Two-Factor Authentication for Standalone System Using Two Fish Algorithm

[1]A Anil, [2]S Mohan Ravi Shankar, [3]S Ganesh Sumanth, [4]T Deeraj, [5]Mrs K Anuranjini

[1,2,3,4]Student, [5]Assistant Professor
[1,2,3,4,5]Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research

Abstract: Data protection is a demanding task in the field of information security. Data sequestration is the primary concern in information technology. At the moment two- factor authentication is extensively used in online surroundings. With this type of authentication indeed if the username and word have been compromised the authentication to lines can not take place, because there we introduced a law that's unique from train to file. Then we present a protection system by cracking and decoding the lines which offer an enhanced position of protection. This paper focuses on the perpetration of two-factor authentication styles by using both druggies-friendly traditional Alphanumeric watchwords and the private key as a gateway for authentication. An attempt has been made by using two-factor Authentication and in this paper, we describe the two-factor Authentication system design and design perpetration. therefore swinging a fresh word adds a redundant subcaste of security.

INTRODUCTION:

From correspondence to plutocrats when everything is getting digital, the Internet becomes the one and main medium of communication in all aspects of our life. Meanwhile smelling, intrusion, and denial of service-like pitfalls to information are also adding day by day. therefore encryption becomes the necessity of the hour. Encryption means the art and wisdom of secret jotting. It stores and transmits information safely over an insecure medium like the Internet by garbling plain textbooks into cipher textbooks with the help of colorful encryption algorithms. The encryption algorithms are generally distributed into two popular types Symmetric crucial encryption and Asymmetric crucial encryption. In Symmetric crucial encryption, the same key is used to cipher and decipher data. The key has to participate before transmission to the sender and receiver. The length of the Key has an important place in Symmetric crucial encryption. For the same algorithm, encryption using a longer key is hard to cryptanalysis means further security as compared to the one using a shorter key.
Security is a major concern moment in all sectors similar as banks, governmental operations, military associations, educational institutions, etc. Government associations are setting norms, passing laws, and forcing associations and agencies to misbehave with these norms without with non-compliance being met with wide-ranging consequences. There are several issues when it comes to security enterprises in this multitudinous and varying diligence with one common weak link being watchwords. The rapid-fire growth in the number of online services leads to an adding number of different digital individualities each stoner needs to manage. But watchwords are maybe the most common type of credential used moment. To avoid the tedious task of flashing back delicate watchwords, druggies frequently bear less securely by using low entropy and weak watchwords. utmost systems moment calculate on stationary watchwords to corroborate the stoner's identity. still, similar watchwords come with major operation security enterprises. druggies tend to use easy-to-guess watchwords, use the same word in multiple accounts, or store them on their machines, etc. likewise, hackers have the option of using numerous ways to steal watchwords similar as shoulder surfing, poking, smelling, guessing, etc. also, watchwords can be written down, forgotten and stolen, and guessed designedly being told to other people.

LITERATURE SURVEY:

[1] Rushikesh Nikam, and Manish Potey. Some online data services often come with security issues such as confidentiality and integrity. The problem scenario ranges multi-fold: to secure organizational data from peer organizations, to provide sharing of data files between users keep the identity anonymous, to handle recovery of vital data modules, etc. This paper proposes a solution to eliminating the above-mentioned problems. The solution aims at achieving Confidentiality using CP-ABE (Ciphertext Policy-Attribute Based Encryption) and user authentication with Multifactor Authentication (MFA). Security is achieved at various levels such as providing a static username-password as the entry-level authentication, followed by OTP based on the token generator technique. These tokens are generated using QR code technology and act as credentials for each user. The provision of default tokens is also available for genuine users that fail to use the QR code generator at some point. This allows availability to authorized users. Encryption is done using CP-ABE.
CP-ABE(Algorithm) In CP-ABE, it is not the set of attributes that do the working but the policies defined over a set of attributes carry the encryption process. In this scheme, the User's private key is based on a group of attributes whereas the ciphertext is based on the access structure defined over system-specific attributes. A user can decrypt a text if his attributes satisfy the policy specified in the cipher text. Policies are defined over attributes using conjunctions, disjunctions, and {n, m}-threshold gates, i.e. n out of m attributes have to be present. In CP-ABE there is no separate access control or authorization mechanism. It is incorporated into the encryption mechanism itself. Users can even obtain their secret keys after data encryption using the access structure is an important add-on. Hence, data can be encrypted even with not knowing the genuine user groups which can decrypt, and only specifying the

policy is quite enough. Future users are given a key based on the attributes that the policy satisfy and such users are only genuine decrypters of the system.

[2] Mousa, Allam**.** In This Paper Some of the important parameters of the Blowfish encryption algorithm are analyzed and examined to see how these parameters may affect the performance of the algorithm. The peflonnance indices here are the security and speed of the algorithm. For each case, the eng. ptioddecryption kq length has been changed and its effect on the performance p is noticed. Moreover, the file size is changed and its effect on the performance of the algorithm was noticed. This has shown that changing the key length does not affect the encryption or decryption time whereas changing the plaintext file size is directly rejected on the processing time.

