Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 02, February-2022

Secure Text Transfer using Diffie-Hellman Key Exchange based on Cloud

Mohd Tajammul
Jain University
Bangalore, India

L. Vijeeth Reddy
Jain University
Bangalore, India

***Abstract*—The cloud computing architecture is widely embraced by businesses. It offers on-demand service, extensive network connectivity, flexibility, and other benefits. However, the use of these traits is hampered by several security issues. When a cloud service user uploads sensitive data to the cloud platform, it must be sent securely. Steganography is a method of concealing private or sensitive information in what seems to be an ordinary text file. Steganography is the process of concealing Text Messages such that they appear to be any other file. When someone looks at the text file, he or she will have no notion that it contains concealed information. Human senses are not trained to hunt for files that contain information, which is what steganography effectively accomplishes. This system allows users to transmit text as a secret message within a text file, where the user uploads the file to send it secretly and provides a key or password to lock the content. This key encrypts the text so that it cannot be read even if it is hacked by a hacker. To decode the secret text, the receiver will require the key. The user then transmits the text file and key to the receiver, who opens the file, enters the key or password for text decryption, and then pushes the decrypt key to obtain the secret text from the sender. You may double-check that your secret message is transmitted without outside influence from hackers or crackers if you use this approach. If the sender delivers this text file to the public, people will have no idea what it is and will get it.**

I. INTRODUCTION

The system allows users to transmit text as a secret message within a text file, where the user uploads the file to send it secretly and provides a key or password to lock the text, which encrypts the content so that even if it is hacked by a hacker, the text cannot be read. The key will be required by the receiver to decrypt the concealed text. The user then transmits the text file and key to the receiver, who first opens the file, then enters the key or password for text decryption, and finally pushes the decrypt key to obtain the sender's secret content.Using this approach, you may double-check that your secret communication is conveyed quietly and without outside influence from hackers or crackers.If the sender sends this text file in public, no one will know what it is, and only the receiver will get it.

II.RELATED WORKS

The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet. To provide a consistent object-oriented programming environment whether object code is stored and executed locally, executed locally but Internet-distributed, or executed remotely.[1]

The .NET Framework has two main components: the common language runtime and the .NET Framework class library. The common language runtime is the foundation of the .NET Framework. You can think of the runtime as an agent that manages code at execution time, providing core services such as memory management, thread management, and remote, while also enforcing strict type safety and other forms of code accuracy that ensure security and robustness. In fact, the concept of code management is a fundamental principle of the runtime. Code that targets the runtime is known as managed code, while code that does not target the runtime is known as unmanaged code. The class library, the other main component of the .NET Framework, is a comprehensive, object-oriented collection of reusable types that you can use to develop applications ranging from traditional command-line or graphical user interface (GUI) applications to applications based on the latest innovations provided by ASP.NET, such as Web Forms and XML Web services.[2]

Passwords are highly used for encryption in untrustworthy environments like cloud storage etc,. This is more about encryption[3]

Studying the history of how this method evolved. For example there is a method of non manual operation where server will take care of that automatically[4-9]

Here the discussion is about the cloud computing, encryption and how to use them, implement and learning about more of existing ways to use[10-23]

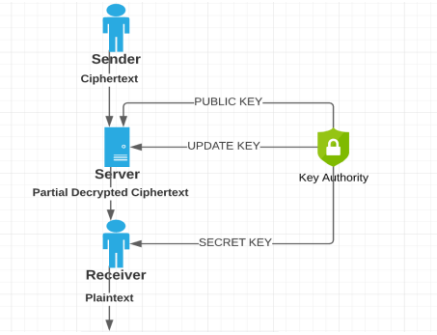
III.GOAL & OBJECTIVE

The goal of this survey is to learn about a safe channel for transmitting and receiving secret text messages. The text message is encrypted and securely transferred to the recipient using Chaff and Winnow and AES (Advanced Encryption Standard) encryption techniques. The system encrypts the user's secret text message and key information before transmitting it to the receiver using AES encryption.

