Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

Analysis And Implementation of Encryption and Firewall in E-Commerce Website for Preventing Security Threats

Shikha Priya Choudhary
Department of Computer Science and Engineering
Amity University Jharkhand
Ranchi, India

Rohit Raj
Department of Computer Science and Engineering
Amity University Jharkhand
Ranchi, India

Abstract— **With worldwide retail e-commerce sales projected to increase several, e-commerce security violations attacks such as phishing attacks, spam emails, malware, DDOS attack, credit and debit card fraud are also increasing. About 76% of the worldwide e-commerce website have been affected by this.**
Cryptography has been emerging as one stop solution to prevent network security attacks. Encryption is also a part of cryptography which refers to the act of encoding data, in this context so that data can be securely transmitted via internet. Encryption can therefore be used to either to keep communication secret (defensively) or to identify people involved in communication (offensively).
Another major method that could be implemented is firewall which gives high level protection to the network. It is a system designed to prevent unauthorized access to or from a private network.

So, this research mainly focuses on how the use of encryption and firewall methods can prevent the security threat for a better user experience.

I. INTRODUCTION

With the growth of digitalization everything has shifted to online platform. From getting information on a topic, interacting with people online to shopping your essential goods, everything could be done by just few clicks from your device keyboard.
Nowadays people are more interested in shopping from online platform or E- commerce websites and this industry is flourishing without any plans to stop in near future.
According to E – commerce statistics, there are 2.14 billion online shoppers worldwide. Amid lockdown, there has been 50% increase in the number of online shoppers worldwide.

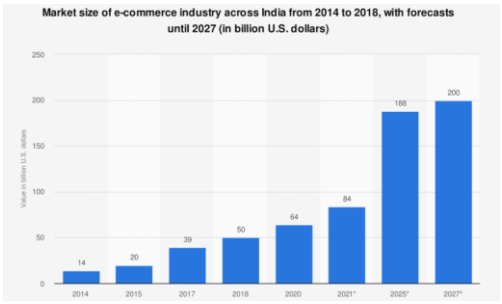

Figure-1

But there are many security threats that come with this online E – commerce websites. These security threats are so dangerous that it could bring severe loss to the company as well as to the online shoppers. The intruders or the black – hat hackers intrudes in between the network between the website and the users and they do all kinds of malicious activities and frauds.

II. LITERATURE REVIEW

We are living in the generation of discoveries and inventions. New trends and technologies are being created. It has been observed that during 2018 to 2019 there has been significant rise in online users. With online advancements things are getting easier and time saving. Most of the business institution from different sector is shifting towards online platform.
A sense of of security threat has been also created**.** ***(Raghavan and Parthiban, 2014)*** There have been significant rise in cases of security threats committed in e-commerce, credit card frauds such as phishing attacks, which is results into a sense of insecurity among users.
In simple words security threat is an attempt to corrupt or steal data. It is a risk which can strongly destroy the assets and can steal important information of organization**.** ***(Thomas Guillet , Rim Moalla , Ahmed Serhrouchni and Abdelatif Obaid)*** security of information and secrets stored in system of various organizations is becoming essential because large and different types of attack are occurring every day. Security is one of important challenge which is to be handled in the era of where all the platforms are becoming online. Current standards of security are not keeping the match with growing standards. Current era is the era of battle to be best;

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

every e-commerce websites want to protect their secret documents and strategy. Security has one of the most important issues faced by e-commerce website in online era ***(Duhigg 2003)***

III. TYPES OF SECURITY THREATS

1.Phishing attacks

→In this the intruder try to send deceptive emails or create a login page which looks exactly similar to the e – commerce page and tries to fetch personal login details. As per reports , it has been observed that 39.9% of the users become victim of this attack every year and their gateway of transaction details get hacked.

