Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 19 Issue 1 Version 1.0 Year 2019
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Review of Various Encryption Algorithms

By Neyole Misiko Jacob
Jomo Kenyatta University of Agriculture and Technology

Abstract- Advancement in technology dictates that information security, user data integrity and security be paramount to protect user information and data from vulnerabilities from malicious intruders- third parties. Need is therefore a factor for information systems to secure user data and information. The concept data encryption ensures that user data is unreadable to third parties keeping their information more safe and secure while using the internet. A lot information on security has been provided by both the physical security and operating system security but neither of these methods have successfully and sufficiently provided a secure mechanism and support on storing and processing of user data and information. This paper reviews the various encryption algorithms that are employed to protect user information and data against various vulnerabilities.

Index terms: *encryption, algorithms, software's, behaviors.*

GJCST-E Classification: *I.1.m*

Review of Various Encryption Algorithms

Neyole Misiko Jacob

Abstract- Advancement in technology dictates that information security, user data integrity and security be paramount to protect user information and data from vulnerabilities from malicious intruders- third parties. Need is therefore a factor for information systems to secure user data and information. The concept data encryption ensures that user data is unreadable to third parties keeping their information more safe and secure while using the internet. A lot information on security has been provided by both the physical security and operating system security but neither of these methods have successfully and sufficiently provided a secure mechanism and support on storing and processing of user data and information. This paper reviews the various encryption algorithms that are employed to protect user information and data against various vulnerabilities.

Index terms : encryption, algorithms, software's, behaviors.

I. Introduction

Advancement in technology dictates that information security, user data integrity and security have become paramount to protect user information and data from vulnerabilities due to technological advances especially the internet or access by third parties. With this there is dire need for information systems to secure user data and information like the use of anonymisation and encryption (Neubauer T, Heurix J, 2011).The concept encryption functions through scrambling of data to make it unreadable by the third party, this is enhanced in a number of ways such as the use of the key size and strength to create strong security of data (Bradford, 2016).

Much as information security has been provided by both the physical security and operating system security, neither of these methods have successfully and sufficiently provided a secure mechanism and support on storing and processing data (Priti V. Bhagat, Kaustubh S. Satpute, Vikas R. Palekar, 2013). This paper reviews the various encryption algorithms that are employed to protect user information and data against various vulnerabilities.

II. Encryption Algorithms

Encryption and cryptography algorithm can be defined as an approach that make data, information or network more secure (Rajdeep Bhanot and Rahul Hans, 2015). As a science, cryptography encamps the use of encryption algorithms to secure data within computer systems. The high reliance of the internet for communication purpose requires that data and information be encrypted to limit intruders from accessing to read messages. The process of information encryption also called cipher text enables users of systems to transfer information and data much securely. There are many encryption algorithms that are used widely. Those available and used in data and information security can broadly be categorized into Symmetric also called private and Asymmetric also called public keys encryption (Prerna Mahajan and Abhishek Sachdeva, 2013).

III. Software Behaviors

By definition encryption is the technology of converting plain text information into cipher text, the cipher text can then be securely communicated over any unsecure network. This process of encryption is usually achieved using encryption algorithm (Rajdeep Bhanot and Rahul Hans, 2015). Users benefit from encryption as it makes their data and information be more confidential, have integrity, be non-repudiation, be authentic and have access Control. There are various encryption algorithms in use currently, whose key size and strength generally being the differences between them (Bradford, 2016).

Bradford further categorizes them as:- Data Encryption Standard (DES), the Triple DES a symmetric algorithm, the RSA a public key encryption algorithm, the Blowfish algorithm, the Twofish algorithm and the Advanced Encryption Standard (AES). Hossain et.al 2016 classified the algorithms as symmetric-key algorithms in which the same key used for both encryption and decryption of data, asymmetric-key algorithms in which a public key is used by a sender to encrypts data and a private key used by receiver for decryption and hashing. (Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, 2016).

