ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Key-Combination Cryptosystem for Scalable File Distribution in Cloud Server Storage

Wathq Asmael Hamed
Master of Science (Information System),
Nizam College (Autonomous),O.U,
Basheer Bagh, Hyderabad.

ABSTRACT:

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.

INTRODUCTION:

1.1 NETWORK SECURITY & CRYPTOGRAPHY:

Network security & cryptography is aconcept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention.

The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password [1]. Network security starts with authenticating the user, commonly with a username and a password. Since this requires just one detail authenticating the user name —i.e. the password, which is something the user 'knows'— this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g. a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g. a fingerprint or retinal scan). Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users [2].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high-level analysis [3]. Communication between two hosts using a network may be encrypted to maintain privacy.

WHAT IS CLOUD COMPUTING?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

HOW CLOUD COMPUTING WORKS?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

LITERATURE SURVEY:

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 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. Also a set of public key, symmetric key and hash algorithms suitable for such environments and studied their workload characteristics It also describes the instructions needed by different algos: Diffie Hellman key exchange, AES, Hash.

All are compared using simple RISC style processor with ALU and shifter and workload characteristics can be determined [5]. AameerNadeem et.al presented, performance of 4 secret key algorithms (DES, 3DES, AES, Blowfish) were compared by encrypting input files of various contents and sized on different hardware program. The algorithms have been implemented in a uniform language, using their standard specifications, to allow a fair comparison of execution speeds. Pentium-II having frequency 266MHz (running Microsoft Windows OS) and Pentium-IV with 2.4 MHz machine (running Windows XP OS) are the basis for time measurement with their goal to measure the encryption times of considered algos. The performance results have been summarized and discussed a tradeoff between performance and security and a conclusion has been presented.

The performance measurement approach was JAVA in which Blowfish was the fastest algorithm among DES, 3-DES, AES and Execution results are presented in ECB mode (for block ciphers) and CFB (for stream ciphers) and concluded on the basis that an algorithm having more complex rounds and a larger number of rounds is generally considered more secure. So, concluded Blowfish as the fastest one among all [6]. Kyung Jun Choi et.al investigated various cryptographic algorithms suitable

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

for used in wireless sensor network utilizing MICA z-type motes & Tiny OS is investigated. Usage of resources including memory, computational time and power for each cryptographic algorithm was characterized experimentally.MD5 and RC4 showed best performance in terms of power dissipation and in terms of cryptographic processing time used. ATMEL AT mega 128L microprocessor is on board in MICA z-based motes. 128KB programmable flash memory used to store executable program code, 4KB SRAM used for temporary storage. To measure encryption key set up time a 128 bit size key that provides 2^128 possible keys was used. RC4 was considered as the best as it is XOR based stream cipher cheaper, less complex, and fastest and uses 8-bit block size which can be efficiently handled by ATMEL [7]. 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 [8]. NeetuSettia et. 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.

Only alphanumeric and special characters are used for analysis of cryptographic techniques. These specifications are selected in option menu of the CrypTool and visual results are set in window option of the CrypTool. For the input plaintext, around 25-sample text are taken and encrypted with various algorithms. The output of above plaintext is cipher text, analyzed with analysis option in CrypTool. Some of the cryptographic algorithms are implemented in C, and their output is taken as cipher text, which is then copied in some text file and that text file is used for the analysis with CrypTool [9].

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. It also includes several computational issues, optimization of cipher as well as the analysis of AES security aspects against different kinds of attacks including the countermeasures against these attacks and also highlighted some of the important security issues of AES algorithm. The future work can done for the distribution of secret key that is considered as a critical issue of AES like other symmetric encryption algorithm [10]. Like 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.