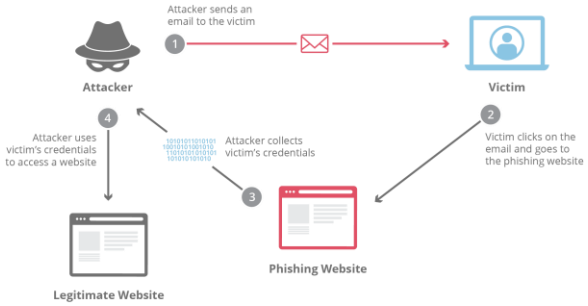

Figure-2

2.DDos(Distributed Denial of Services) attacks

→ In the type of attack , the intruder or the hacker tries to create huge fake traffic in the server of the site so that genuine user could not use the website. They create the fake traffic by using multiple computers. This attack makes the server impossible to make operations in the back – end. It also makes the website bad at user experience.

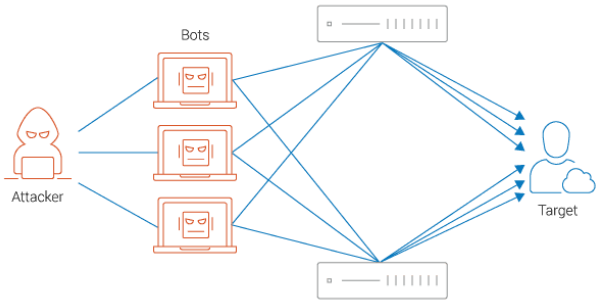

Figure-3

3. Use of Malware

→ Intruders or hackers sometimes execute malicious code on the server of the e- commerce website. Through this they get all the details of user as well as the revenue generated by the website.

All these attacks results in the huge loss of the revenue of these e- commerce websites. Once eBay database got hacked in which 145 million users' personal details were stolen.

Figure-4

IV. WAYS OF COMBATING E-COMMERCE WEBSITE

Though there are various ways to combat these e – commerce security threats but this research mainly focuses on two types which are as follows

1.ENCRYPTION

→It is a part of cryptography which refers to the part of encoding data so that data could be easily transmitted via internet. It basically changes the normal text into cipher texts. Every e- commerce website should implement encryption at various so that they don't suffer any kind of data breach. There are various ways of encryption such salting, peppering and hashing. For attacks like phishing attacks, SSL certification can be used.

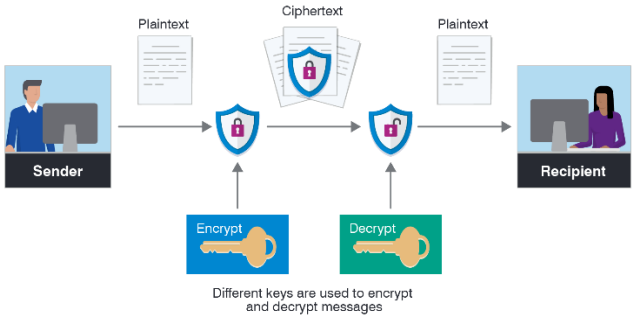

Figure-5

2.FIREWALL

→ It is actually a network security system that analyze and monitors the traffic in the e- commerce websites whether the traffic is of legitimate or genuine users or illegitimate users. For attacks like DDos attacks WAF(Website Application Firewall) could be used.

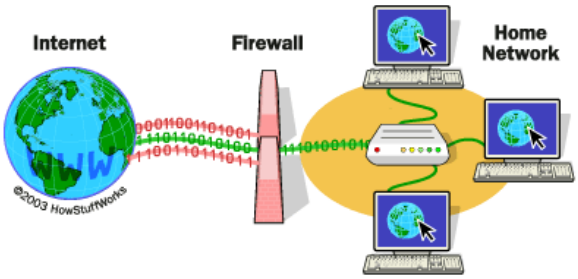

Figure-6

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

V. CASE STUDY OF HACKING OF ISRO AND NASA SATTELITE BY THE CHINESE HACKERS

→India has successfully launched many satellites in space. Every satellite has transponders fitted in it. The work of transponder is to take the data or message from the transmitted system and to respond to the data which is being transmitted to the required system. So the hackers from China tried to attack the data of the transmission system so that transponder could get the required data, henceforth resulting into complete satellite failure.

They failed in their planning as our Indian scientists have already encrypted both of the transmission system as well as the data collection dedicated system.

