IJCTA, 9(23), 2016, pp. 201-209
© International Science Press

Securing Password for Website using Blowfish Encryption and Decryption Technique with Struts2 Framework

Ankur Saxena* Neeraj Kaushik Nidhi Kaushik*** and Ankur Chaurasia******

Abstract : This exploration paper introduces a procedural way to deal with create Encryption and Decryption mechanism of Blowfish for securing secret word classification over the sites utilizing Struts2 system. The struts2 structure is utilized to create MVC based web application. A strut is an exquisite, extensible structure for making venture Java applications. Encryption may be characterized as the encoding of data in such a way, to the point that just a man with the correct information may decipher it. This application is exceptionally helpful and stringent and can be best used by the software experts and utilizes a basic system for key Era component. Final Encryption and decryption with Blowfish is finished by 2-tier framework. The coded information as letter sets, numbers, unique characters, legitimate administrators. We actualize our procedure in struts2 system.

Keywords : Encryption, Decryption, Web, Struts2, Framework, MVC, J2ee, Blowfish.

1. INTRODUCTION

Every person store huge amounts of data like emails, contacts, calendars, documents, photos and on the net. To cover and protect the privacy of online delicate data is another system. This requires that you know which computers will be attached to each other so that the key can be present on each one. It is same as a secret code that each of the computers must know in order to translate the information [1],[2].

Framework : The framework is intended to streamline the full improvement cycle, from building, to sending, to looking after applications .it can be considered as an arrangement of capacities helping the designers in making the applications[3], [4].

Struts 2: Struts 2 is the propelled rendition of Struts system. This new structure has re-invented the MVC system by incorporating to another structure known as Webwork. Few new elements are in the Struts 2 release. At the point when the Struts 1.0 was introduced, Struts was considered as the most famous web structures utilized by the Java designers and it streamlined the utilization of Model – Perspective – Controller (MVC) design by presenting the Activity classes and Action forms [5].

In this Figure1 user send the request (user name and password) to server through web browser and controller of struts2 encoded and decoded (Blowfish techniques) information and back to server through browser as a response.

Encryption: A practice of changing simple text into secret message text is called as Encryption. Encryption technique is used by cryptography to send secret messages through at mid channel. The encryption process requires two parts key and algorithm. [6]

* Amity University Uttar Pradesh Noida, India asaxena1@amity.edu

** Amity University Uttar Pradesh Noida, India nkaushik1@amity.edu

*** Amity University Uttar Pradesh Noida, India *nkaushik2@amity.edu*

**** Amity University Uttar Pradesh Noida, India achaurasia@amity.edu

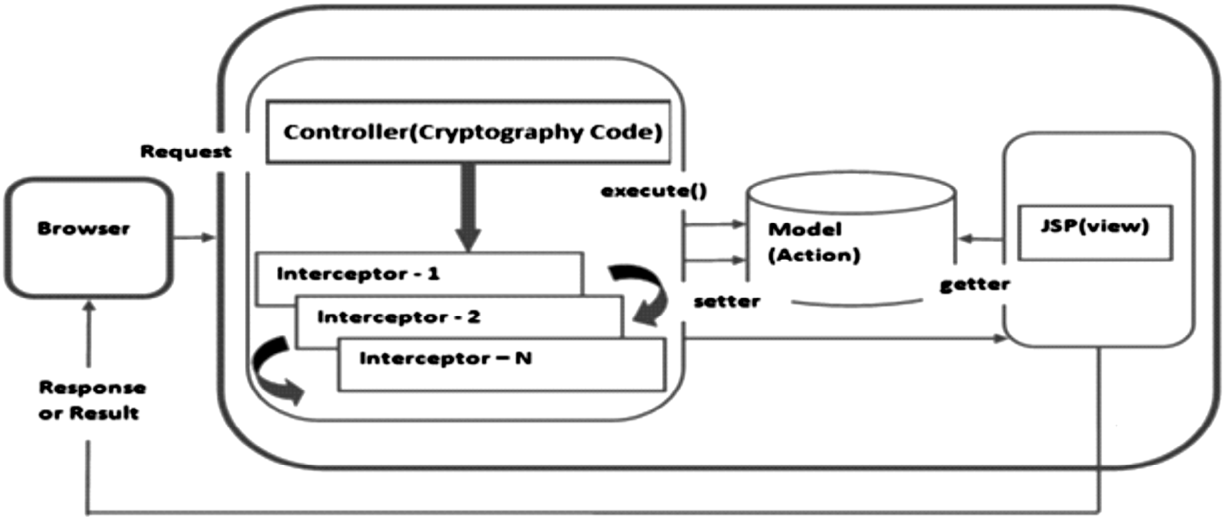


Fig. 1. Request and response scenario of login page with cryptography code in struts2.

