CHAPTER 4

Preventing Session Hijack attacks in Web Applications using Strong and Encrypted Session ID

4.1 INTRODUCTION

The need for using the web applications are increasing in the current scenario. Verification of web users and various access control policies are inadequately secured in web applications. Web applications are vulnerable to Man-in-the-Middle attacks, changing the network packet content and seizing the session of a web application.

A secure framework or architecture is required to access the web applications safely. Current web applications are using the concept of session between the client and server. Third party users or hackers or attackers can sniff the web application session and take over the web session using the session hijack attacks. The best way to protect the web users from the session hijack attack is to encrypt the application layer web session between the client and server.

4.2 SESSION

In computer networking, session is defined as the information or data exchange between the user and web server.

4.2.1 WEB SESSION

The different types of web session are as follows,

(i) TCP session
(ii) Remote session
(iii) HTTP session

4.2.2 SESSION ID

Web site pages do not have memory. A client set from one web page to a different web page will be dealt with by the website as a totally new guest. In order to manage the session, the web server assigns the different session ID to each and every user. Whenever the user visit one web page and select the few things, the session recalls the user's identity.

4.3 DRAWBACKS OF PLAIN TEXT SESSION ID

Current web applications are using the plain text session ID. The attackers can use the network sniffing tools such as wireshark, Snort to capture the session ID. The drawbacks of the plain text session ID are as follows

(i) No of characters of session ID is 30 characters
(ii) Session ID is not encrypted
(iii) Network Sniffing attack is possible
(iv) Session Hijack attack is possible

4.4 ENCRYPTION

Process of converting the plain text to cipher text is called as Encryption.

4.4.1 NEED FOR ENCRYPTION

Due to the increased number of hackers or attackers over the internet, it is necessary to use the encryption techniques in the current web applications to ensure the maximum security.

4.4.2 ADVANTAGES OF ENCRYPTED SESSION ID

If the web applications use the encrypted session ID, then most of the threats and vulnerabilities can be prevented especially session hijack attacks.

The advantages of encrypted Session ID are as follows

(i) No of characters of session ID is up to 212 characters
(ii) Session ID is encrypted
(iii) Network Sniffing attack is not at all possible
(iv) Session Hijack attack can be prevented.

4.5 ARCHITECTURE OF ENCRYPTED SESSION ID TO PREVENT SESSION HIJACK ATTACK

To prevent the hijacking of the web application session by the attackers encrypted session ID is proposed.

4.5.1 ARCHITECTURE OF ENCRYPTED SESSION ID

The following Fig.4.1 illustrates the architecture of the encrypted session ID generation to prevent the session hijack attacks in web applications. Session ID of necessary number of characters are generated using plain Session ID generation algorithm.

The server encrypts the generated plain text session ID and the client decrypts the encrypted session ID using the Secret Key Sharing (SKS) algorithm. When the server sends the encrypted session ID to the client, attacks are executed to capture the session ID. When the client is receiving the encrypted session ID, the following attacks are executed to capture the session ID

