© 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

ENCHANCEMENT OF SECURITY OF FIREWALL BASED CLOUD SERVER USING CUSTOMIZED DATA ENCRYPTION STANDARD

[1]Poonam Verma, Research Scholar, Department of CSA, CDLU Sirsa
[2]Monika Bansal, Assistant Professor , Department of CSA, CDLU Sirsa

Abstract: Cloud computing has grabbed the spotlight in the year 2013 at a conference in San Francisco, with vendors providing plenty of products and services that equip IT with controls to bring order to cloud chaos. Cloud computing trend is increasing rapidly so to make cloud computing more popular the very first step for the organization is to identify exact area where the cloud related threats lie. At an unusual pace, cloud computing has transformed business and government. And this created new security challenges. The development of the cloud service model provide business –supporting technology in a more efficient way than ever before the shift from server to service based technology brought a drastic change in computing technology. However these developments have created new security vulnerabilities, including security issues w hose full impressions are still rising. This paper presents an overview and study of cloud computing, with several security threats, security issues, currently used cloud technologies and security solutions.

Keywords: Cloud Computing, Deployment Models, Threats, Technologies, Security Issues, Service Models.

1. Introduction

Cloud computing is set of resources that are being allocated on demand. Cloud computing proposes new ways to provide services. These new innovative, technical and pricing opportunities bring changes in the way business operated. Cloud computing is the matchless computing technology.

Cloud computing is a new label to an old idea. Cloud computing is a collection of resources and serviced provided by cloud service provider through internet. Cloud services are distributed from data canters sited all over the world. Cloud computing makes possible for its users to use the virtual resources via internet as per requirements. Cloud computing grabbed the spotlight in few years. General example of cloud services are Google Engine, Oracle Cloud, Office 365. As the cloud computing is growing rapidly this also leads to severe security concerns. Lack of security is the only barrier in wide adoption of cloud computing. The rapid growth of cloud computing has brought many security challenges for users and providers**Cloud Computing Model**

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. However, cloud computing technology challenges many traditional approaches to datacenter and enterprise application design and management. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security. It is the very nature of cloud computing-based services, private or public, that promote external management of provided services. This delivers great incentive to cloud computing service providers to prioritize building and maintaining strong management of secure services. Security issues have been categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. Solutions to various cloud security issues vary, from cryptography, particularly public key infrastructure (PKI), to use of multiple cloud providers, standardization of APIs, and improving virtual machine support.

2. Literature Review

Advances in the field of network based computing and applications on demand have led to an explosive growth of application models such as cloud computing, software as a service, community network, web store, and so on. As a major application model in the era of the internet, cloud computing has become a significant research topic of the scientific and industrial communities since 2007 (Qi and Gani, 2012). Furthermore, Cloud computing has generated a lot of interest and competition in the industry and it is recognized as one of the top 10 technologies of 2010 (Tripathi and Mishra, 2011; Sharma, 2012). It is the next generation in computation. Maybe Clouds