Encryption = clear text + secret key +AES or DES algorithm = cipher text (encrypted text)[7]

Decryption: It is just an anti-pole process of encryption of Text [8].

Decryption = cipher text + secret key +AES or DES algorithm = clear text[9]

Here in figure 2 we deal with encrypting and decrypt ing of text string using cryptography API. The Encryption and Decryption is key and password based that is why it is referred as Password Based Encryption (PBE).

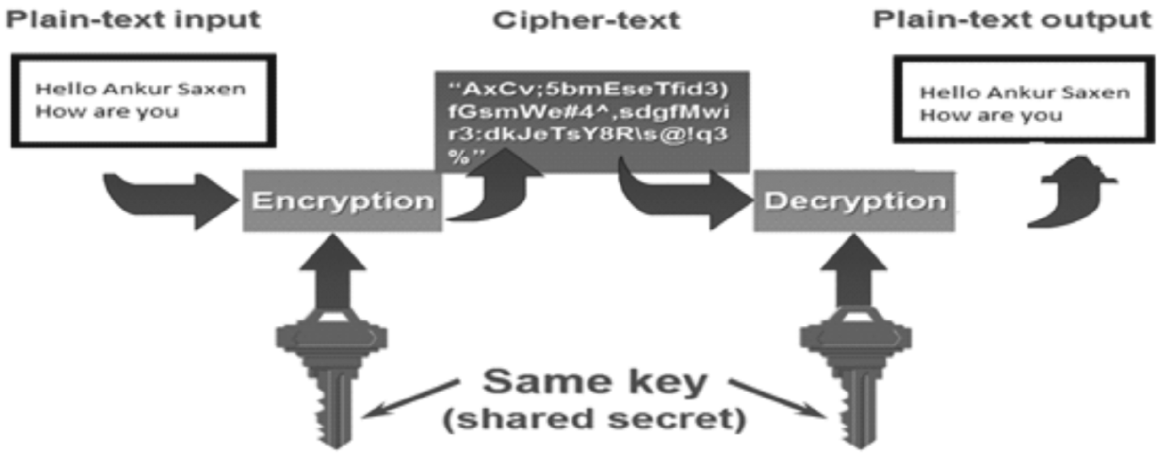


Fig. 2. Encryption and Decryption Mechanism with key.

2. BLOWFISH

Blowfish [10] is 64-bit encryption and decryption based technique for cryptography. It could be variable length of the key, it is based on symmetric block cipher mechanism and algorithm mainly has two parts: namely key expansion and a data- encryption. The key expansion can be used to convert a key of at most 448 bits into several sub key of array type, giving the result as 4168 bytes. The data encryption occurs by usage of Feistel network, which has 16 rounds based and each round is having three components: key dependent permutation, key and data-dependent substitution.

The measure of performance of Blow Fish cryptography schemes are based on several factors such as change in data types –such as. jpeg or .docx or .txt file, power consumption, increased or decreased packet size and change in key size for the selected cryptographic algorithms and techniques.

The Blowfish having considerably good performance compared to other algorithms. Order of performance could be shown like Blowfish > AES > DES.

This section of paper we have to discuss the time consumption of AES and Blowfish cryptography with the help of below table and chart and show better result with Blowfish.

