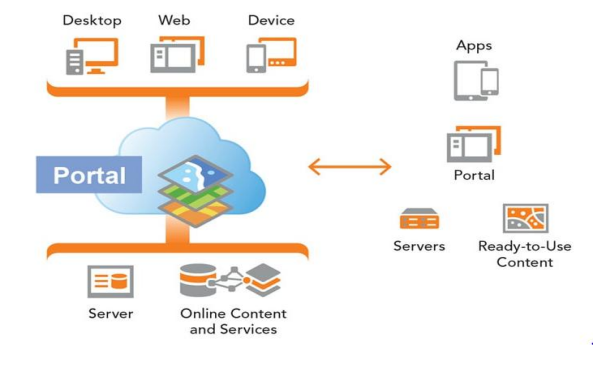
* **INTRODUCTION:**

Maintaining data integrity and data authentication is essential for security in financial transactions, secured content, e-commerce, e-mail, data storage and so on. The broadest definition of authentication within computing systems encompasses identity verification, message origin authentication and message content authentication. In IPSEC, the technique of cryptographic hash functions is utilized to achieve these security services.

* **PROBLEM STATEMENT:**  
  As we know that, MD5 is one way encryption. That means we can’t decrypt MD5 hash string. So, the attack done on hash string are

**1)Brute-force attack:**   
In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.  
**2) Dictionary attack:**  
 A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document. For overcoming these attack we propose the following method.

* **OVERVEIW:**  
  In proposed system, the password will become so secured that there is no chance of Brute force attack or Dictionary attack. In this the system will first manipulate the password after that it will further proceed for MD5 algorithm. But system will apply MD5 algorithm3timeson string. And how it will done we will explain it later. At last the MD5 hashed string will westored in the database.
* **SYSTEM ARCHITECTURE:**
* **APPLICATION OF MD5 ALGORITHM IN PASSWORDAUTHENTICATION:**  
    
  The prerequisite for the security of various Internet applications is the effective identification and authentication of the identity. There are several authentication methods to achieve user authentication.

The current commonly used methods are username/password, digital signature, graphic printing, hardware ID card, etc. Username/password is the simplest and most commonly used method, which is to confirm the validity of the user through password matching.

For ensuring the security of password to prevent users’ password leaking, MD5 algorithm could be used to exchange the content of users’ password. The method is to use MD5algorithm to process the users’ password, and store the changed value in database.

The length of the password content is value of 128 bits. When we verify the users’ identifications, same process the password input by MD5 algorithm, and compare with the MD5 value storedindatabase, if the two values are the same, the user is valid. As the MD5 algorithmic irreversible, the value of information abstract calculated by MD5 cannot get the initial information by inverse algorithm

* **ALGORITHM: Message Digest 5 (MD5) Algorithm**MD5 [3] is a message digest algorithm developed by Ron Rivets of MIT. It is basically secure version of his previous algorithm MD4, which is a bit faster than MD5. This is the most widely used secure hash algorithm, especially in Internet standard message authentication. The algorithm takes messages of any length as input and generates a 128-bit message digest of the input as output. This is mainly used for digital signature applications, where large files must first be compressed in a secure manner before they can be encrypted with a private key (secret) under a public key cryptosystem.

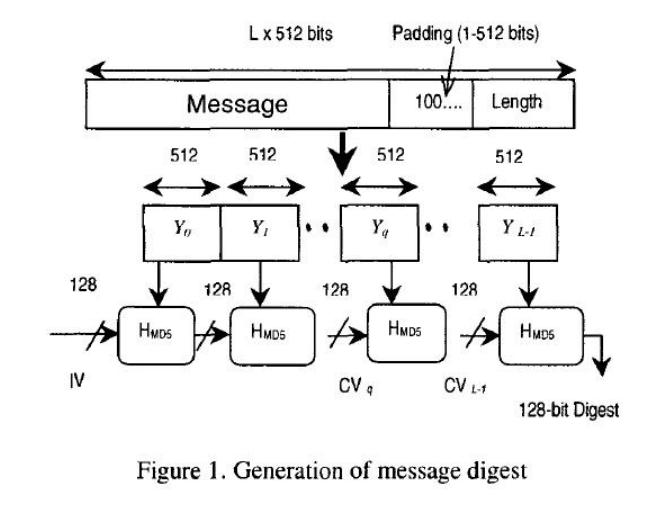
Suppose we have an arbitrarily large message as input, and we want to find its message digest. This process involves the following steps.