(i) Packet Sniffing
(ii) Man-in-the-Middle attack
(iii) Cross Site Scripting

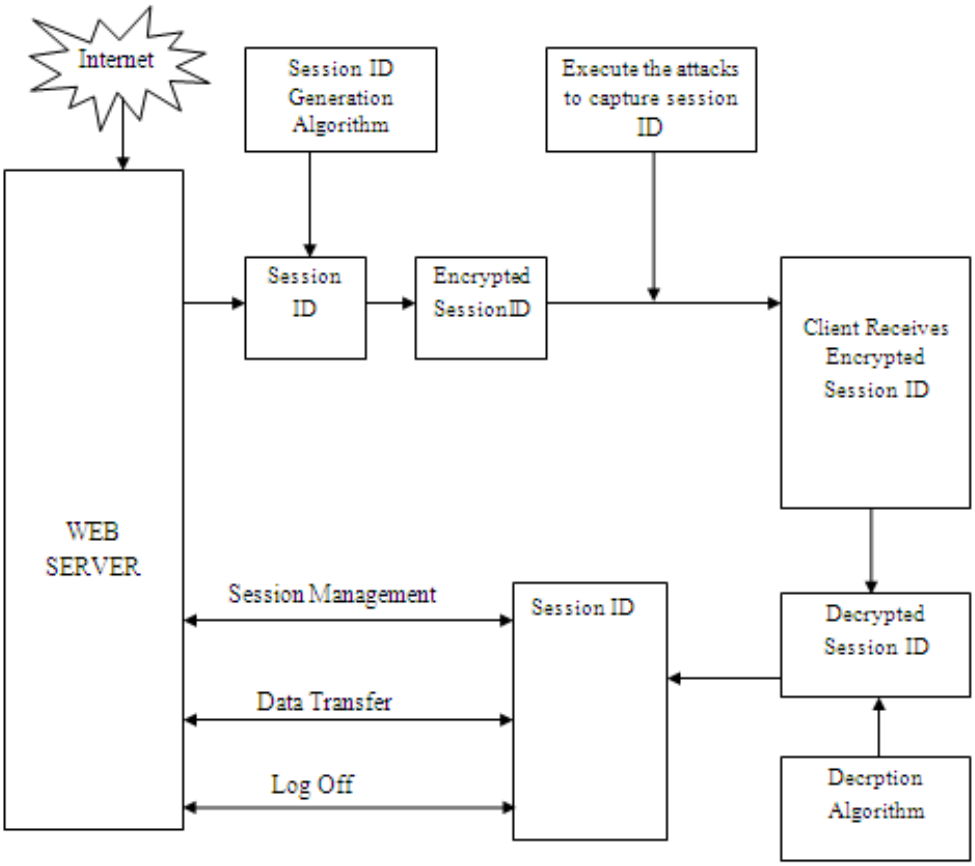

Fig.4.1 Proposed Encrypted Session ID Architecture

4.5.2 PLAIN TEXT SESSION ID GENERATION

The web server generates the normal session ID using the following algorithm. Session ID is generated using Java HTTP session.

```
Generate SessionID( )
 {
    oldid =  generate SessionId( );
    return sessionId;
 }
```

4.5.3 ENCRYPTED SESSION ID GENERATION

Both client and the server use the secret key generated by the secret key sharing algorithm to communicate between them. The same secret key to be used for encryption of session ID and decryption of session ID.

Variables

oldid =simple session id generated in step one
secret key= key established in the phase of secret key sharing

Algorithm : Encrypted Session ID generation

```
Input        : plain text session ID
Output       : encrypted session ID
generate SessionID ( )
          {
            oldid = generateSessionID( );
            Cipher cipher = Cipher.getInstance("AES/ECB/NoPadding");
            cipher.init(Cipher.ENCRYPT_MODE, Secretkey);
             return sessionId;
          }
```

4.6 SECURE COMMUNICATION OF A SESSION

Encrypted session ID is assigned to the client whenever the client log in to the session.

4.6.1 SECURED DATA EXCHANGE

Before establishing any session, the client and server need to share secrete key. This shared secrete key is used for encrypted communication.

4.6.2 SECRET KEY SHARING ALGORITHM

Both the client and the server have to share the secret key before the data transfer. Client's password is encrypted to obtain the cipher text.

Algorithm : Secret Key Sharing

Input : user's login credentials

Output : Secret Key

(i) Client ⟶ create (login, pwd)

(ii) $Request_{client}$ ⟶ $RSA_{public\ key}$ (server)

(iii) $Server_{public\ key}$ ⟶ client

(iv) RSA encryption at client side

C = E (PUs , pwd) where C= encrypted password

(v) Client sends(C) to server

(vi) RSA decryption at server side

P = D (C,PUs,pwd)

(vii) AES algorithm (server)

(viii)

(viii) Check(client = legitimate)

{

$Server_{pwd}$ ⟶ client

Client ⟶ decrypt (pwd)

if (pwd= match)

then

session= continue;

else

session = terminate;

}

The Fig.4.2 shows the diagrammatic steps involved in the Secret Key Sharing algorithm