Encryption is hiding data while being transmitted or stored. That is transforming the information from one form (plain text) into another one (cipher text) by using certain algorithms depending on some keys. On the other hand, decryption is transforming the cipher text back to its plain text using the same algorithm and key. This algorithm consists of some mathematical functions and operations that perform the encryption process in many ways. and the key is a specific number (usually a Large one) that is usually used by the algorithm and its calculations. Key management is the set of procedures supporting the establishment and maintenance of keying relationships between authorized parties. Thus the risk is transferred from the problem of securing the data to the problem of securing and managing keys. An important issue here is choosing the encryption key, this depends on many things such as how long does the data need to be kept secure? What kind of encryption is being used (symmetric or asymmetric)? How valuable is the data being secured? For information that needs to be secure for only minutes, hours, or perhaps weeks, a 64-bit symmetric key will suffice. For data that needs to be secure for years or decades, a 128-bit key should be used. For data that needs to remain secure for the foreseeable future, one may want to go with as much as a 160-bit key.

Blow Fish(algorithm) Some of the Blowfish algorithm specifications can be summarized as [3], [4];

1. Symmetric block cipher.
2. 64-bit Block.
3. Variable-length key, from 32-bit (4 Bytes) to 448
4. Run at an acceptable clock speed.
5. Suitable and efficient for hardware implementation
6. Unpatented and no license is required.

The algorithm consists mainly of two parts; the key-expansion part and the data-encryption part (51. Key expansion converts a key of at most 448 bits into 4168 bytes. There is a P-array and four 32-bitS-boxes. The P-array contains 18, 32-bit subkeys, while each S-box contains 256 entries. Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round [4].

[3] Rizvi, S. A. M. In this Paper The two main characteristics of a good encryption algorithm are Security and Speed. Usually, security algorithms have to be embedded in a variety of applications like e-banking, online shopping, mail, etc. So they should be fast as well as secure in different environments. In this paper, we do a security v/s performance analysis of two algorithms Twofish and AES. First, we will discuss the security issues of both algorithms by considering their safety factor. Then we study the encryption speed of both algorithms by encrypting different types of data (text, image, audio) and analyze their performance in terms of throughput of every algorithm on different sizes of RAMs. The results show the relationship between the performance of algorithms and size of RAM and the type of data.

From mail to money when everything is getting digital, the Internet becomes the one and main medium of communication in all aspects of our life.

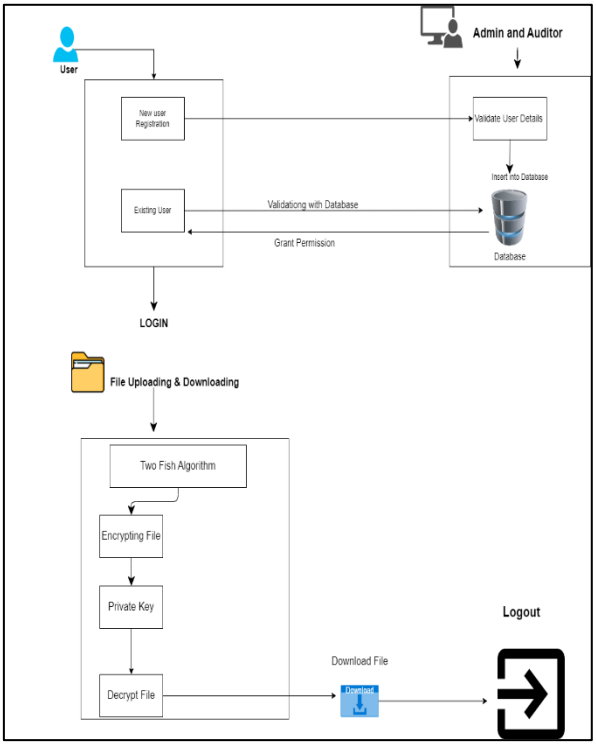
TwoFish and AES(Algorithm) Twofish is an algorithm from Counterpane Internet Security, it is highly suited for large microprocessors and also for smart card microprocessors. A brief overview of the concepts and considerations relevant to the Twofish design procedure is given in [2]. Currently, the best attacks on Twofish use different versions of differential cryptanalysis, None of them succeeds on the full number of rounds with the present computational power. B. AES has a Non-Feistel structure, based on a sophisticated mathematical design. Its simple structure attracts cryptographers and cryptanalysts. It encrypts 128-bit block size with 128/192/256 bit key for 10/12/14 rounds. AES has a safety factor of less than 2, which implies that it is somewhat more delicate for the advancements of cryptanalysis. Making the safety factor of AES equivalent to Two-fish would require 24 rounds of AES. An increase in the number of rounds may reduce its performance.