Similarly, NASA produced satellites also got hacked by the Chinese hackers and their satellites were under the control of Chinese hackers for few hours.

NASA also implemented encryption to their systems which were dedicated to different satellites.

In both of the cases encryption played a very important role for preventing these kinds of security attacks.

The major type encryption that is widely used is as follows ;-

→Hashing

→Salting(an advance version of hashing)

VI. TYPES OF ENCRYPTION

1.Hashing

Hashing changes your data into 40 digit code. Hashing works one way.

Hashing is also encrypted which is called cryptography. It takes one second to implement.

Disadvantages:-

→Every word generates the same 40 digit code every time.

→So, hackers have created Rambo table.

→Rambo table is like a dictionary. Dictionary contains meaning of every word, just like that Rambo table contain hash code of each and every word.

→To avoid this bottleneck of hacking we take following measures ;-

(i)Increase password length at least 14 digits

(ii)Increase password complexity , for eg ;- instead of writing car as your password, write carz123 so that no word could match from the Rambo table.

(iii)Don't login from too many devices

(iv)Don't login too many times in a single day

(v)To completely avoid the disadvantage of hashing , salting concept could be implemented .

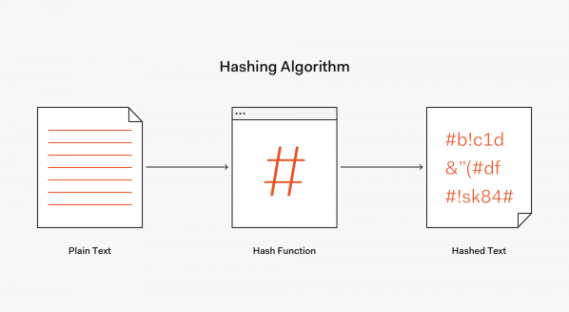

Figure-7

2.Salting

→Salting is actually an advance version of hashing.

→In salting , every time you enter a data , it will generate different 40 digit code.

For eg ;- you enter a data ''What'' ,salting will generate 234uxsdgahsgwg354.

Second time when you enter ''What'', salting will generate 6yutcnvhdjs456s.

So, every time you enter same data or password , it will generate different 40 digit code everytime.

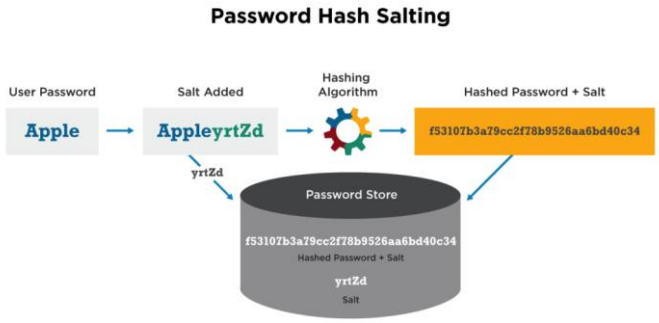

Figure-8

VII. HOW HACKERS FIND YOUR E-COMMERCE WEBSITES?

→E – commerce data hackers always search for data that is vulnerable or easy to target. The websites which uses common software like popular open source languages, shopping cart software or other code libraries. Hackers find high probability of finding vulnerability to the sites using above mentioned software. If hackers find vulnerability, they steal personal data of the user as well as of the company and take the sheer control of the website in their hands.

1.OPEN SOURCE ATTACKS

→This is considered to be one of the most common attack experienced by the e – commerce companies as the companies that use open source tool to build their application with open – sources tools like Magneto(off the self shopping cart used by many businesses) and Word Press (which has e – commerce capabilities and has a content management system).

This does not mean that company should avoid using these tools. Companies just have to be always updated on security patches.

Also be cautious when implementing third party plug ins.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

2.INPUT FIELD CODE INJECTION

→The input field is an area on the website forum that asks users about their sensitive information, this includes user name, phone number, date, credit card number, address etc.

Well this is not the only way but one of the important way to send data to the web server. When inputs aren't properly sanitized , the attackers may fetch out these sensitive data of the users. This is also results in the backend programming language to execute malicious code most of the times.

