IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8411

Secure Message Transmission Using Base 64 Algorithm

Chandragandhi S[1] ,Sugadev S[2] , Sarath.C [3], Akshai Kannan [4] , Kamalesh M [5]

Department of Computer Science and Engineering,
JCT College of Engineering and Technology, Coimbatore, Tamilnadu, India[1-5]

Abstract: Web security is important to keeping hackers and cyber-thieves from accessing sensitive information. Without a proactive security strategy, businesses risk the spread and escalation of malware, attacks on other websites, networks, and other IT infrastructures. Injection and authentication flaws, XSS, insecure direct object references, security misconfiguration, sensitive data exposure, a lack of function-level authorization, CSRF, insecure components, and unfiltered redirects. In this Application the users has to select either want to send something by encrypting or wants to receive by decrypting. If it want to send them it have to select source file previously designed or type some message which is to encrypt and transfer.[1] Whereas on the receiver side again the receiver has to select the file which is to be received from the sender along with decryption key to decrypt the message. Decryption key randomly generate and send to the Receiver inbox. Every receiver has a inbox login and it use graphical password. After logged in receiver can view the decrypted key for open the data.

Keywords: Secure Message Transmission; Base 64; Online web Application; Encryption.

INTRODUCTION

The security of data in today's digital age is very important , steganography and cryptography can be used to secure data in the form of text messages, documents, images, audio and video. Pictures are the most widely used objects both offline and online and also some images are confidential and should not be publicized which is maybe a picture of research or just personal consumption.The internet is simply a large collection of networked .Man has grown to depend on the internet on A continual basis and have incorporated it into their lives.Due to this dependence upon the internet, terrorists have Made the internet a potential attack platform Security, as of now, is the techniques developed to Securely guard information and information systems Store on computers. Potential threats consist of the Destruction of computer hardware, software, theft, Unauthorized use, or disclosure of data.[2] Computer and The information they contain are often considered Confidential systems because their use is typically Restricted to a limited number of users. This Confidentiality can be exposed to danger in a variety of Ways. For example, data and information can be exposed By hackers, viruses and worms. Therefore, security can be Defined as the resistivity degree to, or protection from Harm. Security is one of the basic needs of man since Creation.The case between the first two children (Cain And Abel) of the first human creature, Adam attest to This. It is also a statement of fact that security dynamics Have evolved over the years [1].

Cryptography is an art and science of hiding messages To introduce secrecy in data and information security is Known as cryptography.[1] The word ‘cryptography’ was Derived by combining two Greek words, ‘Krypto’ which Means hidden and ‘graphene’ which means writing

PROBLEM ANALYSIS

Data security is a major issue which we are facing today in this digital world of communication .as we know that today hackers are almost at every corner in search of our useful data which can be hacked by them for their different purpose. So, a system or terminology must required to make that data safe forever by any means during communication. So introduce a web application for security. It gives the security by using Cryptography. In this application we mainly show’s that how to store the file with security using Encryption algorithms. The user will login to the application by giving a valid email id of whom the file security key must be sent. After successful login the user will upload the file the file will encrypt and stored in the given path and security key sent to given mail id.[8] The user will download the decrypted file by giving security key which is received in user mail id.

A.Description of the Proposed Algorithm(Base 64) :

Java provides a class Base64 to deal with encryption. You can encrypt and decrypt your data by using provided methods. You need to import java.util.[1]Base64 in your source file to use its methods. This class provides different encoders and decoders to encrypt information at each level. Base 64 is an encoding scheme that converts binary data into text format

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8411

so that encoded textual data can be easily transported over network un-corrupted and without any data loss String BasicBase64format= Base64. Base64 is used commonly in a number of applications including email via MIME, and storing complex data in XML.

Encode simple String into Basic Base 64 format

StringBasicBase64format=Base64.getEncoder().encodeToString("actualString".getBytes());

Explanation: In above code we called Base64.Encoder using getEncoder() and then get the encoded string by passing the byte value of actualString in encodeToString() method as parameter.

Decode Basic Base 64 format to String

byte[]actualByte=Base64.getDecoder().decode(encodedString);
String actualString= new String(actualByte);
Explanation: In above code we called Base64.Decoder using getDecoder() and then decoded the string passed in decode() method as parameter then convert return value to string.

RELATED WORK

Base 64 Algorithm

The first step is to take the three bytes (24bit) of binary data and split it into four numbers of six bits. Because the ASCII standard defines the use of seven bits, Base64 only uses 6 bits (corresponding to 2^6 = 64 characters) to ensure the encoded data is printable and none of the special characters available in ASCII are used. The algorithm's name Base64 comes from the use of these 64 ASCII characters.[1] The ASCII characters used for Base64 are the numbers 0-9, the alphabets 26 lowercase and 26 uppercase characters plus two extra characters '+' and '/'.