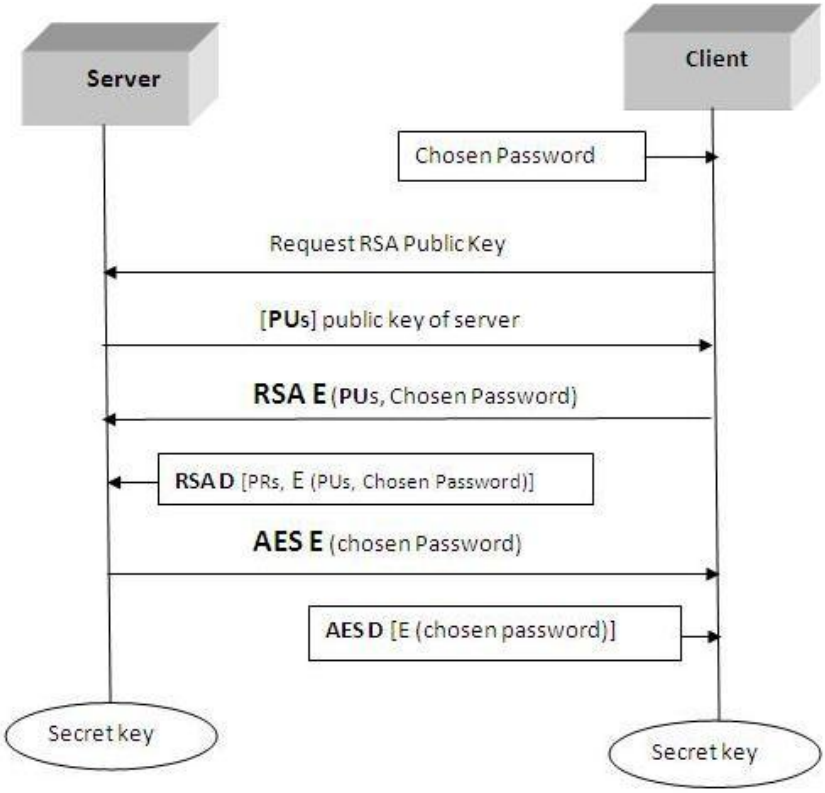

Fig.4.2 Secret Key Sharing algorithm

4.7 ENCRYPTED SESSION ID GENERATION USING SKS ALGORITHM

In order to test the integrity of the session ID , encrypted session ID is generated of various lengths such as 32 characters, 92 characters and 212 characters in three different cases are selected on random basis using secret key sharing algorithm. The criteria for selecting the length of session ID is as follows

(i) The range of the session ID is from 30 to 250 characters.

(ii) Currently used session ID length is 30- 32 characters.

(iii) Minimum of 212 character session ID is required to overcome all the web application attacks.

(iv) Protecting the integrity of the Session ID

(v) Using the server supplied Session ID to the client.

(vi) Assign the Encrypted Session ID to the client.

4.7.1 ENCRYPTED SESSION ID GENRATION FOR N CHARACTERS

(i) generate session ID = n characters

where n = 32 ,92, 212 number of characters

(ii) SID_{new} ⟵ Encrypt { $SID_{n\ chars}$}

(iii) Client receives the encrypted session ID

(iv)while client receiving SID_{new}

do

capture session ID ( )

execute packet sniffing attack ( )

execute man-in the middle attack ( )

execute brute force attack ( )

end

(v)$SID_{attacked}$ ⟵ number of session IDs hijacked

(vi)$SID_{prevented}$ ⟵ number of session IDs not hijacked

(vii)SID⟵ decrypt(SID_{new})

For the first case, 32 number of characters encrypted session ID is generated. Whenever the client is receiving the 32 character encrypted session ID, attacks are executed to capture the session ID.

4.7.2 EXECUTION OF ATTACKS

During the web application session between the client and server, packet sniffing attack and man-in-the-middle attacks are executed to capture the session ID.

4.7.2.1 PACKET SNIFFING ATTACK

Wireshark application is used to capture the network packets. During the data transfer between the client and server, Wireshark is executed to capture the contents of network packets such as Port number, IP address, Acknowledgement number, sequence number , Payload and the Session attributes such as Session ID and etc..10, 20, 30 number of web application sessions are created. The number of session IDs captured for 10,20 and 30 sessions are recorded.

4.7.2.2 MAN-IN-THE-MIDDLE ATTACK

During the data transfer between the client and server, the mitmproxy application is used to capture the https traffic of a web application session. 10, 20, 30 number of web application sessions are created and mitmproxy is executed. The number of session IDs captured for 10,20 and 30 sessions are recorded.

4.7.2.3 BRUTE FORCE ATTACK

Different possibilities of encrypted session IDs are generated.

4.8 EXPERIMENTAL SETUP

In order to test the proposed encrypted session using Secret Key Sharing (SKS) algorithm, the sample web application www.nationalrailways.com is designed using Java and Apache Tomcat Server. The client is authenticated by the user login credentials such as user name and password. The client is log in to the web server by establishing the web

session with the server. The server assigns the unique encrypted session ID for each time the client logs in to the server.

4.9 EXPERIMENTAL RESULTS

RSA keys are used in encrypting and decrypting the session ID for the 3 different lengths of the session ID such as 32 characters, 92 characters and 212 characters. For example, each time the values of p,q,n,e,d will be changing. The sample values of p,q,n, e, d of one web application session are given below

The values of p and q are chosen randomly

'p'=>

'133125582549961745599169700863629452446216655565329677958818749503
007431630337423661240129102196594278989483276005259649883259288825 4
798442542303336323950 7'

'q'=>

'123476827114853284795575770325752207511106752998046692826847985680
819714062893000689159575591058916066782134213417962104069319370099 3
921267333768307465715 9'

The value of n is calculated using n= p * q

'n' =>

'164379245410857557641543769408676439267473563141667230709748498167
801774396077697951590761314957322298258693612001197190127717413680 9
817110354475849190188076037177669565853251499106245859103546661723 7
846367360829245584727983512748729210079037973219089363393806111679 7
523645882456878244862202061503957629180613',