There are other ways also to breach data which includes Buffer overflow attacks(hackers use sneaky tricks of submitting large amount of unwanted data causing web server malfunction) , Error Message Reconnaissance(e commerce websites are loaded with error messages , hackers sometimes uses this message to gain valuable information hence resulting into successful data breaching).

VIII. WAYS OF COMBATING THESE TYPES OF ATTACKS

→For e commerce websites which are using these open sources to run their websites, they can implement the below mentioned precautionary measures: -

1.Sanitize the incoming data carefully which means to remove potentially dangerous characters and ensuring data has correct size and type constraints.

2.Avoid exposing vulnerabilities – this code of the websites should be reviewed time to time by the coders to avoid loopholes of the websites. Coders should alter the code immediately.

3. HTTPS and SSL certificates-This https protocol keeps the sensitive data of the users secure. It also boost up the ranking of your website on Google. It secures data transfer between the user devices and server and thus preventing any kind of interception.

4.Deploying firewall-Deploying firewalls keep away malicious intruders, SQL injections and other security threat attacks that are always continuing to hit headlines. Firewall actually helps in detecting whether the traffic is legitimate or not.

The best type of firewall which suits e – commerce website is Web Application Firewall.

5.WEB APPLICATION FIREWALL-It is a security solution to protect web applications and other internet applications . WAF can identify , filter and block illegitimate or malicious traffic from arriving in the e commerce websites. This is done while sending and receiving information using hyper text transfer protocol (HTTP) in the client server architecture.

It is mainly of 3 types ;-

- Network based WAF
- Host based WAF
- Cloud – based WAF (this being widely used by the modern organisation and enterprises).

IX. FIREWALL TECHNOLOGIES

There are many firewall available in the computer world but most reliable and widely used firewall is mentioned below ;-

1.Packet Filtering

→It is implemented on routers and filters on IP address which is a user defined content. They are application independent and checks packets at network layer. They deliver scalability and good performance but are easy to breach by the hackers because they are unable to understand the context of the given communication.

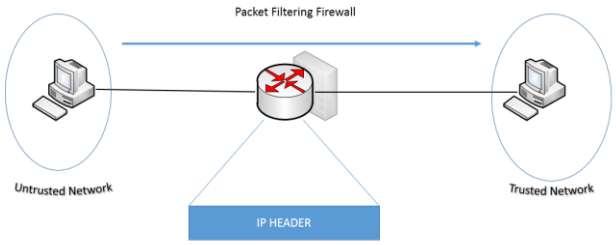

Figure-9

2.Multilayer firewall

→Generally, firewall protects a network from external malicious traffic and not from internal attack. So the concept of multilayer firewall is introduced within a network to protect it against internal attack. Though ,implementation of this idea is limited.

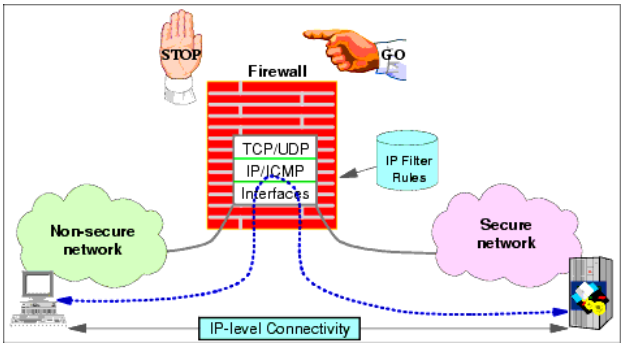

Figure-10

3.Stateful inspection firewall

→It overcomes the limitation of the application firewall and packet filters. With this firewall, the packet is stopped at the network layer and the INSPECT engine takes control of it. The INSPECT engine will extract the state related information for taking security related decisions from all application layer and maintains the information in dynamic state tables for evaluating subsequent connection attempt.

It offers high performance , scalability and highly secure solution.