Table 1. Time Consumption for Image (Encryption)

Image(JPEG)	*Time (Millisecond)*	
	Blowfish	*AES*
Image1	85	100
Image2	96	120
Image3	124	224
Image4	146	257
Image5	187	267
Image6	337	449
AvgTime	**162.5**	**236.16**
Throughput	**17.71**	**12.18**

Table 2. Time Consumption for Image (Decryption)

Image(JPEG)	*Time (Millisecond)*	
	Blowfish	*AES*
Image1	74	90
Image2	92	108
Image3	110	126
Image4	136	152
Image5	157	173
Image6	259	276
AvgTime	138	154.16
Throughput	20.85	18.66

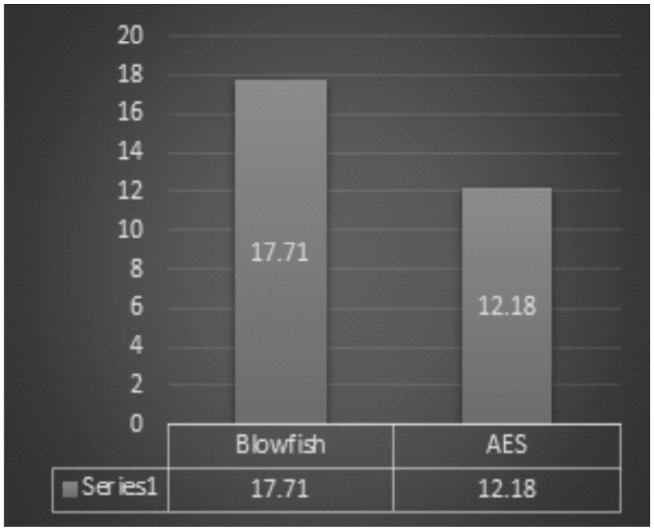


Fig. 3. Time consumption for image (Encryption).

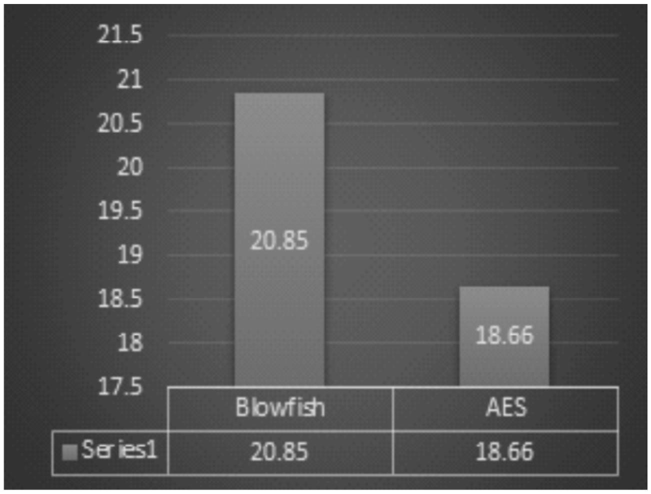


Fig. 4. Time consumption for image (Decryption).

Figure 3 shows the comparative time taken in milliseconds for encryption, Average time and throughput for respective images for both the algorithm. FIGURE 4 shows the comparative time taken in milliseconds for decryption, Average time and throughput for respective images for both the algorithm

3. REVIEW OF LITERATURE

The technical outcome from other quality research article to put more detailed view of the performance of comparison of AES, DES with famous Blowfish techniques and identified from [11], [12] that AES is significantly faster and efficient than their other symmetric techniques. With the transfer of data, symmetric key schemes have least difference in performance and most resources are used in data transfer than calculations. The Data transfer will surely benefit by AES usage if the encrypted data is stored at the other end and decrypted with multiple phases. So that the increase in key size by 64 bits of AES is directly proportional to energy consumption approximately 8% without any data transfer. The difference is negligible. Reduction in number of rounds is directly proportional to power savings but it makes AES insecure and hence should be avoided. Seven or more rounds are fairly secure and could be used to save energy efforts. The study [13] is conducted for different popular secret key algorithms such as DES, AES.

The post implementation of their performance was compared by encrypting input files of differing data types, contents and its sizes. The algorithm testing was done on two different hardware platforms, for comparing the performance status. P-II 266 MHz and P-4 2.4 GHz machines were used for this purpose. It is noticed that 3DES has almost 1/3 throughput of DES. In [14], [15] a study of security measure level has been proposed for a java programming language to analyze four popular Web browsers. This study consider of measuring the performances of encryption process at the programming language's script with the Web browsers. This is followed by conducting tests simulation in order to obtain the best encryption algorithm versus Web browser. Table 3 shows key size and block size of the AES and Blowfish Algorithm.