Base64 Encoding/Decoding Table															
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Q	R	S	T	U	V	W	X	Y	Z	a	b	c	d	e	f
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
w	x	y	z	0	1	2	3	4	5	6	7	8	9	+	/
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63

In our programs, we can simply define this table as a character array. For example in 'C' we will do:

```
/* ---- Base64 Encoding/Decoding Table --- */ char b64[] =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
```

Technically, there is a 65th character '=' in use, but more about it further down.
The ASCII conversion of 3-byte, 24-bit groups is repeated until the whole sequence of original data bytes is encoded. To ensure the encoded data can be properly printed and does not exceed any mail server's line length limit, newline characters are inserted to keep line lengths below 76 characters.
What happens when the last sequence of data bytes to encode is not exactly 3 bytes long? If the size of the original data in bytes is not a multiple of three, we might end up with only one or two remaining (8-bit) bytes. The solution is to add the missing bytes by using a byte value of '0' to create the final 3-byte group. Because these artificial trailing '0's cannot be encoded using the encoding table, we introduce a 65th character: '=' to represent '0'. Naturally, this character can only appear at the end of encoded data.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8411

Example

Let's say we want to convert three bytes 155, 162 and 233. The corresponding 24-bit stream is 100110111010001011101001.

```
155 -> 10011011
162 -> 10100010
233 -> 11101001
```

Splitting up these bits into 4 groups of 6bit creates the following 4 decimal values: 38, 58, 11 and 41.

```
100110 -> 38
111010 -> 58
001011 -> 11
101001 -> 41
```

Converting these into ASCII characters using the Base64 encoding table translates them into the ASCII sequence "m6Lp".

```
38 -> m
58 -> 6
11 -> L
41 -> p
```

METHODOLOGY AND ARCHITECTURE

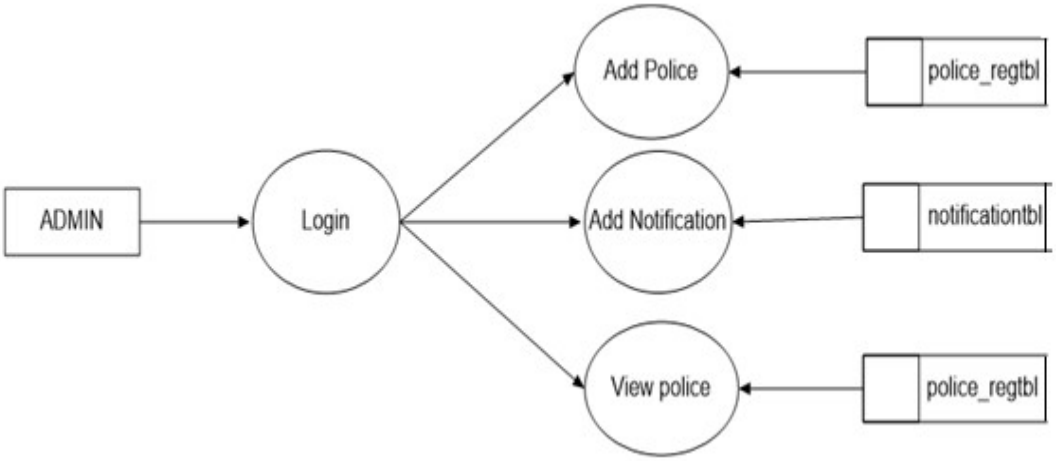
In the proposed system we are trying to automate the manual process. Here users can send and receive the records confidentially. Every receiver has a inbox login and it use graphical password. After logged in receiver can view the decrypted key for open the data.

This system contains 2 main modules based on the services provided. That are,

- Admin
- Police

Admin:

Admin can login by using username and password. Admin manage overall system. And he can add police officers and view their details .He can add all the notification. View the doctor .can view about the police details.



Police:

Police have logged on to the web application with username and password .when the admin add the police, an OTP will be sent to that police's email id .by using these OTP as a password to login . after the login, If he want to send some important files and he have to select source file previously designed and then transfer. the receiver can receive a message to his email id .after logging into the police web application, he has an inbox registration with a username and password,