© 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

can save the world; possibly people can have everything they need on the cloud. It is the next natural step in the evolution of on-demand information technology services and products (Mirzaei, 2008). Basically, a cloud is a visible mass of particles of water or ice suspended in the atmosphere. It is any similar mass in the air particularly of smoke or dust. The Internet is a worldwide network connecting millions of computers that use the Transmission Control Protocol/Internet Protocol (TCP/IP) network protocols to facilitate data transmission and exchange. Therefore the term "cloud" can be used as a metaphor for the Internet. Cloud computing is an internet based service delivery model which provides internet based services, computing and storage for users in all markets including financial, health care & government (Sharma, 2012). It is a style of computing in which IT-related capabilities are provided "as a service", allowing users to access technology-enabled services from the Internet (i.e., the Cloud) without knowledge of, expertise with, or control over the technology infrastructure that supports them (Mirzaei, 2008). Also, according to National Institute of Standards and Technology (NIST) definition (Mell and Grance, 2011), Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Thus this research is an introduction to the terminologies, characteristics, and services associated with cloud computing. The core service models being deployed (such as software, platform, and infrastructure as a service) and generic deployment models employed by service providers and consumers to use and maintain the cloud services (such as the private, public, community, and hybrid clouds) are discussed. Also considered are the benefits, trend and challenges associated with cloud computing. Cloud computing has been cited as the fifth utility'(along with water, electricity, gas, and telephone) whereby computing services are readily available on demand, like other utility services available in today's society [Buyya, Yeo, Venugopal, Broberg, and Brandic, 2009]. This vision is not essentially new. Dating back to 1961, John McCarthy, retired Stanford professor and Turing Award winner, in his speech at MIT's Centennial, predicted that in the future computing would become a public utility'[Wheeler and Waggener, 2009]. In 1969, Leonard Kleinrock, one of the chief scientists of the original Advanced Research Projects Agency Network (ARPANET) project which seeded the Internet, said: 'As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of "computer utilities" which, like present electric and telephone utilities, will serve individual homes and offices across the country'[Kleinrock, 2005,p.4]. It could be argued that cloud computing has begun to fulfil this vision of computing on demand.The first step of studying research into cloud computing is to clarify the concept. Attempts to define cloud computing have come from different perspectives with in practice and academia (as listed in Table 1).Among the various definitions, the one by the NIST (National Institute of Standards and Technology) has gained recent recognition and popularity. For the purpose of this study, the NIST definition of cloud computing is adopted to facilitate the following discussions.The NIST further suggests that a cloud computing model should be composed of five essential characteristics, three service levels,four deployment models [Mell And Grance, 2009].

3.CRYPTOGRAPHY

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances (e.g., improvements in integer factorization algorithms) and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms. Any communication in the language that you and I speak-that is the human language, takes the form of plain text or clear text. That is, a message in plain text can be understood by anybody knowing the language as long as the message is not codified in any manner. So, now we have to use coding scheme to ensure that information is hidden from anyone for whom it is not intended, even those who can see the coded data [1, 2Encryption and Decryption of text Until modern times cryptography referred almost exclusively to *encryption*, which is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called ciphertext).

© 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

Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A *cipher* (or *cypher*) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret parameter (ideally known only to the communicants) for a specific message exchange context. A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societie.

4 .Existing security Mechanism

Much of the theoretical work in cryptography concerns cryptographic *primitives*—algorithms with basic cryptographic properties—and their relationship to other cryptographic problems. More complicated cryptographic tools are then built from these basic primitives. These primitives provide fundamental properties, which are used to develop more complex tools called *cryptosystems* or *cryptographic protocols*, which guarantee one or more high-level security properties. Note however, that the distinction between cryptographic *primitives* and cryptosystems, is quite arbitrary; for example, the RSA algorithm is sometimes considered a cryptosystem, and sometimes a primitive. Typical examples of cryptographic primitives include pseudorandom functions, one-way functions, etc. One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or *cryptosystem*. Cryptosystems are designed to provide particular functionality (e.g. public key encryption) while guaranteeing certain security properties. Cryptosystems use the properties of the underlying cryptographic primitives to support the system's security properties. Of course, as the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem can be derived from a combination of several more primitive cryptosystems. When used with asymmetric ciphers for key transfer, pseudorandom key generators are nearly always used to generate the symmetric cipher session keys. However, lack of randomness in those generators or in their initialization vectors is disastrous and has led to cryptanalytic breaks in the past. Therefore, it is essential that an implementation uses a source of high entropy for its initialization.

5. THREATS TO THE EXISTING SYSTEM

In cryptography, a **brute-force attack**, or **exhaustive key search**, is a cryptanalytic attack that can, in theory, be used against any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It consists of systematically checking all possible keys or passwords until the correct one is found. In the worst case, this would involve traversing the entire search space.