Default length = 210

Table 3. Key and Block Size

S.No.	*Algorithm*	*Key Size*	*Block Size*
1	Blowfish	426	42
2	AES	84	84
3	AES	126	84
4	AES	168	84
5	AES	210*	84

Table 4. Time consuption (Different key size)

Input		*Time (Millisecond)*	
Size(Kb)	*AES 128*	*AES 192*	*AES 256*
55	48	56	67
86	91	104	112
112	102	115	131
600	133	157	168
1000	202	248	271
1025	310	311	330
AvgTime	147.66	165.16	179.83
Throughput	19.49	17.42	16.004

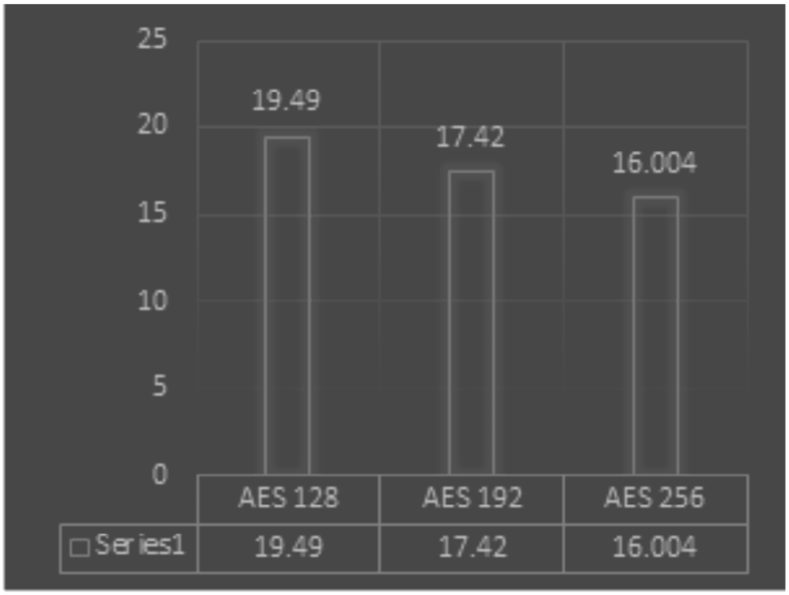


Fig. 5. Analysis with different key size of aes.

Figure 5 shows the comparative time taken in milliseconds for different key size in three variants of AES, Average time and throughput .

Table 5. Time Consumption (Base 64 Encoding)

Packet	*Packet Size*	*Time(Millisecond)*	
		Blowfish	*AES*
P1	1024.00 Kb	516 Ms	655 Ms
P2	1600.04 Kb	629 Ms	720 Ms
P3	2200.50 Kb	862 Ms	910 Ms
P4	2624.57 Kb	986 Ms	1020 Ms
P5	3225.31 Kb	1029 Ms	1286 Ms
P6	5200.50 Kb	1528 Ms	1598 Ms
P7	5665.25 Kb	1714 Ms	1643 Ms
P8	6144.00 Kb	1865 Ms	1868 Ms

Table 6. Time Consumption Hexa decimal encoding.

Packet	*Packet Size*	*Time(Millisecond)*	
		Blowfish	*AES*
P1	1024.00 Kb	516 Ms	655 Ms
P2	1600.04 Kb	629 Ms	720 Ms
P3	2200.50 Kb	862 Ms	910 Ms
P4	2624.57 Kb	986 Ms	1020 Ms
P5	3225.31 Kb	1029 Ms	1286 Ms
P6	5200.50 Kb	1528 Ms	1598 Ms
P7	5665.25 Kb	1714 Ms	1643 Ms
P8	6144.00 Kb	1865 Ms	1868 Ms