IARJSET

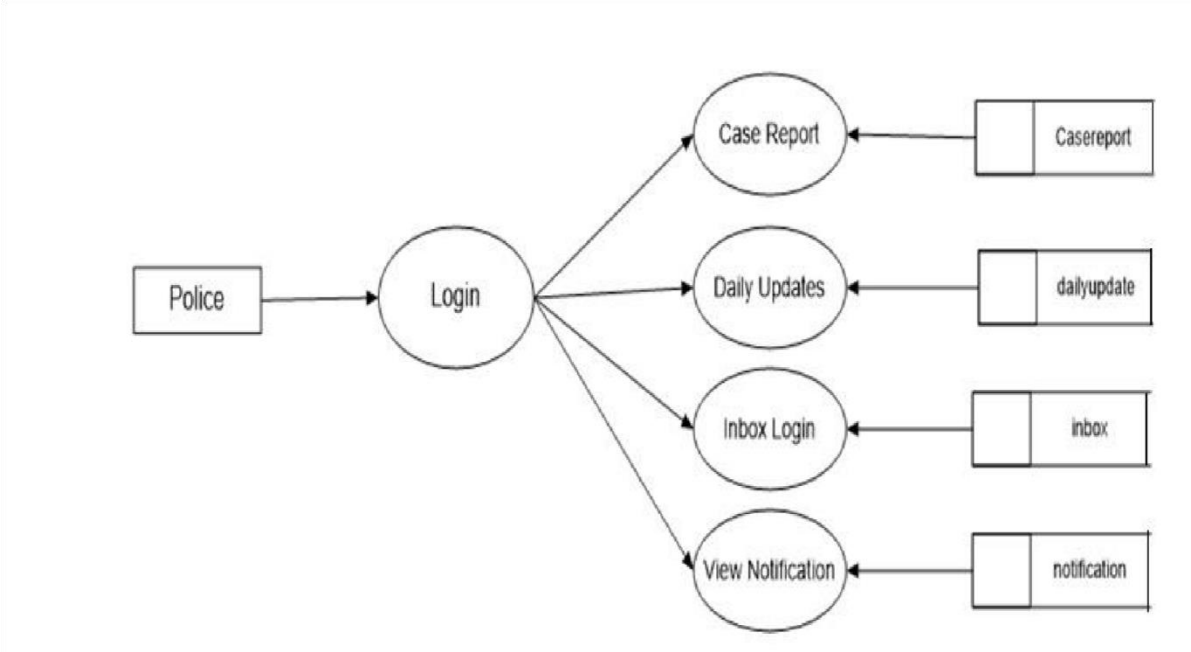
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8411

which is a color code that will be sent to his email id. that part is done by encryption .he has an inbox login to open his case report .with color code, username and encrypted. Copy paste that encrypted key and then click ok button then he can view his case report and to download.



CONCLUSION AND FUTURE WORK

This System helps the whole police departments to get the information safely. Because by using encryption algorithm it helps the department to provide an department way to encrypt and decrypt its data in a secure and controlled way **.** This will helps the police department to manage their record easily through encryption.[15]

Since this project is a web application ,in future ,We can develope the android application of this system by using high secured algorithm of cryptography. my project can do the cryptography by encrypting and decrypting data. dependent on other mailing system like gmail for information transfer.in future I can add the module so after encryption users can transfer information by the same software

REFERENCES

1. Logunleko, A.M., Logunleko K.B., Odufowora M.O, Gbolagade K.A, "A Differential Computational Encryption Modeling Technique on Textual Data", IJSR 2020
2. Pavan Kumar, Lingam Gajjela, Dr.N.Raghavendra Sai, "A Hybrid Hash-Stego for Secured Message Transmission Using Stegnography", ICRAEM 2020
3. R Rahim, R Ratnadewi, D Prayama, E Asri3 and D Satria "Base64, End of File and One Time Pad for Improvement Steganography Security", INCITEST 2018
4. Isnar S, Andysah P, Sumartono U , and Arpan. "Base64 Character Encoding and Decoding Modeling", IJSRCSE 2016
5. Himika Parmar, Nancy Nainan and Sumaiya Thaseen "Generation Of Secure One-Time Password Based On Image Authentication", CS&IT-CSCP 2012
6. R. Bhanot dan R. Hans, "A Review and Comparative Analysis of Various Encryption Algorithms," International Journal of Security and Its Applications, vol. 9, no. 4, pp. 289-306, 2015
7. Mastering Java Security (Cryptography, Algorithms & Architecture) by Rich Helton & Johennie Helton (Wiley/ Dream Tech)
8. M. Bellare, P. Rogaway, "Introduction to Modern Cryptography", 2005.
9. W. Stallings, "Introduction to Cryptography", 1996.
10. P. Nimbe, J.B. Hayfron-Acquah, B. A. Weyori, "An Improved Symmetric Cipher Encryption for Securing Data", Asian Journal of Mathematics and Computer Research, 2015.
11. Avi Kak (2017). AES: The Advanced Encryption Standard. In Computer Network and Security. . PurdueUniversity.
12. Geers Kenneth, (2011), Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence. CCD COE Publication. G. JULIUS CAESAR 2011, CrPaar, Christof, and Jan Pelzl. Understanding Cryptography. Springer, 2010.