Performance Evaluation of Message Security Using Fractal Sieve with MMD

Ch. Rupa

Department of Computer Science and Engineering,
VVIT, Guntur (Dt), A. P, India
{rupamtech@gmail.com}

ABSTRACT

In this paper we measure the performance of proposed approach, message security using Fractal Sieve with Modified Message Digest with respect to response time and time complexity. In this method the authentication of the message is protected by the hash function MMD. The response time of the algorithm is implemented in java is calculated with user load and the different sizes of the data files. The results are compared with the performance measurements of Priya Dhawan and Aamer Nadeem and found to be efficient.

KEYWORDS

Fractal Sieve, MMD, Response Time, Time Complexity.

1 INTRODUCTION

The main popular method of authentication is hash algorithms such as MD5, SHA-1, etc. As well as, the key management has played a vital role in the cryptosystem because it improves the security in the aspect of confidentiality, authentication, non repudiation and integrity. If the encryption key is equal with the decryption key then it is referred as symmetric cryptosystem [2]. At preset, to improve the security of a message many different symmetric key mechanisioms are proposed which satisfy the security factors. The main terminologies of the security are plaintext, Encryption, Ciphertext, and Decryption. Encryption consists of a plain text as the original data which is given as input to the algorithm [15], encryption algorithm performs various substitutions and transformations on the original message. Secret key is given as input to the algorithm. The substitutions and transformations are performed by the algorithm. These are depending on the secret key. Then the cipher text is produced as output which is in the form of unreadable format. It depends on the secret key and plain text. Decryption algorithm produces the plain text by taking cipher text and plain text.

Fractal geometric has specific properties that are self similarity and sensitivity [3, 20]. An encryption algorithm proposed by Kocarev, L [1] is vulnerable to all the four of cipher text only, known plain text, chosen plain text and chosen cipher text attacks [14]. Several well-known encryption algorithms such as Blowfish, IDEA, RC5, etc too are not protected to attacks. In the same way hash function algorithms like MD5 , SHA-1 etc are vulnerable to different attacks by wang's [6], Bert Den Boer and Bosselaers [4]. We used a novel approach that is resistant to all the four encryption attacks including Wang's collision attack on message digest. i. e Fractal Sieve with MMD [20].

In this paper portrays the techniques and simulation choices made to evaluate the performance of the compared algorithms. In addition to that, discussed the methodology related parameters like:

DOI : 10.5121/ijsptm.2013.2403

system parameters, experiment factors and experiment initial settings. These are considered for evaluating the performance of the cryptographic hash function MMD which is an algorithm that takes a random block of data and returns a fixed-size bit string i.e message digest or hash value [20]. All hash functions have potential collisions, though with a well-designed hash function, collisions should occur less often or be more difficult to find. A method is proposed as a solution to the attack which was proposed by Xiaoyun Wang [6]. The traditional MD5 algorithm uses 32-bit chaining variables to produce a 128-bit hash. We, in our proposed system use Modified Message Digest (MMD) [7, 8] which is using 64-bit chaining variables to produce a 128-bit hash of the given file thereby reducing the probability for a collision to occur [20].

The rest of the paper is organized by the following way. Section 2 consists of related work. Proposed method is described in section 3. Section 4 holds the results and its study.

2. RELATED WORK

There is enormous literature on the results obtained from Priya Dhawan [21] and Aamer Nadeem [22]. Here, we proposed an advanced authentication method by considering the factors of response time, Complexity and security that utilizes fractal functions and Hash functions in cryptography. Dhawan and Ammer have done experiments to find the performance of MD5. Performance Methodology adopted for the proposed scheme is using a Testing tool of JUnit. The main ingredients of the JUnit test are Unit test cases and wrapper test cases.

To set the maximum number of concurrent users need to use the load method of JUnitPerf for executing the modified message digest. Table 1and table 2 contains the speed benchmarks to 4KB and 135KB data files using existing approaches [21, 22].