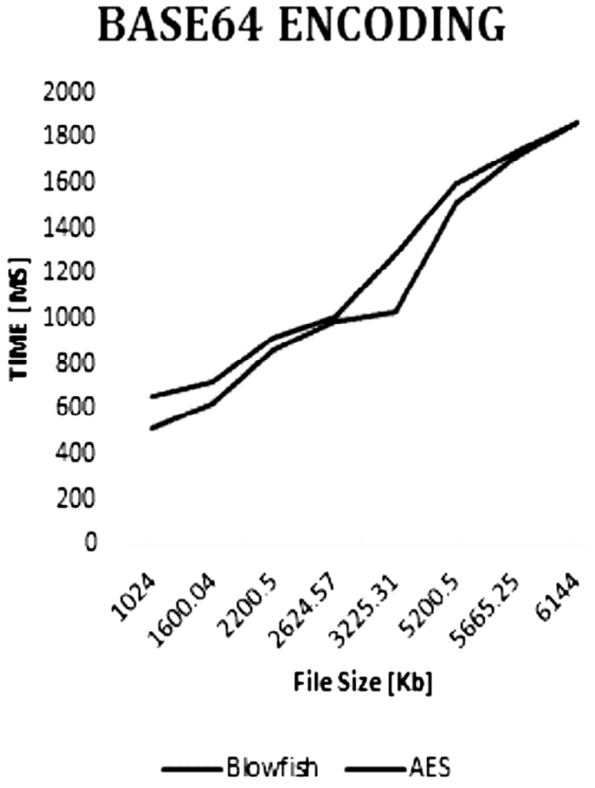


Fig. 6. Time consumption (Base 64 Encoding)

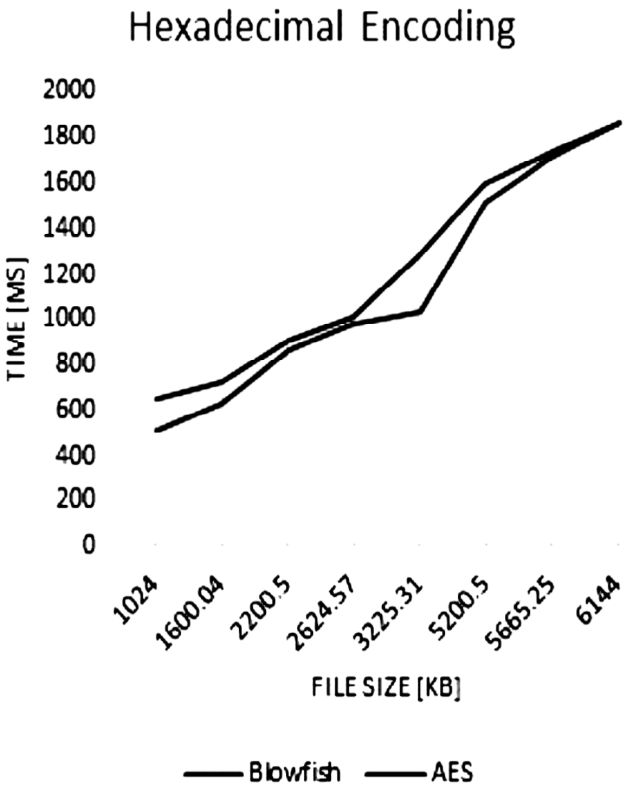


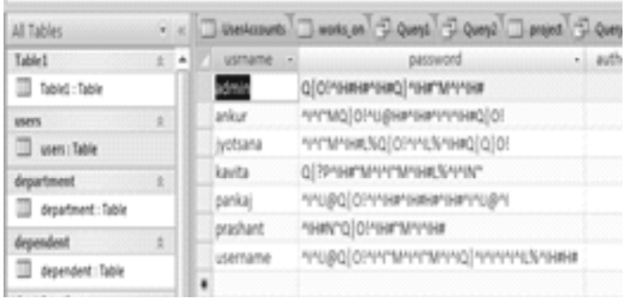
Fig. 7. Time consumption hexadecimal encoding.

Results of Base 64 and Hexadecimal encoding techniques employed for algorithms namely Blowfish and AES are given in Figure 6 and Figure7. It is identified that two methods almost gives the same result and hence no significant difference is there due to change in encoding methods.

