International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-8, Issue-9S, July 2019

A New Method for Modifying Blowfish Algorithm for IoT

Shally Nagpal, Suneet Kumar, Suresh Chand Gupta

Abstract**:** ***Due to rapid development of internet and web applications, the prominence and the importance of the information exchange using the internet is growing. Communication through internet faces data safety as an important issue. Data has to be safe when communicating as slightly loss or danger to transmitted data can be responsible for excessive harm to the society. For network safety encryption plays a vibrant part. Many times it is little bit confusing to choose best encryption, as there are many cryptography methods for securing the data during transmission. For many applications Blowfish is currently assumed to be insecure. So it turns out to be essential to enhance this procedure through addition of different levels of safety so that it can be used in several reliable communication channels. Blowfish algorithm is modified in a way that it is platform independent; however the present encryption schemes are restricted to platform dependent proposal. This proposed modified blowfish algorithm supports text, images and media files.***

Index Terms**:** ***Network Security, Symmetric Block Cipher, Cell Automata, Internet of Things, Entropy.***

I. INTRODUCTION

The notation malicious hackers, from time to time called crackers, confer with persons who breakdown into PCs without authorization. Network Security (NS) has gained massive prominence inside the past few ages as it is the key element of net based totally protection mechanism and also with the rise of hand held Wi-Fi information appliances the capacity to perform protection function with confined computing resources has become more and more significant. In particular protection is needed against modern attacks that can be very dangerous [7]. Automation of attacks, privacy worries is some of the important traits of modern attacks.

A. Cryptography

Cryptography is the learning of undercover (crypto) script (graphy). Cryptography is the discipline or talent of covering the ideologies and techniques of reworking an understandable communication into implicit kind or incomprehensible kind and then remodeling the message returned to its authentic type. As the ground of cryptography has bigger past; cryptography these days is thought as the study of strategies and programs for securing the integrity and authenticity of transmit of statistics in hard situations. Cryptography encrypts data in one of this way that no one can study it, excepting the individual that holds the key. Greater advanced crypto techniques make certain that the data being communicated has not been altered in transit.

Blowfish can be efficiently used for encryption and protection of facts and it is a Symmetric Block Cipher (SBC). [8]. Blowfish is ideal for securing statistics, takes a variable key usually from 32-48 bits. Blowfish set of rules, iterating a simple encryption feature 16 instances. Blowfish designed in 1993 by Bruce Schneider as a firm, open alternate to present encryption set of rules [3].

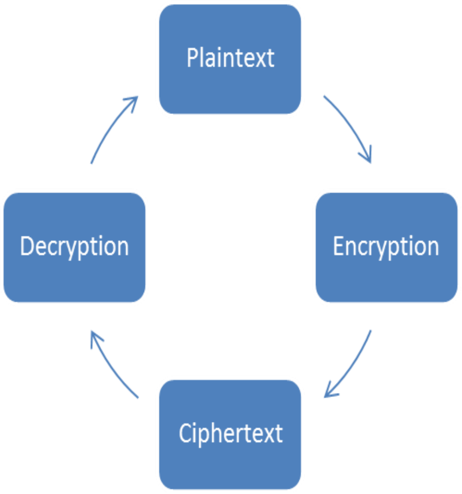


Figure 1: Conventional Encryption Model

II. RELATED WORK

Afaf M. Ali Al-Neaimi et al. [1] proposes a method which improves the execution of the blowfish set of rules. This is finished with the aid of constructing another structure for the sixteen adjusts within the first calculation by means of supplanting the interest with every other offered undertaking. This structure affects usage of numerous to discharge keys. The usual of cell automata (CA) is applied to create those special keys in a primary and compelling manner. The projected technique offers tremendous encryption, and the framework is extremely safe to endeavors of violation the cryptography key.

M. Anand Kumar et al. [2] this work chiefly center around two generally utilized symmetric encryption calculations, for example, Blowfish and Rejindael. These calculations are looked at and execution is assessed. Exploratory outcomes are given to show the execution of these calculations.

