EFFICIENT FILTRATION WITH SATISFYING QUERIES IN DATA SECURITY

Mr. M. Kannan
Assistant Professor and Head i/c
Department of Computer Science with Data Science
SRM Arts and Science College, Kattankulathur
kannancitm@srmasc.ac.in
https://doi.org/10.34293/9789361639715.shanlax.ch.036

Abstract

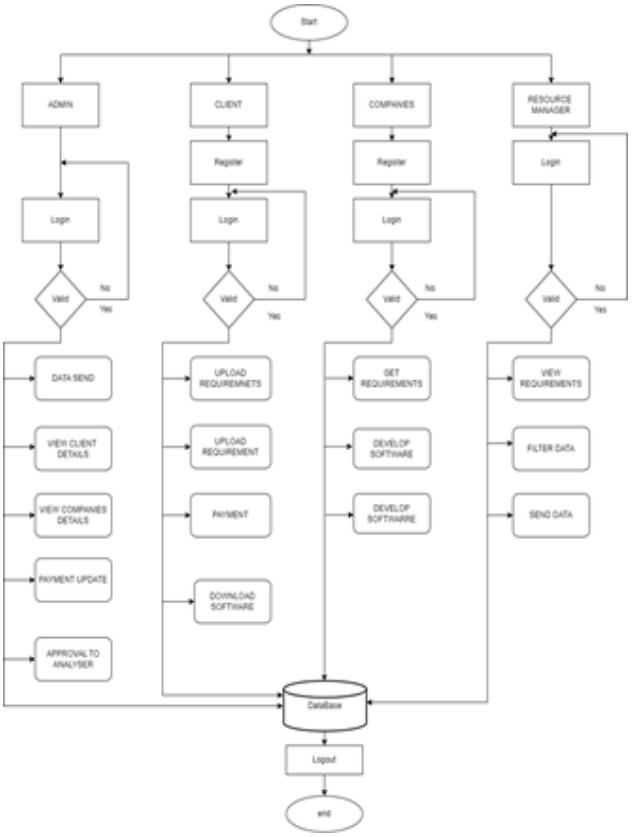
Cryptography is used to offer the excessive stage of protection to the statistics despatched via way of means of encryption and decryption method. The AES algorithm (additionally called the Rijndael algorithm) is a symmetrical block cipher algorithm that takes simple textual content in blocks of 128 bits and converts them to ciphertext the use of keys of 128, 192, and 256 bits. Since the AES algorithm is taken into consideration secure, it's miles with inside the international standard. AES algorithm makes use of a 128-bit symmetric, or single-key, block cipher that encrypts and decrypts records. The AES encryption method creates ciphertext, that is an unreadable, efficaciously indecipherable conversion of plaintext statistics, the model of records that people can examine and understand. This utility has proposed on securely get the software program necessities with extra ordinary agencies and expand the software program. Firstly lot of software program mission are uploaded then it could be filtered via way of means of shortest of entirety statistics. It may also more over has been stored in encrypted layout that is used to save you the statistics from the unauthenticated client. The encryption has consists of key generator a good way to used to generate particular key for each encryption method, it moreover has been very securely coping with of statistics. After a key has been generated, the equal Key Generator item may be re-used to generate similarly keys. The Key generator has been the use of to generate extraordinary keys randomly with assist of RNG (Random Number Generator) at on every occasion whilst encrypting the statistics. The fundamental purpose of this advice gadget is to deal with the software program requirement statistics and software program as securely keep in database.

Keywords: *Encryption, Ciphertext and Random Number Generator*

Introduction

Although software has to be easy to use and secure for the IT industry, non-IT companies have strict requirements of software security. To put it simply, businesses outside the IT industry need to process software securely. These may include government agencies, banks, and other businesses that require access to sensitive information in a highly regulated environment.

