IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

DATA - ENCRYPTION AND DECRYPTION

Priyanshu Preet
Student ECE
Roorkee College of Engineering
Uttarakhand, India

Prince Thakur
Student ECE
Roorkee College of Engineering
Uttarakhand, India

Saurav Hari Pillai
Student ECE
Roorkee College of Engineering
Uttarakhand, India

Saurabh Kumar Singh
Student ECE
Roorkee College of Engineering
Uttarakhand, India

Under the guidance of
Mr. DILEEP KUMAR JAISWAL
(Assitant Professor)
Roorkee College of Engineering ,Roorkee, India

ABSTRACT
Nowadays, most companies that have a transaction process want to ensure that there are no possible failures. For instance, if sudden damage happens at the primary database, the second one will take over the responsibility of previous work automatically. This process can happen if the company systems have data replication. Data replication is a process that copies and maintains data from a database in one computer or servers to a database in another so that all users share and store the same level of the information. This also increases data availability and enhances data access relevant to their task without interfering with the work of others. The problem is how to make sure that connection/value in data replication is secure. In view of this issue, this paper proposed a secure data replication using encryption algorithm. Encryption is the process of converting readable characters into another version of transformation to prevent unauthorized access. So that valuable data information will be more secure and this method shows that data from a database will be encrypted first then replicated to another server. The unauthorized user also cannot sniff into the database server easily. Thus, this paper approaches encryption of data replication using Advanced Encryption Standard (AES) encryption is a symmetric encryption algorithm which can encrypt and decrypt data or text. AES was created to be efficient and support block- length of 128 bits and key lengths of 128, 192, and 256 bits. This is useful to ensure that sensitive data is secured.

KEYWORDS - *Java, cryptography*

I.INTRODUCTION

The great development of the Internet and World Wide Web makes the number of people surfing the internet by accessing system development increase. 1.7 billion people have used the internet since 2012. Despite the rapid growth of the internet, a large amount of data was shared and used by database systems. If this continues to happen the database performance will become slower than usual. World Wide Web is an information platform where documents and other web resources which are identified by Uniform Resource Locators (URLs) are then linked by hypertext links and can be accessed through the internet. Internet and World Wide Web are two different things which are usually used without much dissimilarity but linked to each other. The Internet is a worldwide system which enables multiple computers to connect with each other while the web is an application that makes use of the system. Without the Internet people cannot access the Web. The Web is a path between the Internet and computers that allows people to communicate and share information, whereas the Internet is the connection between computers for data transmission. Information

Replication is the activity or procedure of putting away information in excess of one site or hub. This is essential for enhancing the accessibility of information. There can be full replication, in which a duplicate of the entire database is put away at each site. There can likewise be halfway replication, in which case, some sections of the database are duplicated and others are not recreated. There are advantages to data replication which are improved availability and increasing parallelism. For example, if one of the sites containing experience failure, we have another database server to use. Thus, queries can be continued to be processed in spite of the failure of one site. In terms of increasing parallelism, both database servers can run queries simultaneously. This can speed the execution and reduce waiting time. This data replication will be implemented by using MySQL. For instance, MySQL database was quite popular among database systems as it is a very attractive task in the implementation of replication. MySQL replication is a database that processes and allows you to easily maintain multiple copies of a MySQL data by having them copied automatically from a master to a slave database. Master server is a database that has original copy of data while Slave server is database that contains replicated copy of data. Data encryption is used all over the place in todays connected society. As a modern society becomes more connected, and more information becomes available there is need for safeguards which bring data integrity and data secrecy. In addition, authenticating the source of information gives the recipient, with complete certainty, that the information came from the original source and that it has not been altered from its original state. Data encryption translates data into another form, or code, so that only people with access to a secret key formally called a decryption key or password can read it. Encrypted data which cannot be read by humans is called ciphertext, while human readable data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Types of data encryption are divided into two types which are symmetric encryption and asymmetric encryption. The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks. The examples of encryption algorithms that are popular are AES, Blowfish, Two fish, Triple DES, MD5 and many more

I. TECHNOLOGY

Symmetric-key algorithms: These algorithms use the same key for both encryption and de cryption. Examples include the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES).

Asymmetric-key algorithms: These algorithms use a pair of keys for encryption and decryption, a public key and a private key. Examples include the RSA algorithm and the Elliptic Curve Cryptography (ECC) algorithm.