Sweta K. Parmar et al. [3] Different Cryptography systems can be utilized for protecting the data during communication, so it can make slight bit difficult to choose finest one. From the survey the blowfish calculation is discovered predominant than alternate calculations.

Christina L et al. [4] Different calculations and conventions are utilized to secure the information. The calculation productivity is estimated by completing time and output per unit time. Effectiveness of the calculation depends on key size; bigger key size may influence the effectiveness.

Revised Manuscript Received on July 02, 2019.

Shally Nagpal MMDU (Ambala)
Suneet Kumar MMEC ,Maharishi Markandeshwar**,**
Suresh Chand Gupta Panipat Institute Of Engineering And Technology

The program reproduction result gives the better execution and also security.

Manju Suresh et al. [5] starting with the idea of IoT, design and safety matters, this study divides different safety components for IoT and the criticalness of cryptography techniques for IoT. A proficient cryptographic calculation "Blowfish" is chosen in view of a few examinations. An alteration in Blowfish computation is introduced by changing its Function module 'F'. Encryption time and throughput examination of existing and changed blowfish calculation are considered for comparison.

Avinash M Ghorpade et al. [6] Cryptography expect a key part in the field of framework security. At the present time various encryption estimations are available to safe the data however these computations eat up package of figuring resources, for instance, battery and CPU time. This paper for the most part focuses on normally used symmetric encryption count (calculation) which is Blowfish computation (calculation). Test outcomes are given to outline the execution of this figuring.

III. PROPOSED WORK

A new design for boosting the safety of blowfish algorithm is proposed. This approach design will not contradict the safety of the unique algorithm via retaining all the mathematical criteria of blowfish continue to be unchanged. Various Other Issues Have Been Analyzed Such As Scalability I.E. Key Size And Block Size Variation Is Referred As Scalability, Encryption Ratio I.E. Measures Quantity Of Data That Is To Be Encrypted And Key Length Value I.E. It Plays A Dominant Part That Shows How Data Is Encrypted. There Are Various Motives Why One Would Need To Encrypt Facts In Software: To Make Assured That Documents Transferred To Common Storage (Microsd Card And So On.) Are Without Problems And Not Accessible To Others. If A Key Is Stored Along With The Encrypted Facts, Or While A Document Private To The Application, It Is Fairly Smooth To Extract It And Decrypt The Statistics. Customers Are Quite Familiar With Passwords, And Accordingly A Manner To Generate Sturdy Cryptographic Keys Based Totally On Humanly Achievable Passwords Is Wanted.