We propose a secure control mechanism for most of the software missions using the Advanced Encryption Standard (AES) algorithm. And to control this tricky process, we have to create a new intermediary mechanism. Cryptography is a way to add an extra layer of security to the data being transferred by using encryption and decryption techniques. The Advanced Encryption Standard (AES) algorithm is used to encrypt the statistics (model of information that people can read and understand) into ciphertext (an unintelligible, and practically indecipherable, transformation). This tool has proposed a safe method for obtaining the software program requirements from exceptional agencies and expand the software program.



In the current system, there are no security measures in the program. Unlike most software projects, we have no filtering process to separate the project that will have the shortest completion date from the vast majority of projects that we will not be able to predict which company will do a good job on the project. Also, explain the software requirement to the company. Inversion - there is no shift row/inverse shift row transformation available. Rows serve as the input data. For left and right cyclic shift processes rows are used. The bits in rows other than the first are changed by cyclic filtering or prediction. As a result, the efficiency of the project is very low. The software requirements also cannot be gathered in a secure manner. Code storage that is optimal for the legal access only.

Proposed System

We have developed a system in which every client can get a unique ID and password. The intermediating process is a new way of thinking that we are trying out. According to Customers, it is quite convenient to upload and download the information about the company name. This system has also introduced an encryption technique to help improve security and potentially prevent cyberattacks from ever happening at all.

By managing the encrypted values with administrator view the file can be accessed by authorized users. The administration defined the fair price which the client can pay to purchase the software. A quality software programming provident coverage is a set of instructions that define the procedures and methods, a business.

Conclusion

Added new keywords to rephrase the architecture for encrypted cloud-based data sharing and search (including the security concept). Moreover, we have proposed an optimized scheme that satisfies the concept by combining identity-based signed encryption, asymmetric pair group conversion, identity-based proxy re-encryption, and the searchable "least frequent keyword" approach. We also proved the security of the protocol in the generic bilinear group model. Our solution is highly promising for implementation in very large databases and is cost effective compared with its conference counterpart.

Future Enhancement

Our proposed version has already implemented AES algorithm. According to the key, the proposed method can effectively produce the user key, which can be used to encrypt the data and shield the data from malicious users. The filtration process will help you to determine which project will be finished first. This is how the system is used to identify which business can try to take on this project at the right time and in the right way. AES is an encryption method that stores data in an encrypted form in order to secure it from malicious users. As a result, our proposed version is highly effective and satisfies industrial requirements. The proposed version is suitable for the industrial requirement and gives good output. Primary Advantage of this device is that we can choose the company which is able to perform this task perfectly at that time.

The most important thing is the protection of the code and the integrity of the software program until it reaches the client. This technology is used to protect code from illegal access and modification, verify the integrity of the software, and safeguard the software after it's already in operation.

References

1. Siavosh Benabbas, Rosario Gennaro, and Yevgeniy Vahlis. Verifi- able delegation of computation over large datasets. In Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, volume 6841 of LNCS, pages 111–131. Springer, 2011.
2. Ran Canetti and Susan Hohenberger. Chosen-ciphertext secure proxy re-encryption. In Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, pages 185–194. ACM, 2007.
3. David Cash, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, and Michael Steiner. Highly-scalable search- able symmetric encryption with support for boolean queries. In Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, volume 8042 of Lecture Notes in Computer Science, pages 353–373. Springer, 2013
4. Peng Jiang, Fuchun Guo, Kaitai Liang, Jianchang Lai, and Qiaoyan Wen. Searchain: Blockchain-based private keyword search in decentralized storage. Future Gener. Comput. Syst., 107:781–792, 2020.

5. Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Tran Viet Xuan Phuong, and Qi Xie. A DFA- based functional proxy re-encryption scheme for secure public cloud data sharing. IEEE Transactions on Information Forensics and Security, 9(10):1667–1680, 2014.
6. KaitaiLiang, Cheng-Kang Chu, XiaoTan, DuncanS.Wong, Chun- ming Tang, and Jianying Zhou. Chosen-ciphertext secure multi- hop identity-based conditional proxy re-encryption with constant- size ciphertexts. Theory. Comput. Sci., 539:87–105, 2014.
7. KaitaiLiang, Joseph K. Liu, Duncan S. Wong, and WillySusilo.An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing. In Computer Security