As we all know, the security threats are increasing everyday. There is no guarantee that sharing information with another person is processed safely without any obstruction of hacking or cracking. By the end of this survey we will learn about a method which will be using encryption to hide the actual message and share the information you want securely.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 02, February-2022

IV.ARCHITECTURE



V.EXISTING SYSTEM

There was no such security technique used for hiding text data and sending it securely to the receiver.
Sending a text message to another party would be easily readable by anyone.
By applying various combinations, hackers would easily break the security of the text message.
No such secure path was used to send a text message securely.

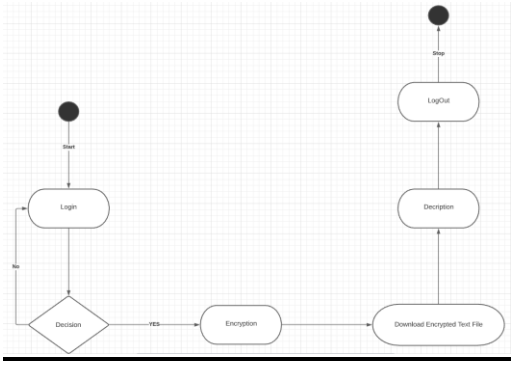
Drawbacks of the existing system

- Maintenance of the system is very difficult.
- There is a possibility of getting inaccurate results.
- User friendliness is very less.
- It consumes more time for processing the task.

VI.PROPOSED SYSTEM

- Considering the anomalies in the existing system, computerization of the whole activity is being suggested after initial analysis.
- The project is developed using Visual Studio with Asp .Net with C# as a programming language.
- There is only one entity who will have the access to the system either it would be a sender or a receiver.
- Users first need to login using its login credentials and then only he/she can access the system.
- Steganography is the technique of hiding private or sensitive information within something that appears to be nothing be a usual text file.
- Steganography involves hiding text so it appears to be a normal text file containing encrypted data.
- If a person views that object which has hidden information inside, he or she will have no idea that there is any secret information.
- What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them.
- What this system does is, it lets user to send text as secrete message inside an text file where, user uploads the file to send it secretly and gives a key or a password to lock the text, what this key does is, it encrypts the text, so that even if it is hacked by hacker it will not be able to read the text.
- Receiver will need the key to decrypt the hidden text.
- A secret key is generated using the Diffie Hellman Key Exchange Algorithm for better security.
- User then sends the text file and key to the receiver where the receiver first opens the file, and then he enters the key or password for decryption of text, he then presses the decrypt key to get secret text from the sender.
- By using this method, you can double ensure that your secret message is sent secretly without outside interference of hackers or crackers.
- If the sender sends this text file in public, others will not know what it is, and the receiver will receive it.
- The system uses an online database to store all related information.

VII.FLOW CHART



VIII.CONCLUSION

This is my survey of System Design about “Secure Text Transfer” application based on Asp .Net with C# i.e. Web Application. On my way of survey I also found out about the method where there will be no need for a manual code sending process. Instead the server itself will generate one code and send it to the mentioned receiver's mail.

