a new block cipher," in Proceedings of the IEEE International Conference on Computer Design: VLSI in Computer and Processors, pp. 501-513, 1991.

xv. Uma Somani, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

xvi. Randeep Kaur1 ,Supriya Kinger ,"Analysis of Security Algorithms in Cloud Computing",International Journal of Application or Innovation in Engineering & Management ,Volume 3, Issue 3, March 2014.

xvii. Diffie-Hellman Key Agreement Method ,"https://www.ietf.org/rfc/rfc2631.txt".

xviii. Mr. Randhir Kumar, Dr. Ravindranath C. C ,"Analysis of Diffie Hellman Key Exchange Algorithm with Proposed Key Exchange Algorithm",International Journal of Emerging Trends & Technology in Computer Science ,Volume 4, Issue 1, January-February 2015 .

xix. Akashdeep Bhardwaj ."Security Algorithms for Cloud Computing ", International Conference on Computational Modeling and Security (CMS 2016).

xx. Jennifer Seberry, Vinhbuu To and Dongvu Tonien,"A New Generic Digital Signature Algorithm ".

xxi. Akhil Behl “Emerging Security Challenges in Cloud Computing ”, IEEE World Congress on Information and Communication Technologies, 2011 pp.217-222.

xxii. AL.Jeeva, Dr.V.Palanisamy And K.Kanagaram “Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms” International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, Pp.3033-3037.

xxiii. Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing Wiley Publishing, Inc. Indianapolis, Indiana 2010.

xxiv. Leena Khanna, Prof. Anant Jaiswal “Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them”, International Journal of Advanced Research in Computer Science and Software Engineering 3(3), March - 2013,pp. 279-283.

xxv. Priyanka Arora, Arun Singh, Himanshu Tyagi —Analysis of performance by using security algorithm on cloud network in international conference on Emerging trends in engineering and management (ICETM2012), 23-24 june, 2012

xxvi. D. Feng, et al. "Study on cloud computing security." Journal of Software 22.1 (2011): pp.71 -83.

xxvii. K.S. Suresh, “Security Issues and Security Algorithms in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, October 2012, pp. 110-114

xxviii. Ritu pahal,”efficient implementation of AES”,IJARCSSE ,volume3, issue 7,2013

xxix. D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, “Performance Evaluation of Symmetric Encryption Algorithms”,Communications of the IBIMA Volume 8, 2009

xxx. Yogesh Kumar, Rajiv Munjal and Harsh Sharma,”Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures”, IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.