[4] Zhou, Xin, and Xiaofei Tang. In this Paper Cryptographic technique is one of the principal means to protect information security. Not only has it ensure the information is confidential but also provides a digital signature, authentication, secret sub-storage, system security, and other functions. Therefore, the encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery, and counterfeiting. The encryption and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, also depends on the key confidentiality. Key in the encryption algorithm has a pivotal position, once the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information, it means the encryption algorithm is useless. Therefore, what kind of data you choose to be a key, how to distribute the private key, and how to save both data transmission keys are very important issues in the encryption and decryption algorithm. This paper proposed an implementation of a complete and practical RSA encrypt/decrypt solution based on the study of the RSA public key algorithm. In addition, the encrypt procedure and code implementation are provided in detail.

PROPOSED SYSTEM:

In this system, we proposed a private key as a fresh authentication to the account and the individual lines through encryption and decryption ways.
Then, we used the Two- Fish Algorithm. It's a symmetric key block cipher.
In cryptography, a symmetric key is used both to cipher and decipher the information.
It uses a block size of 128 bits, having a crucial length of 256 bits. It takes 16 rounds of encryption.

SYSTEM ARCHITECTURE:



MODULE DESCRIPTION:

- Congregation and Endorsement of Data.
- Generation of Authentication Keys - Random Class function.

Congregation and Endorsement of Data:

In today's world user data is the primary asset to any organization and sector. Authentication enables organizations to keep their networks secure by permitting only authenticated users or processes to gain access to their protected resources. In the initial stage of this step, we are getting the user's information through the user registration process. We treated it as input for our application. Thereby getting the user's information, owners are validating their input. Later, we are enabling users to use the application for uploading and downloading their files securely.

Generation of Authentication Keys - Random Class function:

In this module, we are providing the user authentication in one more layer by providing a key known to be secret in addition to the username and password. True Random Number generation is surprisingly difficult to do right. One of the results is that even now, there is no 'approved' or 'standardized' method for generating truly random numbers. By using the random function, we are creating the secret key and the private key for the user. When the user is allowed to upload a file, here we are creating a specific key to access the file. Whenever the user uploads a file, it moves to the next module in processing.

CONCLUSION:

We feel that two-factor data authentication for the train-to-train is a better option for advanced security for the stoner's train. Maintaining and Keeping up the challenges can be anticipated, similar to advances in the calculation that are making it precipitously easier to wordbook- attack a word database security to a standard is going to be tougher and further worrisome with time. Some of

with time. Two-factor confirmation is frequently being utilized to work around the

Accordingly, security prerequisites aren't altered, yet proliferation introductory failings in word administration. While two-factor verification does enhance security also it builds customer resistance. Integrated two-factor authentication gives the stylish convenience to more security, so a two-factor evidence invention that can be moved over to coordinate the two rudiments all the more nearly has the stylish capacity to come as conditions change and also to amplify customer uptake of optional two-factor authentication. As the confirm medium for authentication, our view can be suitably and securely used. The abecedarian study is that using our proposed two-factor authentication will provoke further essential security. This, consequently, should formulate universal security

FUTURE WORK:

In the future, two-factor data authentication may be used to efficiently secure lines online. The encryptions made using two- fish algorithms are most welcoming as they're the unborn technologies. Hereafter the encryption and decryption ways would be better and more accurate when they're made using machine literacy ways and models.

REFERENCES:

1. Rushikesh Nikam, and Manish Potey. "Cloud storage security using multi-factor authentication." 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE). IEEE, 2016.
2. Mousa, Allam. "Data encryption performance based on Blowfish." 47th International Symposium ELMAR, 2005. IEEE, 2005.
3. Rizvi, S. A. M., Syed Zeeshan Hussain, and Neeta Wadhwa. "Performance analysis of AES and TwoFish encryption schemes." 2011 International Conference on Communication Systems and Network Technologies. IEEE, 2011.
4. Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." Proceedings of 2011 6th international forum on strategic technology. Vol. 2. IEEE, 2011.
5. A. Nadeem and M. Y. Javed, “A performance comparison of data encryption algorithms”, Information and Communication Technologies, ICICT 2005, pp.84-89, 2005.
6. Li, Yibin, et al. "Privacy protection for preventing data overcollection in a smart city." IEEE Transactions on Computers 65.5 (2015): 1339-1350.
7. Krikor, Lala, et al. "Image encryption using DCT and stream cipher." European Journal of Scientific Research 32.1 (2009): 47-57.
8. Shubhi Mittal, Shivika Arora and Rachna Jain “PData Security using RSA Encryption Combined with Image Steganography”,2016.
9. A. K. Singh and I. Gupta, ‘‘Online information leaker identification scheme for secure data sharing,’’ Multimedia Tools Appl., vol. 79, no. 41, pp. 31165–31182, Nov. 2020.
10. E. Zaghloul, K. Zhou, and J. Ren, ‘‘P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing,’’ IEEE Trans. Big Data, vol. 6, no. 4, pp. 804–815, Dec. 2020