Load	Time Taken (ms)
20	0.015
30	0.032
40	0.062
50	0.078
60	0.109

Table 1. Response time for 4 KB

Load	Time Taken (ms)
20	0.016
30	0.015
40	0.032
50	0.078
60	0.141

Table 2. Response time for 135 KB

3. PROPOSED METHOD

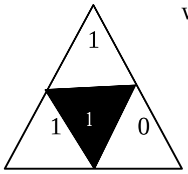
The purpose of the proposed scheme is to give a sophisticated and robust authentication method in the information security concept. As a part of that, uses two phases that are encrypt the data by using sierpinski sieve fractal algorithm [9, 10, 11] as described in the section 3.1 to get the ciphertext (Enc_i) and immediately find the message digest to either original data or encrypted data by using MMD hash algorithm [7] *H(d)* as mentioned in 3.2. The ciphertext and message digest should be participated in the communication from the seder side.

$$Enc_i \leftarrow Sierpinski(d); \quad H(d) \leftarrow MMD(d)$$

At the receiver side, decrypt the message by using the same sierpiski sieve [13] method by applying reversely and calculate the hash value of the either original data or encrypted data. If this hash value is equal with the receiving hash value then confirm it as an authorized message otherwise not. Some attacks are also existed in the present existing algorithms. Hence, here we used modified message digest as a hash function.

3.1. Symmetric Key Encryption using Fractal Geometry

The data that is present at the middle of a triangle is the secret key. The data which is encircling the middle triangle is the original text. The plain text and the key are placed in a selected order such as middle, top, right and left. Based on the keys, the transformation of the plain text is passed out to achieve the cipher text. Both the sender and receiver share the same key so this is symmetric encryption and is normally called as fractal symmetric encryption [9]. First of all the inner triangles are filled with secret key, then the outer triangles are filled with plain text as shown in Fig 1[2, 20].



where key is located at ▼
and data is located at △

Fig 1. N = 1

Let us consider the plain Text is 101and key is 1. According to the proposed procedure of the Gasket If Key is 1 do the right circular shift of the plain text. 1 ← 1, 1← 0, 0← 1 then occurs the cipher text as 011. Main algorithm of this procedure is as follows.

3.2. MMD Hash function

The proposed Message Digest algorithm has 6 steps [20]. The Modified Hash function algorithm is:

1. Calculation of the padding bits.
2. Appending the original length.
3. Division of message into 512-bit blocks.
4. Initialization of 64 - bit chaining variables.
   a. consider the combination of *a*, *b*, *c* and *d* as a 512-bit single register.
5. Performing rounds.

Now, we have four rounds. In each round, we process all the 16 sub-blocks belonging to a block. The inputs to each round are:

a. 16 sub-blocks.
b. Conversion of 256 - bit variables *a, b, c, d* in to 128 - bit variables.
c. some constants, designated as *t*.

This algorithm is vulnerable to Wangs collision attack [XYH05]. The modified algorithm reduces this by using 64 - bit chaining variables instead of a 32-bit one.

In our proposed system we use MMD which is a solution to overcome the Wang’s collision attack by using 64-bit chaining variables instead of 32-bit chaining variables [CRA08]. The chaining variables used in MMD are:

a = F071C170CF7D000 b = 22E55F6C56F76800 c = 1639A228DDC77100   d = 003C56485C7D3706

The Message Digest hashes of the same above two files (attacked by Wang's) using 64-bit chaining variables are:

```
C:\Documents and Setting\Administrator\ Desktop>md5sum hello.exe
   e8f82366773d97200f62ae77131934a1
C:\Documents and Setting\Administrator\ Desktop>md5sum erase.exe
   67ce77b48593b323bcf6cb44e33cbd02
```

Collision attack was happening in the existing hash functions at step 4(Initializing chaining variables). Because it is using 64- bit chaining variables, the possibility that two messages produces the same message digest using existing message digest algorithm is in the order of 2^{64} operations [6]. With the help of Modified Message digest algorithm increase the complexity of the algorithm. This module helps to avoid the collision attack demonstrated by Wang thereby making the algorithm more secure and reliable.