The Triple DES a symmetric algorithm makes use of three individual keys with 56 bits, was designed to replace the Data Encryption Standard (DES) algorithm which was much vulnerable to hackers, the RSA a public key encryption algorithm utilized by modern computers to encrypt and decrypt messages. The Blowfish algorithm which is a symmetry cipher used to split and encrypt messages individually whose advantages are its speed and the overall operation effectiveness.

The Twofish algorithm, keys used in this algorithm vary up to 256 bits in length and use

Author: Jomo Kenyatta University of Agriculture and Technology.
e-mail: Jneyole434@gmail.com

symmetric technique for only one key. It is regarded as one of the fastest algorithm and is ideal for use in both hardware and software systems. The Advanced Encryption Standard (AES) which is the algorithm trusted as the standard by many numerous organizations. It is extremely efficient and largely impervious to attacks except for brute force.

A study conducted by Rejani R and Deepu.V. Krishnan on the test of algorithms concluded that between AES, DES, 3DES, RC2, Blowfish, and RC6, Blowfish was the best encryption algorithm between different symmetric and asymmetric encryption algorithms (Rejani. R, 2015). The study further advanced that DES algorithm was no longer secure especially with the advancement in the computer processing power whereas the AES encryption algorithm is faster and flexible hence widely applied in many security applications.

A research on encryption Algorithms AES, DES and RSA for Security by Prerna and Sachdeva (2013) indicated that DES algorithm is used to provide a standardized method to protecting sensitive commercial and unclassified data. The Advanced Encryption Standard (AES) algorithm is appropriate for both hardware and software implementation and is of greater speed, while the Rivest-Shamir-Adleman (RSA) which is widely used Public-Key algorithm is used to encrypt data to provide security so that only the concerned user can access it.

In comparison therefore AES has a block size of 128 bits, DES 64 bits while RSA has a minimum of 512 bits. In terms of encryption and decryption, the AES algorithm is faster while DES is moderate and RSA algorithm is much slower. AES is excellently secured while DES is not enough secured and RSA is the least secure algorithm. All the algorithms are inherently vulnerable to brute forced attacks- a trial and error means employed by various application programs to decode or decrypt encrypted data for instance passwords or Data usually on the internet (Rouse, 2006).

A long this DES is prone to linear and differential cryptanalysis attacks which involves cracking codes to decode privacies through violation of authentication schemes by breaking cryptographic protocols (Heward, 2014), while RSA is vulnerable to oracle attacks that exploit the availability of weaknesses in system. On the other hand the asymmetric algorithm includes: - RSA, DSA, Diffie-Hellman, El-Gamal and Pailier. The hashing which includes the MD5, MD6, the SHA and SHA256 (Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, 2016).

The RSA Rivest-Shamir-Adleman an asymmetric encryption and decryption algorithm uses a public and private key. The public key which is described to everyone is used for encrypting messages. The messages encrypted with the public key are usually decrypted through the private key. RSA performs generation, encryption and decryption of algorithm keys (Priyanka Arora, Arun Singh and Himanshu Tyagi, 2014). The DIFFIE-HELLMAN key has a specific approach of exchanging cryptographic keys that enable two parties having no understanding of each other to equally make a shared-secret key over an insecure communications path. The keys are then encrypt the posterior communications using a symmetric key cipher.

The PAILLIER algorithm has homomorphic properties that facilitate it to perform normal addition operations on several encrypted values to achieving the encrypted sum, they are then decrypted later with no knowledge of the sum value (Priyanka Arora, Arun Singh and Himanshu Tyagi, 2014). The motivation behind the hash functions is the management of data security, integrity and consistency (Neyole, 2015). The Message Digest5 for instance takes random data information of text and binary as input and generate a fixed size hash value as the output.