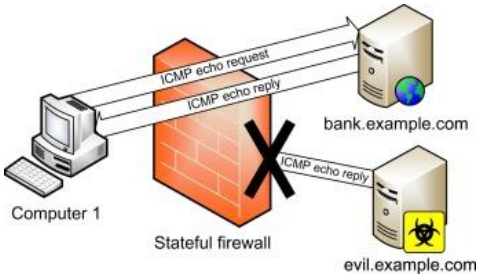

Figure-11

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

4.Application Layer Firewall

→It operates in user space at the application layer of the OSI model which controls traffic between directly connected networks.

This firewall has a dedicated alarm system to monitor the security of the firewall and it also responds to attempts to check the security of firewall.

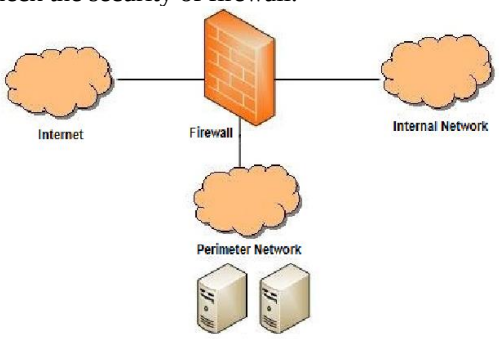

Figure-12

5.Authentication service of the firewall

→It is a service provided by the firewall. It provides a mechanism by which the identity of the user can be verified. This allows websites and other organisation to acclaim their security policies and restrict the access of the resources of the users.

X. JSH ALGORITHM

→JSH stands for Jumbling Salting Hashing.

In jumbling part, password undergoes three processes namely "Addition", "Selection" and ''Reverse''. Addition process generates a value required for determining the numbers of characters that has to be added to the password. Selection process is responsible for selecting characters from pre-defined character set that has to be added to the password. Reverse process deals with reverse the output of selection process.

Salting part deals addition of salt in jumbled password. Usually, selection of salt depends on timestamp value which is determined at the creation of account by the user. After this, the jumbled and salted password is given to hashing procedure where Secured Hash Algorithm (SHA – A predefined hashing algorithm) is implemented.

"Randomness in Security" is achieved by implementing this JSH algorithm.

→The algorithm for implementing JSH algorithm is given below.

//Random () is a pre defined method responsible for calling random value from pre defined set of objects.

// **Process array P [ ]**:

The process array will store the plain text password with randomly generated characters. This array is used for actual encryption process

This Process array will store

//**SaltarrayS[]:**

Salt array will be used to store time – stamp value from the users. In the mentioned case, user sign up time value is actually the timestamp value.

//**input:** plain text form password.

//**output:** Jumbled salted and hashed form of password will be generated.

INITIALIZE 'x'to0;

STORE length of plaintext form password in variable "x" as input;

CREATE a Process arrayP[ ], such that P[length=x];

STORE each character in array block;

//P{0,1,2...x-1) ={passwordofcharacters}

*1) /*Jumbling technique implementation*/*

Function for jumbling(P[])

{

2) //Addition process of jumbling technique implementation

A.

Label1: CALL Random() function;

//Random() function will return random value from pre defined set of integer value.

SET' 'l' as principle random value;

If(l>=x)

STORE random value generated by Random()function;

3) Else

Goto **Label 1** ;

break;

4) EndIf

B.

UPDATE the array P[] ofsize(x+1) as mentioned:

// the above array is called as "Process array"

Processarrayofsize(x+l)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

C.

DEFINE the set of characters C. Size(C) = V;

V = any large value;

C = {special characters ,operators, A…..Z, a….z,0…9};

//For a particular password entry , the character set should be different.

5)

6) //Selection Process of jumbling technique implementation

*7) /*This process is also randomized as this process is responsible for selecting characters from a given character set. All these symbols later on added withplain-textpassword.*/*

A.

CALL Random() function 'l' times;

// At each iteration, random value will be generated which will act as an index of the character in the character set.

/* for instance : character set C ={ 7,%,A,10,*,y,W,5,-, #, @,| }

CALL Random( )

Number generated:3

hence character selected : D*/

B.