4 RESULTS AND ANALYSIS

Table 3and table 4 shows the speed benchmarks to 4KB and 135KB data files using proposed approaches [20]. Fig 2 shows the comparison results for 4 KB files with the existing and proposed approaches. As well as Fig 3 gives the comparison information for 135 KB files. These testing results show that modified message digest has a better performance than existing technique [21, 22].

Load	Time Taken (ms)
20	0.045
30	0.056
40	0.059
50	0.078
60	0.109

Table 3. Bench mark values for 4KB data files

Load	Time Taken (ms)
20	0.015
30	0.057
40	0.159
50	0.200
60	0.225

Table 4. Bench mark values for 1354KB data files

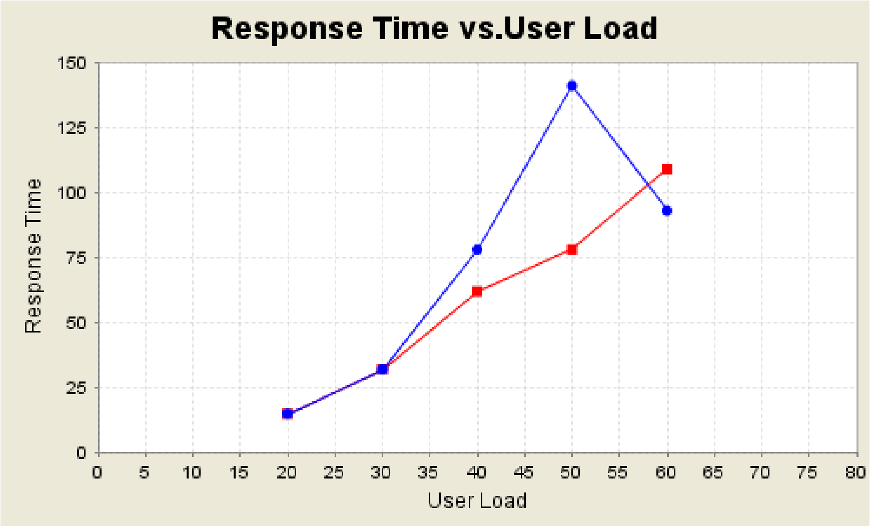


Fig 2. Comparision result for 4 KB Data File

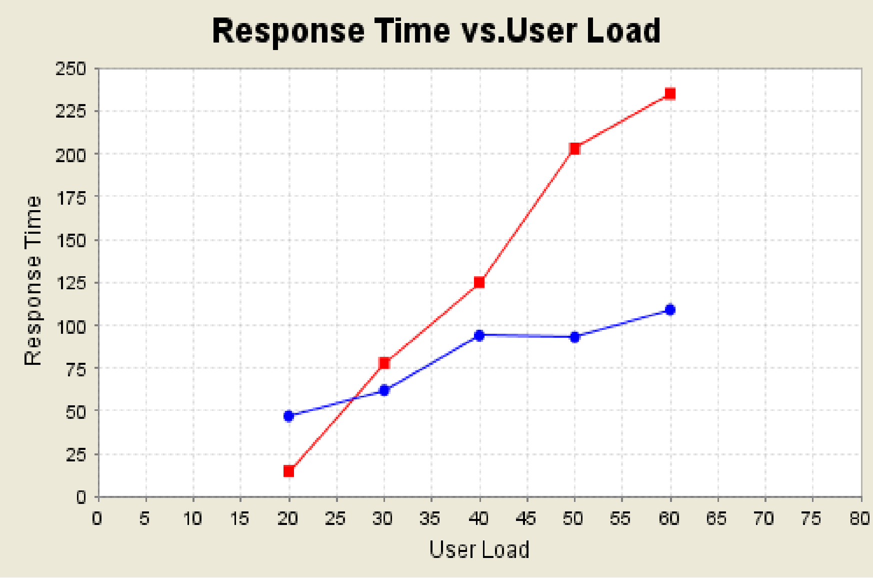


Fig 3.Comparision results for 135 KB Data files with the existing

6. CONCLUSION

The test results which are presented showed that modified message digest with fractal geometry has a better performance than existing approaches by the Aamer and Dhawan. According these tests demonstrate that authentication schemes and hashing algorithms carry different amounts of load, and have various performance characteristics. The sizes of data being passed to find the hashing value, as well as to cryptographic techniques are also significant.