4. METHODOLOGY

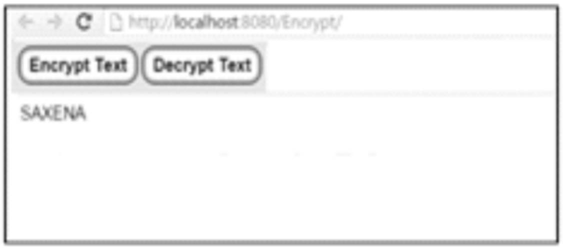
Encryption and Decryption model of Blowfish is executed with Tomcat 6 Server map by URL: http:\\localhost:8080. Tomcat is an open source tool developed by the Apache Software group. Tomcat implements and execute the Java Servlet and the JavaServerPages from Sun microsystems, and provides a “pure Java” HTTP server environment for Java program to run [16]. This in turn executes the Encrypt file which eventually runs Encrypt password which encrypts the user information, matches it with the stored data and hence validates the username and password in the Database.

This result of Blowfish cryptography can run on any webserver or application server like Tomcat 6 server .Figure8 shows the database interaction phase. If a user already registered with the website into his account, his password is encrypted and matched to the password stored in the any database (oracle, sql). If the information given by the user end is correct, then the user is permitted to move the next phase. If a user registers him for the first time in this page, then his password is encrypted and stored in the database (oracle,sql). Figure 9 show the normal text with database. Figure 10, 11 gives glimpse of how encrypted passwords are kept in database first tier and second tier. Figure 12, 13 gives glimpse of how decrypted passwords are kept in database. Figure 14 show the actual text in browser. In case a user forgets his Password then his password is decrypted and sent him back after getting a serial publication of security checks.



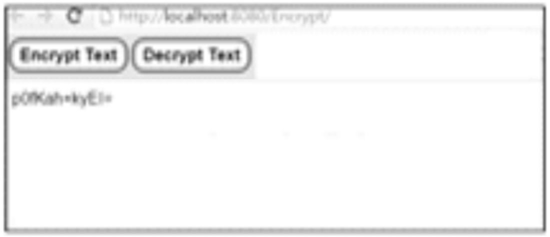
usrname	password
admin	Q[O!^lH#H#^lH#Q]^lH#^M^l^lH#
ankur	^l^l^MQ]O!^U@H#^lH#^l^l^lH#Q[O!
jyotsana	^l^l^M^lH#L%Q[O!^l^lL%^lH#Q[Q]O!
kavita	Q[?P^lH#^M^l^l^M^lH#L%^l^lN^
pankaj	^l^U@Q[O!^l^lH#^lH#H#^lH#^l^U@^l
prashant	^lH#N^Q]O!^lH#^M^l^lH#
username	^l^U@Q[O!^l^l^M^l^l^M^l^lQ]^l^l^l^lL%^lH#H#