Hash functions: These algorithms create a fixed-size hash value (also known as a message digest) from input data. They are used for data integrity checks, but are not generally used for encryption. Examples include the Secure Hash Algorithm (SHA) and the Message Digest Algorithm (MD5).

Digital signatures: These are used to authenticate the source of a message and to ensure that the message has not been tampered with. They are often used in conjunction with asymmetric-key algorithms.

Quantum cryptography: This is a emerging field that involves using quantum mechanical phenomena, such as the principle of superposition, to perform cryptographic tasks. It is still in the early stages of development, but has the potential to provide significantly more secure encryption than classical methods.

II. PROPOSALS

Secure communication: Encryption is used to secure communication over networks, such as the internet, to prevent unauthorized parties from accessing the information being transmitted. This includes applications such as email, instant messaging, and virtual private networks (VPNs).

Data storage: Encryption is also used to protect data stored on devices, such as laptops, smartphones, and servers. This ensures that the data remains confidential even if the device is lost or stolen.

Payment systems: Encryption is essential for secure online transactions, such as online shopping and banking. It helps to protect sensitive financial information from being accessed by unauthorized parties.

Internet of Things (IoT): Encryption is used to secure the communication between IoT devices, such as smart home devices and wearable devices. This helps to prevent attackers from accessing the data being transmitted by these devices.

Cloud computing: Encryption is used to protect data stored in the cloud and to secure the communication between cloud servers and clients.

In the future, encryption and decryption will continue to be important for securing data and communication in a wide range of applications. There is also likely to be an

increasing focus on developing new and more secure encryption algorithms, as well as on finding ways to efficiently implement and use encryption in new technologies, such as quantum computers.

III. RESULTS

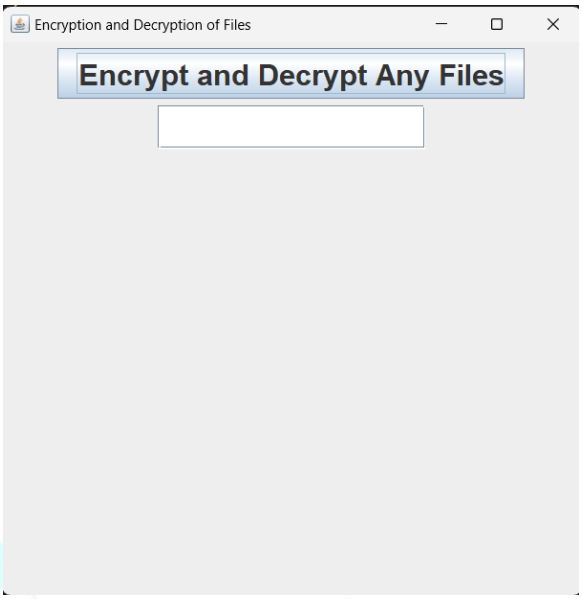
So here we can see that it is finally working and we have given it a interface to make it to easier for the user to use all we can say it gives us a GUI. The effectiveness of encryption and decryption depends on several factors, including the strength of the algorithm being used, the length and complexity of the keys being used, and the security practices of the organization implementing the encryption.

One key factor that determines the effectiveness of encryption is the strength of the algorithm being used. Strong algorithms are resistant to cryptographic attacks and are able to withstand efforts to break them. On the other hand, weaker algorithms may be more vulnerable to attacks and may be easier to break.

The length and complexity of the keys being used is also important. In general, longer and more complex keys provide stronger encryption, as they are more difficult to guess or crack.

Finally, the security practices of the organization implementing the encryption are also important. This includes things like properly securing and managing keys, regularly updating software and protocols, and following best practices for secure communication and data handling.

Overall, encryption is an effective method for protecting the confidentiality, integrity, and authenticity of data. When implemented correctly, it can help to ensure that sensitive information is secure and is only accessible to authorized parties. However, it is important to regularly review and update encryption protocols and practices to ensure that they remain effective.



IV. SIMULATION

To simulate the encryption and decryption of data, you will need to choose an encryption algorithm and then implement it in your simulation. This will typically involve writing code that takes the plaintext data and the encryption key as input, and produces the encrypted ciphertext as output. To decrypt the data, you will need to use the decryption key and the same algorithm to reverse the process and produce the original plaintext data.

It is important to note that the security of an encrypted system is only as strong as the encryption algorithm and key being used. Therefore, it is important to choose a strong and secure algorithm, and to keep the key secret to prevent unauthorized access to the encrypted data.