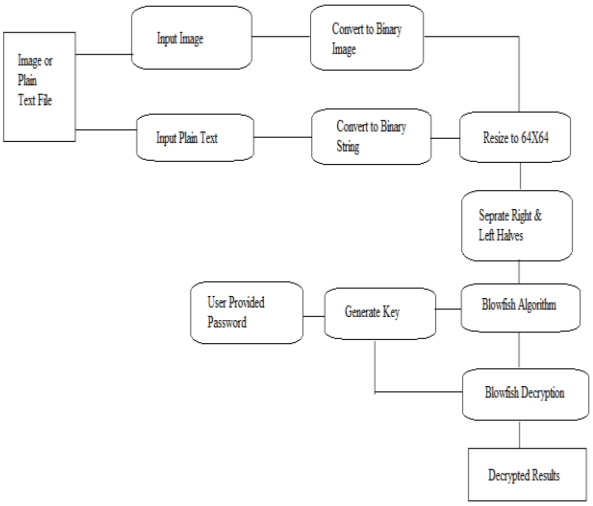


Figure 2: Proposed Encryption Scheme

IV. RESULTS AND DISCUSSION

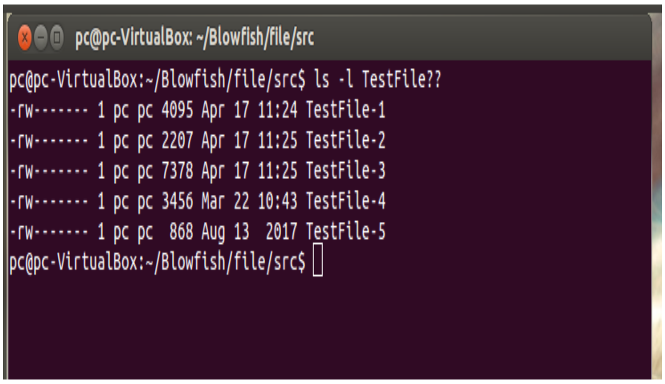
Evaluation Parameters

(a) Entropy

The entropy of a document is an index of its information content. The entropy is measured in bits per character. From the information theory point of view, the data in the current window can be viewed as a message source. To calculate the information content one examines the probability distribution of this source. It is assumed here that the individual messages (characters in the document / file) are stochastically independent of each other and are transmitted by the source with a uniform probability

(b) Encrypted/Decrypted File Size (KB)

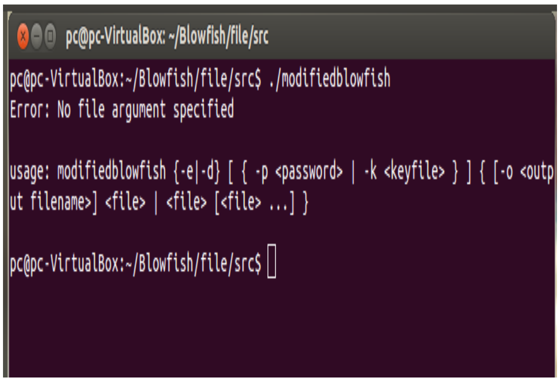
Size of Cipher text generated.



```
pc@pc-VirtualBox:~/Blowfish/file/src$ ls -l TestFile??
-rw------- 1 pc pc 4095 Apr 17 11:24 TestFile-1
-rw------- 1 pc pc 2207 Apr 17 11:25 TestFile-2
-rw------- 1 pc pc 7378 Apr 17 11:25 TestFile-3
-rw------- 1 pc pc 3456 Mar 22 10:43 TestFile-4
-rw------- 1 pc pc  868 Aug 13  2017 TestFile-5
pc@pc-VirtualBox:~/Blowfish/file/src$
```

Figure 3: Sample text files

Figure 3 shows the plaint text files used for encryption



```
pc@pc-VirtualBox:~/Blowfish/file/src$ ./modifiedblowfish
Error: No file argument specified

usage: modifiedblowfish {-e|-d} [ { -p <password> | -k <keyfile> } ] { [-o <outp
ut filename>] <file> | <file> [<file> ...] }

pc@pc-VirtualBox:~/Blowfish/file/src$
```

Figure 4: Modified Blowfish Encryption switches

Figure 4 shows the various switches and options available in modified blowfish algorithm.

Table I: Size and Entropy of Encrypted Files

Plain Text Files	Size (KB)	Encrypted Files	Size (KB)	Decrypted Files	Size (KB)
TestFile-1	4095	TestFile-1p	4388	TestFil-1n	4095
TestFile-2	2207	TestFile-2p	2500	TestFil-2n	2207
TestFile-3	7378	TestFile-3p	7684	TestFil-3n	7378
TestFile-4	3456	TestFile-4p	3748	TestFil-4n	3456

TestFile-5	868	TestFile-5p	1172	TestFil-5n	868

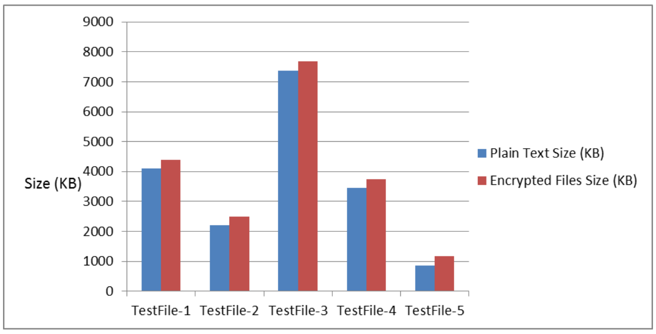


Figure 5: Plain text vs. Encrypted files size (kb)