Fig. 8. Fetch the data from the Data…ase



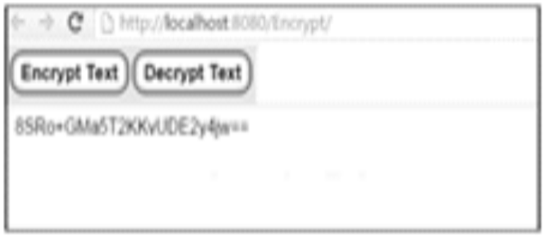
SAXENA

Fig. 9. Screen text



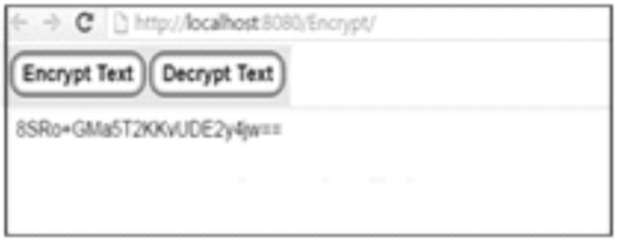
p0fKah+kyEI=

Fig. 10. Encryption with key1



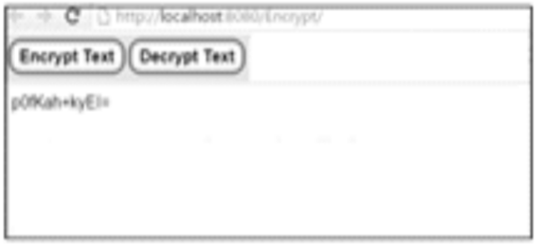
8SRo+GMa5T2KKvUDE2y4jw==

Fig. 11. Encryption with key2



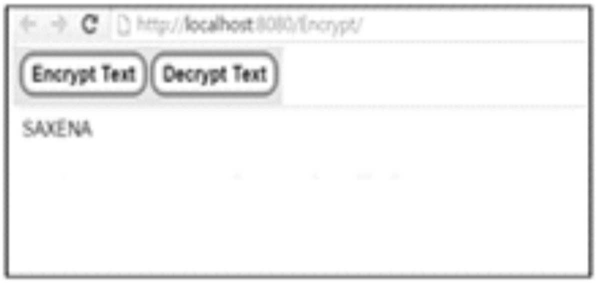
8SRo+GMa5T2KKvUDE2y4jw==

Fig. 12. Decryption with key1



p0fKah+kyEI=

Fig. 13. Decryption with key2



SAXENA

Fig. 14. Final Text show after final Decryption

5. RESULT AND DISCUSSION

Now we have to find out the advantage of Blowfish cryptography technique with Struts2 over the traditional cryptography AES. The average data rate is calculated for Blowfish and AES based on the recorded data. The

Formula used for calculating average data rate is

$$\text{Avg Time} \;=\; \frac{1}{\mathrm{N}b}\sum_{\mathrm{I}=1}^{\mathrm{N}b}\frac{\mathrm{Mi}}{ti}(\mathrm{K}b/s)$$

Where

AvgTime = Average Data Rate (Kb/s), Nb = Number of Messages,Mi = Message Size (Kb), Ti = Time taken to Encrypt Message Mi

With the help of below table and chart and show why Blowfish with struts2 results is better than AES.

Table 7. Time consumption (Encryption)

Input	***Time (Millisecond)***	
Size(Kb)	***Blowfish***	***AES***
55	48	56
86	91	104
112	102	115
600	133	157
1000	202	248
1025	310	311
AvgTime	147.66	165.16
Throughput	19.49	17.42

Table 8. Time consumption (Decryption)

Input	***Time (Millisecond)***	
Size(Kb)	***Blowfish***	***AES***
55	50	58
86	82	96
112	100	127
600	131	144
1000	220	257
1025	320	375
AvgTime	150.5	176.16
Throughput	19.12	16.33

FIGURE 15 shows the comparative time taken in milliseconds for encryption, Average time and throughput for respective input sizes for both the algorithm. FIGURE 16 shows the comparative time taken in milliseconds for decryption , Average time and throughput for respective input sizes for both the algorithm.

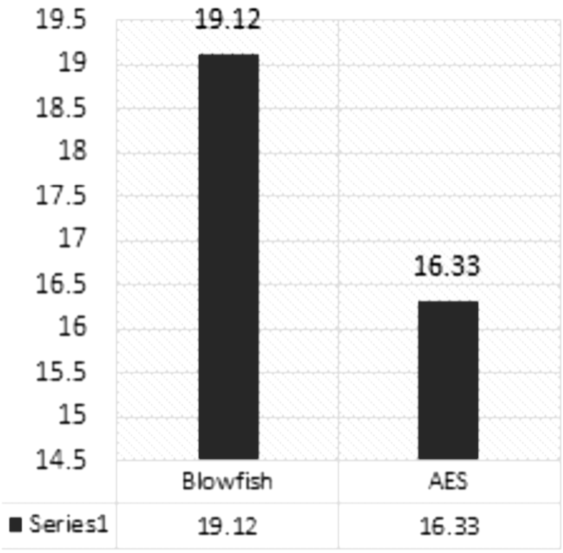


Fig. 15. Time consumption (Encryption)