REFERENCES

[1] Kocarev, L.: Chaos-based Cryptography: A Brief Overview, IEEE Circuits and Systems Magazine 1(3), 6-21 (2001)

[2] Buchmann, J.A.: Introduction to Cryptography, pp.71-74 .Springer, Heidelberg (2001)

[3] Devaney, R.L.: Measure Topology and Fractal Geometry. pp.65-75 (1990)

[4] B. Bert Boer and A. Bosselaers, “Collisions for the compression function of MD5”, Advances in Cryptology - Eurocrypt ‘93, pp. 293-304. Springer - Verlag, (1994)

[5] H. Dobbertin, “Cryptanalysis of MD5 Compress”, Presented at the rump session of Eurocrypt ‘96, May 14, (1996).

[6] Xiaoyun Wang, Dengguo Feng, Xuejia Lai and Hongbo Yu, “Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD”, Science & Communication, http://eprint.iacr.org/ 2004 /199.pdf, (2004).

[7] Ch. Rupa and P. S. Avadhani, “An Improved Method to Reduce the Occurrence of Collision Attack on Hash Function”, International Journal of Computer Science and Mathematical Applications, Vol 2, No 1-2, pp. 139-149. (2008).

[8] Ch. Rupa and P. S. Avadhani, “Message Encryption Scheme Using Cheating Text”, ITNG: Sixth International Conference on Information Technology: New Generations International Journal of Computer Science and Mathematical Applications, ISBN: 978-0-7695-3596-8/09(indexed by IEEE,dblp), pp. 470-475. IEEE, (2009).

[9] Kumar, S.: Public Key Cryptographic System using Mandelbrot Sets. In: IEEE Explore.

[10] Alia, M.A., Samsudin, A.B.: Generalized Scheme for Fractal Based Digital Signature (GFDS). IJCSNS International Journal of Computer Science and Network Security 7(7) (July 2007)

[11] Rubesh Anand, P.M., Bajpai, G., Bhaskar, V.: Real-Time Symmetric Cryptography using Quaternion Julia Set. International Journal of Computer Science and Network Security 9(3), pp. 20-26. (2009)

[12] Dr. Ch. Rupa, P. S. Avadhani, Information Security using Chains Matrix Multiplication, Advances in Intelligent and Soft Computing, Vol. 167, pp:703-712. Springer-CSIA, (2012)

[13] DV Popel, Sierpinski gaskets for logic functions representation Multiple-Valued Logic, ISMVL (2002).

[14] URL: http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/.

[15] Rubesh Anand, P.M., Bajpai, G., Bhaskar, V.: Real-Time Symmetric crypto graphy using Quaternion Julia Set. International Journal of Computer Science and Network Security 9(3), pp. 20-26. (2009).

[16] Christian Cachin, Jan Camenisch: “Encrypting Keys Securely”, IEEE Security & Privacy, pp: 66-69. IEEE, (2010).

[17] Sean O’Melia, Adam J. Elbirt “Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions”, IEEE Trans. VLSI Syst. 18(11), pp. 1505-1518. (2010)

[18] Yongge Wang and Yvo Desmedt ,”Perfectly Secure Message Transmission Revisited”, IEEE Transactions on Informaiton Theory, Vol. 54, No. 6, IEEE, pp 2582-2596. (2008)

[19] Steven M. Bellovin, et. al, “Risking Communications Security: Potential Hazards of the Protect America Act”, Elsevier, vol. 6 no. 1, pp. 24-33. (2008)

[20] Ch. Rupa, Sk. Rizwana et. Al, “Information security using Fractal sieve and MMD “, CCSIT Springer, 2013

[21] Aamer Nadeem et. Al, “A Perforamnce Comparision of Data Encryption Algorithms”, IEEE information and communication, pp. 84-89, 2005.

[22] Priya DHawan, “Performace Comparision: Security Design Choices”, Microsoft Developer Network, 2002, http://msdn2.mirosoft.com/en us/library/ms978415.aspx