In the training phase, Principal Component Analysis (PCA) on several important packet fields was done to reduce the data dimension, and then constructed the most appropriate profile based on the PCA results. In the detection phase, an anomaly score defend against unknown attacks is demanding increased research in this area [11]. Yudhvir Singh et.al considered various attacks such as simulation based attacks on cipher text only, known plain text and manual analysis in the network The simulation based information theory tests such as Entropy, Floating Frequency, Histogram, N-Gram, Autocorrelation and Periodicity on cipher text were done. The simulation based randomness tests such as Frequency Test, Poker Test, Runs Test and Serial Test on cipher text were done. Finally, they proposed KK' cryptographic algorithms in search for the best compromise in security. With these automatic test techniques it was found that the traditional cryptographic techniques are weaker and bit manipulation based are stronger and other cryptographic techniques are moderate to analyze. The Caesar and ROT-13 cipher was found to be weakest with the simulation based tests analysis and Byte Addition, Binary EX-OR and KK' cipher are the strongest among these ciphers. [12].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

IMPLEMENTATION:
SYSTEM MODEL:

» Data Owner (Alice): In this module we executed by the data owner to setup an account on an untrusted server. On input a security level parameter 1λ and the number of ciphertext classes n (i.e., class index should be an integer bounded by 1 and n), it outputs the public system parameter param, which is omitted from the input of the other algorithms for brevity.

» Network Storage: With our solution, Alice can simply send Bob a single aggregate key via a secure e-mail. Bob can download the encrypted photos from Alice's Dropbox space and then use this aggregate key to decrypt these encrypted photos. In this Network Storage is untrusted third party server.

KEY GENERATION:

» Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic algorithms which requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked.

» The public key is used to encrypt plaintext whereas the private key is used to decrypt ciphertext .Data owner to randomly generate a public/master-secret key pair.

ENCRYPTION:

» Encryption keys also come with two flavours symmetric key or asymmetric (public) key. Using symmetric encryption, when Alice wants the data to be originated from a third party, she has to give the encrypted her secret key; obviously, this is not always desirable.

» By contrast, the encryption key and decryption key are different in public key encryption. The use of public-key encryption gives more flexibility for our applications.

AGGREGATE KEY TRANSFER:

» A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows.

The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen.

» Messages can be encrypted via Encrypt by anyone who also decides what ciphertext class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of ciphertext classes via Extract.

» The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally; any user with an aggregate key can decrypt any ciphertext provided that the ciphertext's class is contained in the aggregate key via Decrypt

CONCLUSION:

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. We have studied various cryptographic techniques to increase the security of network.

REFERENCES:

[1] Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323.

[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with JayshreeUllal, senior VP of Cisco.

[3] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[4] Sanchez-Avila, C. Sanchez-Reillol, R, —The Rijndael block cipher (AES proposal): A comparison with DES, 35th International Conference on Security Technology 2001, IEEE.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[5] Murat Fiskiran, Ruby B. Lee, —Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments, IEEE International Workshop on Workload Characterization, 2002. WWC-5. 2002.

[6]AameerNadeem, Dr. M.YounusJaved, —A performance comparison of data Encryption Algorithm, Global Telecommunication Workshops, 2004 GlobeCom Workshops 2004, IEEE.

[7] Elkamchouchi, H.M; Emarah, A.-A.M; Hagras, E.A.A, —A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes, the 23rd National Radio Science Conference (NRSC 2006).

[8] Like Zhang, Gregory B. White, —Anomaly Detection for Application LevelNetwork Attacks Using Payload Keywords, Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007).

[9]SuhailaOrner Sharif, S.P. Mansoor, —Performance analysis of Stream and Block cipher algorithms, 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[10]PunitaMellu&Sitender Mali, —AES: Asymmetric key cryptographic System, International Journal of Information Technology and Knowledge Management, 2011, Vol, No. 4 pp. 113-117.

[11]YudhvirSingh, YogeshChaba, —Information Theory test based Performance Evaluation of Cryptographic Techniques, International Journal of Information Technology and Knowledge Management, Vol 1,No.2,2008 , pp. 475-483.

[12] YanWang, Ming Hu, —Timing Evaluation of known cryptographic Algorithm, International Conference on Computational Intelligence and security, 2009.

AUTHORS BIOGRAPHY:

WATHQ ASMAEL HAMED, pursuing his Master of Science in Information System, from Nizam College (Autonomous),O.U,Basheer Bagh, Hyderabad,India.