1. **Padding:**

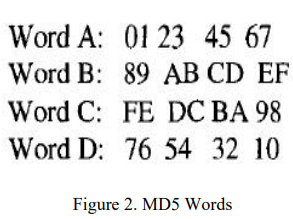
Pad the message to ensure that its length plus 64 is divisible by 512. In other words, its length is equal to 448 mod 512. Even if the length of the message is already equal to 448modulo512, filling is always performed. It consists of a 1-bit, followed by the necessary number of O-bits.

1. **Appending length:**

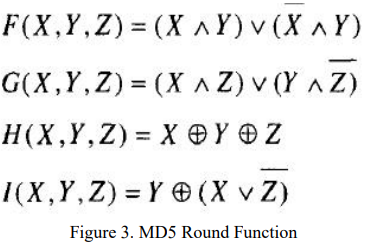
64-bit binary representation of the original message is appended to the result of step(1). The expanded message must be a multiple of 512-bits. The expanded message is represented as a sequence of L 512-bit blocks shown in figure.



1. **Initialize the MD buffer:**  
    The variables IV and CV are represented by the four-word buffer (ABCD) used to calculate the message digest. Here, each A, B, C, D is a 32-bit register, they are initialized to IV, and the following values are expressed in hexadecimal. The lower byte is placed first.



1. **Process message in 16-word blocks :**  
   This is the heart of the algorithm, which includes four “rounds” of processing. It is represented in Figure 1 and its logic is given in Figure 2. The four rounds have similar structure but each uses different auxiliary functions F, G, Hand I



Each round consists of 16 steps. In the 16 steps of each cycle of loop, 16 information blocks with 32 bits are used by different orders. The first cycle is according to the original order; the next three cycles are used after exchange order, the exchange formulas are: ρ2(i) =( 1+5i)mod16，ρ3(i) = ( 5+ 3i) mod16，ρ4(i) = 7imod16. The four loop variables are upgraded in order. Each variable in the second loop is conducted for the third time in the same order and different k [i] and s [i] according to the exchange formula. After 64 steps are completed by mode 32, the initial value and the values of a, b, c, d are added, and then cascaded, and the 128-bit MD5 code is calculated. After all L512-bit blocks have been processed, the output from L th stage is the 128-bit message digest. The constants and Boolean formulas in the algorithm make the algorithm more complicated and less collision.  
  
**Additional Encryption Algorithm Interference:**Before MD5 scheming, add associate cryptography algorithmic program to interfere theMD5process. the essential thought is to write the user's secret through self-defined cryptography algorithmic program to urge cipher code; get MD5 data abstract price by MD5 algorithmic program. There area unit innumerous styles of self-defined cryptography. Take user secret “RISHABH” as associate example to elucidate one amongst the Kinds self-defined cryptography algorithmic program. Presume the secret's “xsw”.  
  
1. Take the length of key as the index to make the plain code as a matrix (fill by spaces with insufficiency), the key and its length are self-defined. The results are like below:

R I S

H A B

H \_ \_

Note:- Here “\_” is a space.  
2. Conduct exclusive-or operation to the elements in each row and corresponding character;

X S W

↑ ↑ ↑

R I S

H A B

H \_ \_

The results are:

& \* $

/ ^ ]

/ A W

* **Code:  
    
  Conclusion:**The MD5 algorithm solves the transmission and storage problems through the clear formof the traditional password form and other security issues. It has proved to be an efficient andstraightforward password authentication algorithm. But it is also threatened by collisionattacks and dictionary attacks. It needs a safer method. This article analyses the applicationofMD5 algorithm and security in password authentication, and puts forward solutions against conflict attacks and dictionary attacks to improve the implementation and security of MD5
* **Refrences:**[1] Xiaoling Zheng. J. Jing, “Research for the application and safety of MD5 algorithmin password authentication” , 2017, International Conference on Fuzzy Systems and Knowledge Discovery vol. 2219

[2] J. Deepakumara, H.M. Heys, R. Venkatesan, “FPGA implementation of MD5 hash algorithm”, 2018, Canadian Conference on Electrical and Computer Engineering vol. 1254

[3] M. Kioon, Z. Wang, “Security Analysis of MD5 Algorithm in Password Storage”, 2019, Applied Mechanics and Materials vol. 347-350

[4] D Rachmawati, J T Tarigan, A Ginting, “A comparative study of Message Digest 5(MD5)and SHA256 algorithmic rule” , 2017, Journal of Physics Conference vol. 978(1)

[5] Zhang Shaolan, Xing Guobo, Yang Yixian, “Improvement to MD5 and Security Analysis[J]” , 2016 Computer Application, vol.29(4):947-949