XI.REFERENCES

[1] Microsoft Developer Network (MSDN): http://msdn2.microsoft.com/en-us/default.aspx: This is a valuable online resource, and is a must for any developer using Microsoft tools.
[2] http://www.asp.net/: This is the official Microsoft ASP.NET web site. It has a lot of: tutorials, training videos, and sample projects.
[3] Clemens Zeidler, Muhammad Rizwan Asghar “AuthStore Password-based Authentication and Encrypted Data Storage in Untrusted Environments”,2018.
[4] http://ijics.com/gallery/58-may-1148.pdf
[5] https://www.researchgate.net/publication/317339928_A_study_on_diffie-hellman_key_exchange_protocols
[6] https://www.researchgate.net/publication/276232372_A_New_Three-party_Key_Exchange_Protocol_Based_on_Diffie-Hellman
[7] https://www.researchgate.net/publication/321947600_The_Generalized_Diffie-Hellman_Key_Exchange_Protocol_on_Groups
[8] https://www.researchgate.net/publication/289101681_Modification_of_Diffie-Hellman_Algorithm_to_Provide_More_Secure_Key_Exchange
[9] https://link.springer.com/content/pdf/10.1007%2F3-540-48892-8_26.pdf
[10] Alam T., Tajammul M., Gupta R. (2022) Towards the Sustainable Development of Smart Cities Through Cloud Computing. In: Piuri V., Shaw R.N., Ghosh A., Islam R. (eds) AI and IoT for Smart City Applications. Studies in Computational Intelligence, vol 1002.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 02, February-2022

[11] Tajammul, M., Shaw R.N., Ghosh A., Parveen R. (2021) Error Detection Algorithm for Cloud Outsourced Big Data. In: Bansal J.C., Fung L.C.C., Simic M., Ghosh A. (eds) Advances in Applications of Data-Driven Computing. Advances in Intelligent Systems and Computing, vol 1319.
[12] Tajammul, M, Parveen, R., "Cloud Storage in Context of Amazon Web Services", International Journal of All Research Education and Scientific Methods, vol. 10, issue 01, pp. 442-446, 2021.
[13] Tajammul, M., Parveen, R., "Auto Encryption Algorithm for Uploading Data on Cloud Storage", BIJIT - BVICAM's International Journal of Information Technology, vol. 12, Issue 3, pp. 831-837, 2020.
[14] Tajammul, M., Parveen, R., "Key Generation Algorithm Coupled with DES for Securing Cloud Storage," International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019 no. 5, pp. 1452–1458, 2019.
[15] Tajammul M., Parveen R., "Two Pass Multidimensional Key Generation and Encryption Algorithm for Data Storage Security in Cloud Computing", International Journal of Recent Technology in Engineering, Vol. 8, Issue-2, pp. 4152–4158, 2019.
[16] Tajammul M., Parveen R., "Algorithm for Document Integrity Testing Pre-Upload and Post- Download from Cloud Storage", International Journal of Recent Technology in Engineering, Vol. 8, Issue-2S6, pp. 973–979, 2019.
[17] Tajammul, M., Parveen, R., "Auto Encryption Algorithm for Uploading Data on Cloud Storage", BIJIT - BVICAM's International Journal of Information Technology, vol. 12, Issue 3, pp. 831-837, 2020.
[18] Tajammul, M., Parveen, R., and M. Shahnawaz, "Cloud Computing Security Issues and Methods to Resolve: Review," Journal of Basic Applied Engineering and Research, vol. 5, no. 7, pp. 545–550, 2018.
[19] Tajammul, M., Parveen, R., Delhi, N. (2018). Comparative Study of Big Ten Information Security Management System Standards, International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 2, pp. 5-14, 2018.
[20] M. Tajammul, R. Parveen, N. K. Gaur and S. D, "Data Sensitive Algorithm Integrated with Compression Technique for Secured and Efficient Utilization of Cloud Storage," 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON), 2021, pp. 1-9, doi: 10.1109/GUCON50781.2021.9573648.
[21] Tajammul, M., Parveen, R., (2017). Comparative Analysis of Big Ten ISMS Standards and Their Effect on Cloud Computing, 978-1-5386-0627 8/17/31:00c2017IEEE; 9001; 362367.
[22] Tajammul, M., and R. Parveen, "To Carve out Private Cloud with Total Functionality," 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2020, pp. 831-835, doi: 10.1109/ICACCCN51052.2020.9362826.
[23] M. Tajammul, R. Parveen and I. A. Tayubi, "Comparative Analysis of Security Algorithms used in Cloud Computing," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 2021, pp. 875-880, doi: 10.1109/INDIACom51348.2021.00157.