When password guessing, this method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used because of the time a brute-force search takes. When key guessing, the key length used in the cipher determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. A cipher with a key length of N bits can be broken in a worst-case time proportional to 2^N and an average time of half that. Brute-force attacks can be made less effective by obfuscating the data to be encoded, something that makes it more difficult for an attacker to recognize when he/she has cracked the code. One of the measures of the strength of an encryption system is how long it would theoretically take an attacker to mount a successful brute-force attack against it. Brute-force attacks are an application of brute-force search, the general problem-solving technique of enumerating all candidates and checking each one. The term "brute-force" is not the only term to name such a type of attack. It can also be called "bruteforce", "brute force" and just "brute" (that is common in names of programs that perform brute-force attacks). Limitation of brute-force attack The resources required for a brute-force attack grow exponentially with increasing key size, not linearly. Although US export regulations historically restricted key lengths to 56-bit symmetric keys (e.g. Data Encryption

© 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

Standard), these restrictions are no longer in place, so modern symmetric algorithms typically use computationally stronger 128- to 256-bit keys.

There is a physical argument that a 128-bit symmetric key is computationally secure against brute-force attack. The so-called Landauer limit implied by the laws of physics sets a lower limit on the energy required to perform a computation of $kT \cdot \ln 2$ per bit erased in a computation, where T is the temperature of the computing device in Kelvin's, k is the Boltzmann constant, and the natural logarithm of 2 is about 0.693. No irreversible computing device can use less energy than this, even in principle. Thus, in order to simply flip through the possible values for a 128-bit symmetric key (ignoring doing the actual computing to check it) would theoretically require $2^{128} - 1$ bit flips on a conventional processor. If it is assumed that the calculation occurs near room temperature (~300 K) the Von Neumann-Landauer Limit can be applied to estimate the energy required as $\sim 10^{18}$ joules, which is equivalent to consuming 30 gigawatts of power for one year. This is equal to 30×10^9 W×365×24×3600 s = 9.46×10^{17} J or 262.7 TWh (more than 1/100th of the world energy production). The full actual computation – checking each key to see if you have found a solution – would consume many times this amount. Furthermore, this is simply the energy requirement for cycling through the key space; the actual time it takes to flip each bit is not considered, which is certainly greater than 0.

However, this argument assumes that the register values are changed using conventional set and clear operations which inevitably generate entropy. It has been shown that computational hardware can be designed not to encounter this theoretical obstruction (see reversible computing), though no such computers are known to have been constructed.

6 PROPOSED WORK

The **Data Encryption Standard** (**DES**, was once a predominant symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world. Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the National Security Agency (NSA), the NBS eventually selected a slightly modified version (strengthened against differential cryptanalysis, but weakened against brute force attacks), which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977. The publication of an NSA-approved encryption standard simultaneously resulted in its quick international adoption and widespread academic scrutiny. Controversies arose out of classified design elements, a relatively short key length of the symmetric-key block cipher design, and the involvement of the NSA, nourishing suspicions about a backdoor. The intense academic scrutiny the algorithm received over time led to the modern understanding of block ciphers and their cryptanalysis.

DES is now considered to be insecure for many applications. This is mainly due to the 56-bit key size being too small; in January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes (see chronology). There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES). Furthermore, DES has been withdrawn as a standard by the National Institute of Standards and Technology (formerly the National Bureau of Standards).Some documentation makes a distinction between DES as a standard and DES as an algorithm, referring to the algorithm as the **DEA** (**Data Encryption Algorithm**).Symmetric-key algorithm **Symmetric-key algorithms** are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both encryption of plaintext and decryption of ciphertext. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. Other terms for symmetric-key encryption are **secret-key**, **single-key**, **shared-key**, **one-key**, and **private-key** encryption. Use of the last and first terms can create ambiguity with similar terminology used in public-key cryptography. Symmetric-key cryptography is to be contrasted with asymmetric-key cryptography. Cloud computing is still evolving but its benefits are enormous. Cloud computing provides excellent support for amazing infrastructures, applications and services such as shared resource pool, broad network base, reduced IT cost or rapid elasticity of the cloud to handle varying customers demands as well as

© 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

cloud computing various service and deployment models which is part of the main reason for adopting this computing system. Thus this makes cloud computing an open shared system volatile to security breaches and other challenges.