V. CONCLUSION

Encryption and decryption are important techniques for securing data and communications. Encryption is the process of converting plaintext into ciphertext using a mathematical algorithm and a key. Decryption is the reverse process of decrypting the ciphertext back into plaintext using the same key.

There are various encryption algorithms available, each with their own strengths and weaknesses. Some commonly used encryption algorithms include symmetric-key algorithms, such as AES and DES, and asymmetric-key algorithms, such as RSA and Elliptic Curve Cryptography.

In symmetric-key encryption, the same key is used for both encryption and decryption, while in asymmetric-

key encryption, a pair of keys is used, a public key for encryption and a private key for decryption.

It is important to use strong encryption algorithms and keys to ensure the security of the data. Additionally, proper key management is crucial in ensuring the security of the encryption process.

Overall, encryption and decryption play a vital role in securing data and communications in today's digital age. It is important to choose the appropriate encryption algorithm and implement it securely to protect sensitive information.

VI. REFERENCES

- William Stallings, Cryptography and Network Security Principles and Practice, seventh edition, 2017.
- Beg, A.H, Noraziah, A.Abdulla, A.N and Rabbi, K.F, Framework of Resistance layer synchronous replication to improve data availability into a heterogeneous system, international journal of computer theory on engineering, 5(4), 611, 2013.
- Nidhi Singhal and J.P.S.Raina, Comparative analysis AES and RC4 for better Utilization, International Journal of Computer Trends and Technology, July to Aug Issue 2011. [4] M.Pitchaiah, Philemon Daniel and Praveen, Implementation of Advanced Encryption Standard (AES) Algorithm, International Journal of Scientific & Engineering Research Volume 3, Issue 3, March, 2012.
- Nishtha Mathura and Rajesh Bansodeb, AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection, 7th International Conference on Communication, Computing and Virtualization, 2016.
- Manju Suresh and Neema M, 4 Hardware implementation of Blowfish algorithm for the secure data Transmission in Internet of Things, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, RAEREST, 2016.
- S.Suganya and R.Kalaiselvan, An Optimization and Security of Data Replication in Cloud Using Advanced Encryption algorithm, International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 5 Issues, 6 June 2016.
- Amandeep Kaur and Sarpreet Singh, Improved Storage Security Scheme using RSA & Twofish algorithm at Window Azure Cloud, International Journal of Computer Trends and Technology (IJCTT), volume 4 Issue, July 2013.
- Sumalatha Potteti and Namita Parati, Secured Data Transfer for Cloud Using Blowfish algorithm, International Journal of Soft Computing and Artificial Intelligence, ISSN: 2321-404X, Volume-3, Issue-2, and November, 2015. [10] Neha and Mandeep Kaur Enhanced Security using Hybrid Encryption Algorithm, International Journal of Innovative Research in Computer and Communication Engineering, (An ISO 3297: 2007 Certified Organization)Vol. 4, Issue 7, July, 2016.
- M Rama Raju and J Purna Prakash Protecting Data in Cloud Storage Using Blowfish Encryption Algorithm and Image-Based One-Time Password CSE Department, Christu Jyothi Institute of Technology & Science, 2016.
- Sakshi Joshi Arpit Agrawal, Secure Storage and Replication Using Hybrid Cryptographic Algorithm for Cloud Environment, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 1, January, 2018.
- Rizky Riyaldhi, Rojali and Aditya Kurniawan, Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.Box Modification Mapping In Mix Column, 2nd International Conference on Computer Science and Computational Intelligence 2017, ICCSCI 2017, 13-14 October 2017, Bali, Indonesia.
- P. Princy, a Comparison of Symmetric Key Algorithms Des, Aes, Blowfish, Rc4, Rc6: A Survey, Research Scholar, School of Computer Science, Engineering and Applications, Bharathidasan University, Trichy, India and May, 2015.
- Ayush Kesarwani and Milind Mathur, Comparison between Des, 3des, Rc2, Rc6, Blowfish and Aes, Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.
- Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).
- http://shodhganga.inflibnet.ac.in/bitstream/10603/42667/9/09_chapter%201.p df
- https://ubuntuforums.org/archive/index.php/t-922217.html
- https://www.linuxtrainingacademy.com/mysql-master-slave-replicationubuntu- linux/
- http://manpages.ubuntu.com/manpages/trusty/man1/ccrypt.1.htm