The input data can be of any length and size, but the output hashed value is always fixed (Neyole, 2015). For MD5 the input message is allocated to groups of 512-bits then the message is then packed by making its length divisible by 512 (Priyanka Arora, Arun Singh and Himanshu Tyagi, 2014). The MD5 is mostly used in the database design to encrypt passwords. It's faster to use but suffers with the challenges of easy decryption using web based applications such as HashKiller. The SHA- Secure Hashing Algorithm on the other hand is a hashing algorithm that is structured differently and are named SHA-0, SHA-1, SHA-2, and SHA-3. SHA-0 whose original version was the 160-bit hash function (Neyole, 2015) this algorithms are more secure and stable especially in the design of database systems.

IV. Conclusions

Does increased security provide 100% assurance to technology consumers? With the Internet as a major essential communication between billions of people and also a tool for commerce, social interaction, and the exchange of an increasing amount of personal information, security has become a matter of grave concern. There are a number approaches to data and information security where many applications to securing commerce and payments are employed to manage private communications and user data and information. But in all this, encryption which makes use of encryption algorithms makes communication more secure to user data and information.

With the many encryption algorithms schemes in existence each out to improve on security of system, data, information and communication channels managers have enhanced them on data and information to facilitate users with more system integrity and confidentiality while working with them. The main concerns of these schemes is to optimize technology use. The Hash functions for instance, are well established to ensure data integrity where any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. This then ensures user with a high degree of confidence (Kessler, 2017).

As the number of attacks and their sophistications increase, attacks on encryptions such as brute-force requires that systems be equipped with the various algorithms to support each other to the management of the systems. On performance analysis, the best algorithms both symmetric and asymmetric should possess the following aspects:- the set of keys and the enciphering algorithm should be free from complexity, the implementation of the process should be as simple as possible, errors in ciphering should not propagate and cause corruption of further information in the message and the size of the enciphered text should be no larger than the text of the original message among other measures (Pfleeger, Charles P. and Shari Lawrence, 2006).

References Références Referencias

1. Bradford, C. (2016, July 31st). *Storagecraft Recovery Zone*. Retrieved from 5 Common Encryption Algorithms and the Unbreakables of the Future: http://www.storagecraft.com/blog/5-common-encryption-algorithms/
2. Heward, G. (2014, January 26th). *Cryptanalysis and Attacks*. Retrieved from Experts-Exchange: https://www.experts-exchange.com/articles/12460/Cryptanalysis-and-Attacks.html
3. Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz. (2016). Performance Analysis of Different Cryptography Algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering*, pp. 659-666.
4. Kessler, G. C. (2017). *An Overview of Cryptography.* Australia: McGraw-Hill.
5. Neubauer T, Heurix J. (2011). A Methodology for the Pseudonymization of Medical data. *International Journal of Medical Information*, pp. 190-204.
6. Neyole, J. M. (2015). Vulnerability of data security using MD5 function in php database design. *International Journal of Science and Engineering*, pp. 11-16.
7. Prerna Mahajan and Abhishek Sachdeva. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology Network, Web & Security*, pp 1-9.
8. Priti V. Bhagat, Kaustubh S. Satpute, Vikas R. Palekar. (January 2013). Reverse Encryption Algorithm: A Technique for Encryption & Decryption. *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, pp.90-96.
9. Priyanka Arora, Arun Singh and Himanshu Tyagi. (2014). Evaluation and Comparison of Security Issues on Cloud Computing Environment. *World of Computer Science and Information Technology Journal*, pp. 179-183.
10. Pfleeger, Charles P. and Shari Lawrence. (2006). Making Good Encryption Algorithms. In C. P. Pfleeger, Security in Computing 4th Edition (pp. pp. 176- 181). Upper Saddle River, NJ 07458 USA: Pearson Education, Inc.
11. Rajdeep Bhanot and Rahul Hans. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal of Security and Its Applications*, pp. 289-306.
12. Rejani. R, a. D. (2015). Study of Symmetric key Cryptography Algorithms. *International Journal of Computer Techniques*, pp. 45-51.
13. Rouse, M. (2006, July). *Brute force cracking*. Retrieved from TechTarget network of technology: http://searchsecurity.techtarget.com/definition/brute-force-cracking.