FILL the Processarray with characters as mentioned below:

---

x(characters of the password)|l(selected characters)

C.

STORE the original length of an array(x+l) in variable 'FIX'

For i= 0 to (x+l-1)

While(l!=0)

SET j to0;

j= (FIX mod l);

Create 'temp' variable;

temp =P[j] ;

P[j]=P[i];

P[i]=temp;

//Index within the range 0 to (x+l – 1) would be output of above mentioned mod function. So, swap output index 0^{th} position.

l= l-1;

8) End While

9) End For

//Reverse process of jumbling implementation

A.

If(l mod 2==0)

Reverse the process array; // when l is even number

10) Else

Don't reverse the process array;//when l is odd number

RETURN (P); // Pass the process array to salting function

End If

}//jumbling function ended

*11) /*Salting technique implementation*/*

Function salting(P[])

{

A.

STORE Timestamp value of Sign-up process for each user;
OBTAIN the length of timestamp as 't';

CREATE Salt[size=t] array that will store random salt characters;

Salt[] ={characters obtained from Time stamp value};

UPDATE an array P of size (x +l + t) as shown:

process array becomes

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

process array of size(x+l+t)

B.

FILL process array with

Jumbled password of size(x +l)| Salt characters of size t

Return (P);// Pass process array to hashing function

12) *}//salting function ended*

/*Hashing Technique implementation*/

Function hashing (P [])

{

A.

The use of pre-defined SHA algorithm, for eg;- (SHA0,SHA1,SHA3 and SHA3) could be implemented in Hashing function

}//**hashing function ended**

XI. FIREWALL LIMITATION

→Configuration of firewall is a complex process when it comes to providing of maximum security possible.
Most of the firewall only blocks traffic that is coming from outside. There are possibilities that your own system is communicating with outside network without your knowledge.
Configuration of firewall is a costly process, so many small e commerce websites couldn't afford it.
The major issue users of the E commerce websites face is transactions fraud. As soon as the intruders hack the e commerce websites, the first thing they do is fetching of password. After knowing the password, they get all your details. So, it is very much needed that organisations should implement the encryption technique. After analyzing the case study of china attack on ISRO satellite, it is very much clear that hashing and salting could be a powerful weapon to avoid the intruders fetching password of the users of these e – commerce websites.

XII. SURVEY REPORT

→Survey was conducted by me from around 50 people from google forms as to know. The results of the survey are as follows:
(i)Receiving spam e-mails are very common among the users from e-commerce websites. People believe in those spam e-mails and they are cheated. From my survey 70% of the respondents got spam emails from e-commerce website.

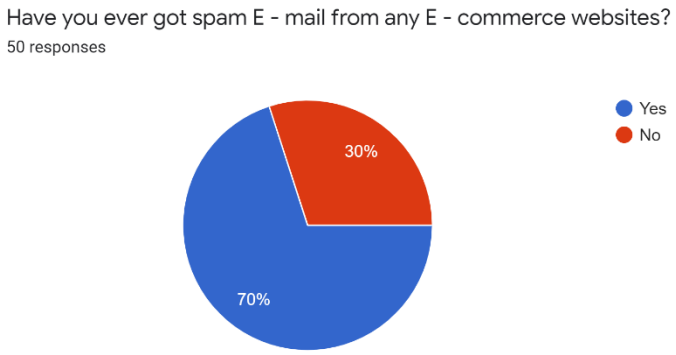

Figure-13

(ii) Many e-commerce websites make people aware of the financial fraud. According to survey 82 % of respondents agreed that they know about financial fraud through e-commerce website.

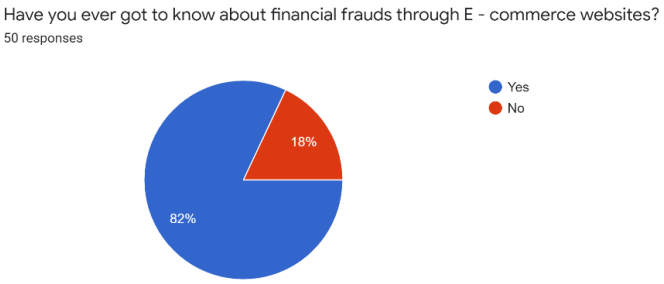

Figure-14

(iii)Whatsapp allows the featue of end-to-end encryption which that the content will only be shared between the sender and receiver, not third person have the rights to access that. Only 46% of the respondents are aware of end-to-end encryption of whatsapp video call.