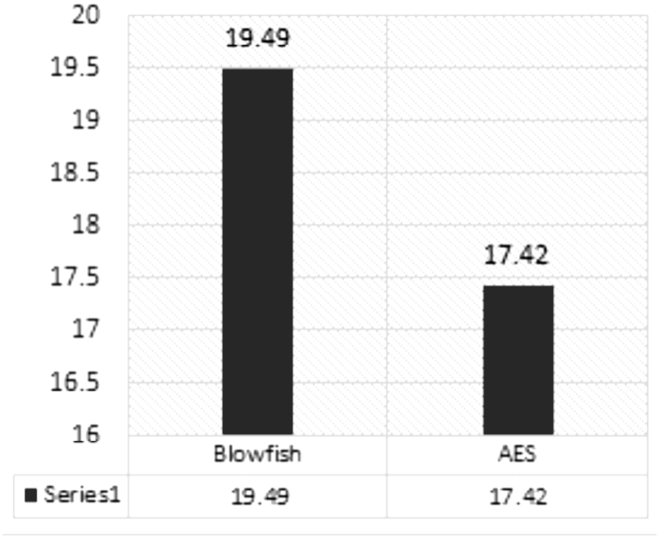


Fig. 16. Time consumption (Decryption)

6. CONCLUSION AND FUTURE WORK

This paper has proposed to take care of the password security issue in sites. The advanced architecture design of Struts2 with Blowfish techniques can effectively safeguard the business information. This is a straightforward web application which can be very useful for programming Experts. The encryption application created and depicted in this paper won't not be equivalent to other popular encryption algorithms however its accessibility demonstrates that devices can be produced that could satisfy the needs of an industry without depending on obtaining costly techniques from the business and development sector. A considerable measure of extension work can be done in this field with numerous other frameworks to augment the cryptography structural planning. Some industry experts also work Blowfish with integration of spring, struts and hibernate in future.

7. REFERENCES

1. Saxena A,Jakhmola R "Securing Confidential Data using Java/J2EE" International Journal of Science technology & Management Vol. 2 Issue 3, July 2011 (54-59).
2. Kumari J, Singh S, Saxena A" An Exception Monitoring Using Java" International Journal of Computer Science Trends and Technology (IJCST), Vol 3,Issue 2 2015,12-18
3. Sarkar D D, Jaiswal A , Saxena A "Understanding Architecture and Framework of J2EE using We… Application" International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1253-1257.
4. Saxena A, Chaurasia A " Key and Value Paired Data using Java Hash Ta…le" International Journal of Engineering and Management Research Volume-4, Issue-1, Fe…ruary-2014,81-89.
5. Saxena A"Web Based Custom Validation Using Framework in Java" International Journal of Computer Science Trends and Technology (IJCST), Vol 3,Issue 1 2015,90-96
6. Tham…iraja E, Ramesh G, Umarani R" A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012,226-233.
7. Mahajan P , A Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security" Glo…al Journal of Computer Science and Technology Network, We…& Security Volume 13 Issue 15 Version 1.0 Year 2013,15-22.
8. Agarwal V,Agarwal S, Deshmukh R" Analysis and Review of Encryption and Decryption for Secure Communication" International Journal of Scientific Engineering and Research (IJSER)Volume 2 Issue 2, Fe…ruary 2014,1-3;
9. Prashant G, DeepthiS&SandhyaRani.K. "A Novel Approach for Data Encryption Standard Algorithm". International Journal of Engineering and Advanced Technology (IJEAT) Volume-2, Issue-5, June 2013, pp. 264.
10. Tingyuan Nie Teng Zhang," A study of DES andBlowfish encryption algorithm, Tencon IEEE Conference,, 2009.
11. Chandramouli R, ''Battery power-aware encryption - ACM Transactions on Information and System Security (TISSEC)," Volume 9, Issue2, May. 2006.
12. Hirani S, ''Energy Consumption of EncryptionSchemes in Wireless Devices Thesis,'' university of Pittsburgh, April 9, 2003. Retrieved October 1, 2008,
13. Nadeem, A.; Javed, M.Y, "A Performance Comparison of Data Encryption Algorithms,"IEEE Information and Communication Technologies, 2005. ICICT 2005. First International Conference, 2006-02-27, PP. 84- 89.
14. S.Z.S. Idrus,S.A.Aljunid,S.M.Asi, ''Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008 ,PP 20-25.
15. Krishnamurthy G.N, Dr. V. Ramaswamy, Leela G.H and Ashalatha M.E," Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanche effect", International Journal of Computer Science and Network Security, 8(3), 2008.
16. Saxena A "HANDLING OF SYNCHRONIZED DATA USING JAVA/J2EE" International Journal of Management, IT and Engineering,Volume 1, Issue 7,182-194.