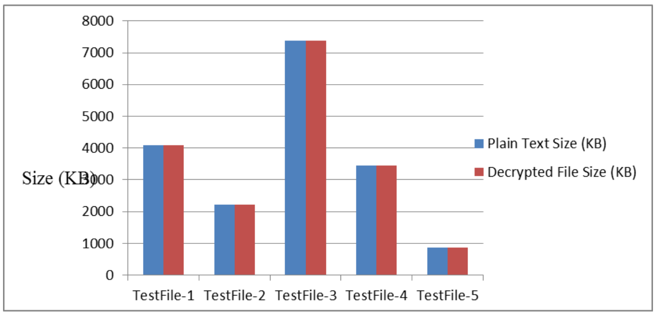


Figure 6: Plain text vs. Decrypted files size (kb)

As shown in table 1 and figure 6 size of plain text files and decrypted files come out to be same.

Verifying Hardness of Keys (Entropy)

Table 2: Entropy of Encrypted Files

Encrypted Files	Size (KB)	Entropy
TestFile-1p	4388	**7.86**
TestFile-2p	2500	**7.77**
TestFile-3p	7684	**7.93**
TestFile-4p	3748	**7.86**
TestFile-5p	1172	**7.41**

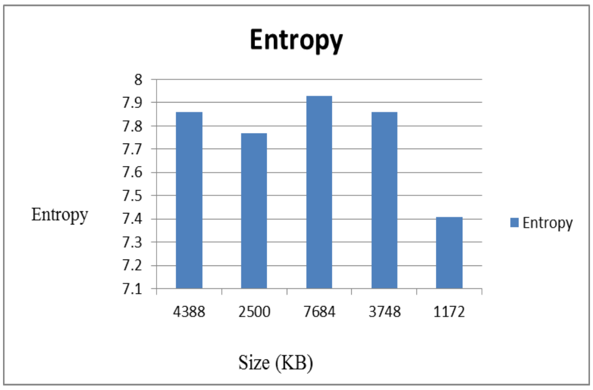
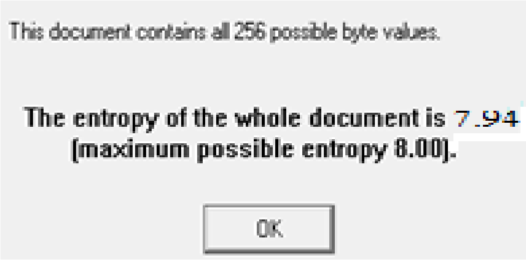


Figure 7: Entropy

As shown in table 2 and figure 7, entropy varies from 7.41 to 7.93



This document contains all 256 possible byte values.

The entropy of the whole document is 7.94 (maximum possible entropy 8.00).

Figure 8: Entropy of Modified Blowfish

Table III: Entropy of Encryption Algorithms

Encryption Algorithm	Entropy
DES	7.82
3-DES	7.81
AES	6.47
Modified Blowfish	7.94

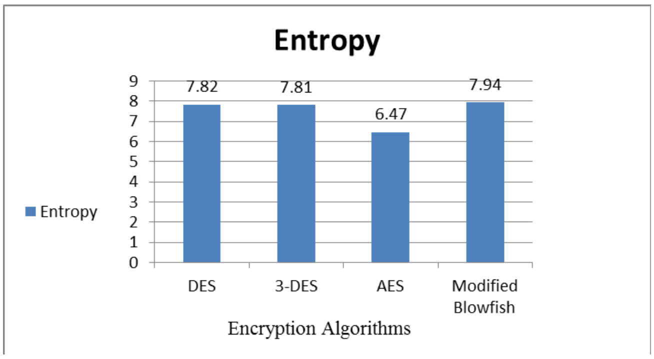


Figure 9: Encryption Algorithms

As shown in table 3 and figure 9, modified blowfish has higher entropy value as compared to existing encryption schemes.