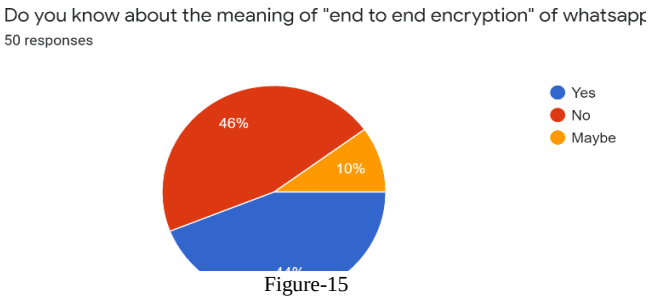

Figure-15

(iv) Maximum of the people use e-commerce website for their shopping. Many people feel safe to share their details and many not. According to the survey only 10% of the respondents feel safe to share their details.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

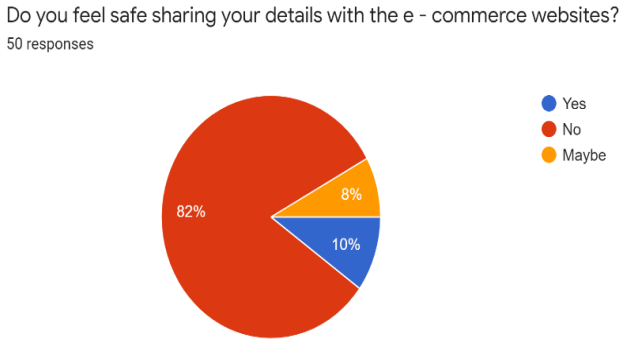

Figure-16

XIII. FUTURE SCOPE AND CONCLUSION

→Some more modifications need to be done on this algorithm in the upcoming future. Instead of Salting Hashing Algorithm (SHA), other alternative hashing techniques can also be used. E-commerce is the future of shopping more and more people are now shifting to online shopping from offline. E-commerce website is changing the business strategy, buying and selling things and also goods services are being provided from the pc itself.

Considering all these facts e-commerce websites should have a secure environment so that people do not need to worry about their security issues like stealing their personal data, financial fraud and access to their credit cards. Some new and advanced method should be used in firewall and encryption as to prevent security threats and also it should be updated with time to time as hackers find out some new ways to commit fraud.

After completing my research paper, I came to a conclusion that firewall and encryption can be used as to prevent security threats. E-commerce website is emerging, and more and more people are shifting to it but parallelly security threats are also becoming an issue. So, in my research paper I tried to implement JSH algorithm which makes the encryption strong, and the method of hashing, jumbling and salting are together applied as to make the website more secure to the users.

I also learnt about many technologies in my research paper. There were many limitations of encryption and firewall which I have mentioned in my paper.

REFERENCES

[1] Churi, Prathamesh & Kalelkar, Medha & Save, Bhavin. (2014). JSH Algorithm: A Password Encryption Technique using Jumbling-Salting-Hashing. International Journal of Computer Applications. 92. 10.5120/15982-4900.

[2] B., Patel & Patel, Ravi & Patel, Amit. (2011). To study the Risk or Issues of Firewall: Solution with different approach.

[3] Bali, Udit & Udgata, Mr & Churi, Prathamesh. (2018). Symmetric Jumbling-Salting Encryption Algorithm for Files. 82-86. 10.1109/CTIT.2018.8649503

[4] Agrawal, Ekta & Pal, Parashu. (2017). A Secure and Fast Approach for Encryption and Decryption of Message Communication. International Journal of Engineering Science and Computing. 7. 5.

[5] Abie, Habtamu. (2000). An Overview of Firewall Technologies.