So there is need to focus on solutions of the various challenges to maintain the dependence level of organization for deploying the cloud computing without any hesitation and also the need of technical support for elastic scalability to serve the ever pressing demand of the customer.

Hacking has both its benefits and risks. Hackers are very diverse. They may bankrupt a company or may protect the data, increasing the revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end. While ethical hacker help to understand the companies' their security needs, the malicious hackers intrudes illegally and harm the network for their personal benefits. An Ethical and creative hacking is significant in network security, in order to ensure that the company's information is well protected and secure. At the same time it allows the company to identify, and in turn, to take remedial measures to rectify the loopholes that exists in the security system, which may allow a malicious hacker to breach their security system. They help organizations to understand the present hidden problems in their servers and corporate network. The study also reveals that the valid users are the ethical hackers, till their intensions are clear otherwise they are a great threat, as they have the access to every piece of information of the organization, as compare to total and semi outsiders.This also concludes that hacking is an important aspect of computer world. It deals with both sides of being good and bad. Ethical hacking plays a vital role in maintaining and saving a lot of secret information, whereas malicious hacking can destroy everything. What all depends is the intension of the hacker. It is almost impossible to fill a gap between ethical and malicious hacking as human mind cannot be conquered, but security measures can be tighten.

7 REFERENCES

1. Logik Bomb: Hacker's Encyclopedia (1997)
2. sHafner, Katie; Markoff, John (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster. ISBN 0-671-68322-5.
3. Sterling, Bruce (1992). *The Hacker Crackdown*. Bantam. ISBN 0-553-08058-X.
4. Slatalla, Michelle; Joshua Quittner (1995). *Masters of Deception: The Gang That Ruled Cyberspace*. HarperCollins. ISBN 0-06-017030-1.
5. Dreyfus, Suelette (1997). *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Mandarin. ISBN 1-86330-595-5.
6. Verton, Dan (2002). *The Hacker Diaries : Confessions of Teenage Hackers*. McGraw-Hill Osborne Media. ISBN 0-07-222364-2.
7. Thomas, Douglas (2002). *Hacker Culture*. University of Minnesota Press. ISBN 0-8166-3345-2.
8. Taylor, Paul A. (1999). *Hackers: Crime in the Digital Sublime*. Routledge. ISBN 978-0-415-18072-6.
9. Levy, Steven (2002). *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. Penguin. ISBN 0-14-024432-8.
10. Ventre, Daniel (2009). *Information Warfare*. Wiley - ISTE. ISBN 978-1-84821-094-3.
11. Bhushan Lal Sahu,Rajesh Tiwari, *Journal of Advanced Research in Computer Science and Software Engineering* 2(9) (2012) 33-37.
12. ELC Technologies (2010). *Cloud Computing: What You Should Know*". Available at http://publicweb2.unimap.edu.my/~ict/v4/images/doc/ELC_Cloud_Computing_Guide.pdf
13. Han Qi, Abdullah Gani (2012). *Research on Mobile Cloud Computing: Review, Trend and Perspectives*. Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP), pp. 195-202.
14. Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, *International Journal of Soft Computing and Engineering* 2(1) (2012) 421-424.
15. Nariman Mirzaei (2008). *Cloud Computing*. Available at: http://grids.ucs.indiana.edu/ptliupages/publications/ReportNarimanMirzaeiJan09.pdf
16. Peter Mell, Tim Grance (2011). *The NIST Definition of Cloud Computing*, the National Institute of Standards and Technology Report. 2011.
17. Sultan Ullah, Zheng Xuefeng (2013). *Cloud Computing Research Challenges*. IEEE 5th

International Conference on Biomedical Engineering and Informatics, pp 1397-1401.

18. Tripathi A., Mishra A. (2011). *Cloud Computing Security Considerations*. Signal Processing, Communications and Computing (ICSPCC), IEEE International Conference.
19. Mohammad Reza Modarres Zadeh, *International Letters of Social and Humanistic Sciences* 3 (2013) 21-29.
20. sLeah Garner-O'Neale, Jelisa Maughan, Babalola Ogunkola, *International Letters of Social and Humanistic Sciences* 2 (2014) 41-55.