V. CONCLUSION

Network safety has become significant issue for personal pc users, agencies, and the army. The net structure itself allowed for plenty security threats to arise. Many corporations use firewalls and encryption mechanisms for security from the net. The corporations build an "intranet" to stay attached to the net however protected from probable dangers. Information integrity is quite an difficulty in protection and to keep that integrity we tends to enhance as to provide the better encryption procedures for safety. Many of the current encryption schemes support only basic text formats. The existing simulation demonstrates the decryption and encryption is completed using modified blowfish procedure. Existing blowfish algorithm is improved to deliver more safety as shown by higher entropy compared to existing encryption algorithms, therefore nobody in between source and destination will hack the records. A comparative study of modified Blowfish and existing encryption Algorithms is achieved to offer a few measurements at the encryption and decryption. The efficiency of the updated blowfish algorithm is measured by hardness of the key. Blowfish is the finest as far as implementation time, memory utilization, control utilization, safety and accordingly appropriate for

IoT.

REFERENCES

[1] Afaf M. Ali Al-Neaimi, Rehab F. Hassan, ”New Approach for Modifying Blowfish Algorithm by Using Multiple Keys”, International Journal of Computer Science and Network Security, VOL.11 No.3, March 2011, pp.21-26.

[2] M. Anand Kumar and Dr.S.Karthikeyan, ”Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms”, I. J. Computer Network and Information Security, 2012, 2, pp.22-2.

[3] SWETA K. PARMAR, K.C. DAVE, ”IMPLEMENTATION OF DATA ENCRYPTION AND DECRYPTION ALGORITHM FOR INFORMATION SECURITY”, International Journal of Advances in Science Engineering and Technology, Volume- 1, Issue- 2, Oct-2013,pp.7-10.

[4] Christina L , Joe Irudayaraj V S, ”Optimized Blowfish Encryption Technique”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 7, July 2014, pp.5009-5015.

[5] Manju Suresh , Neema M, ”Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things”, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, 2016 ,pp.248 – 255.

[6] Avinash M Ghorpade, HarshavardhanTalwar, ”The Blowfish Algorithm Simplified”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, Issue 4, April 2016, pp.3343-3351.

[7] WenlongShen, Bo Yin, Yu Cheng, Xianghui Cao and Qing Li,” Privacy-Preserving Mobile Crowd Sensing for Big Data Applications”, IEEE ICC ,2017,pp.1-6.

[8] G. Manikandan, N. Sairam and M. Kamarasan, ”A New Approach for Improving Data Security using Iterative Blowfish Algorithm”, Research Journal of Applied Sciences, Engineering And Technology 4(6): pp. 603-607, 2012

AUTHORS PROFILE

Shally Nagpal is research scholar in CSE Deptt in MMDU (Ambala). She has completed her M.Tech from BPSMV Khanpur Kalan in year 2017. She has two years of educational expertise. She has completed his B.Tech from Maharishi Markandeshwar College Of Engineering MMDU(Ambala) In 2011.She has published three paper one in international journal ,one in international Conference and one in national conference. Her research area is security in Big Data.She has attended many workshops.

E-Mail id –shally.ngpl@gmail.com

Suneet Kumar obtained his Doctorate degree in computer science and engineering in 2012. He holdsMaster’s degree in computer science and engineering from Bhagwant university, Ajmer ,Rajasthan passed in 2006. His totalexperience is 16 year, presently, working as Associate Professor(CSE) in MMEC ,Maharishi Markandeshwar Deemed To Be University since Feb-2015. He has presented 5 papers in international /national conferences and published 17 paper in international journals. He has conducted various international ,national conferences,seminars and workshops also.

E-mail: suneetcit81@gmail.com

Suresh Chand Gupta obtained his Doctorate degree in computer science and application. He holds Master’s degree in computer science and engineering fromThapar university, Patiala ,Punjab passed in 2002. His totalexperience is 20 year, presently, working as Chairperson and Professor(CSE) in ,Panipat Institute Of Engineering And Technology since Nov-2016.He is author of two books. He has presented 17 papers in international /national conferences and published 24 paper in international journals.He is a CSI member and NBA convenor. He has conducted various international ,national conferences,seminars and workshops also.

E-mail: sureshgupta.cse@piet.co.in