The value of e is chosen

'**e**' => '65537',

'**d**'=>

'63677926705385532957009219490478316677947095854870495342464483749395783273076591781665108995897531142838270189686534236583342076972286855970946843552864013244136732082051193504831296540655412738027597902495009180740066924639466723743389445220110252610249364092240278130749541923013345165274974352280503598225'

The following Fig.4.3 shows the generated secret key using secret key sharing algorithm

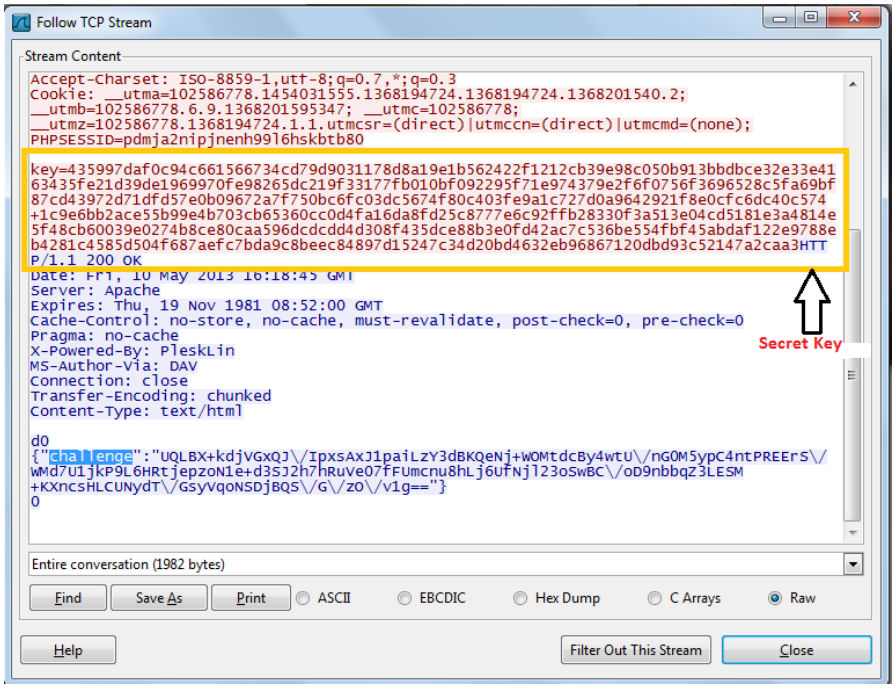

Fig.4.3 Generated Secret Key

4.9.1 32 CHARACTERS ENCRYPTED SESSION ID

The web server generates the 32 characters session ID and encrypt the 32 character session ID using Secret Key Sharing algorithm. The encrypted 32 characters session ID is assigned to the client. The generated session ID of the 4 web application sessions are shown in the Table.4.1

Table.4.1 32 character plain Session ID and Encrypted Session ID

No	plain Session ID (Length=32)	Encrypted Session ID
1	61BBF1C93852828924718BCA037854F0	iQHBPW6HDFKejs7QlOnmUVgzCPNJz1oyCF4S0x/+AhlvqpNuS9IJLg==
2	DDAF120DB46480BD6F2F33DA89C7EF81	tQIfNJqHDFJmqTakxTMDWC0rCKjODO5RdRNGecol1U6W8WBm+t4DUA==
3	945A6E5AB65C1203B78B1CEC54C6E22F	rAIGmrSHDFIv+gvuRmqTb1WAvUVlWAhjTR34zXh5N84iOxrj+FglLg==
4	0A35043F669179D7D229993FD0519C17	4wN2FsKHDFI48ycrLQPfa4GDDi/GAfaymvbalYA0itjCHSop/qosmw==

The attacks such as packet sniffing and man-in-the-middle attacks are executed to capture the Session ID. In order to test the integrity of the session ID, 10 numbers of sessions, 20 numbers of sessions and 30 numbers of sessions are established between the client and the server in the created web application. For each and every session, the number of session IDs captured and the number of session IDs prevented are tabulated in Table.4.2

Table.4.2 Attack results of 32 character encrypted session ID

No	Metrics	32 chars encrypted Session ID		
		10 sessions	20 sessions	30 sessions
1	Number of unique session IDs generated	10	20	30
2	Number of session IDs attacked	1	2	2
3	Number of session IDs prevented	9	18	28
4	Session Hijack Prevention Rate	90 %	90 %	94 %

Table.4.2 shows that 32 character encrypted session ID is having 90 % session hijack prevention rate for 10 sessions, 90% for 20 sessions and 94 % for 30 sessions.

4.9.2 92 CHARACTERS ENCRYPTED SESSION ID

The web server generates the 92 characters session ID and encrypt the 92 character session ID using Secret Key Sharing algorithm. The encrypted 92 characters session ID is assigned to the client. The generated session ID of the 4 web application sessions are shown in the Table.4.3

Table.4.3 92 character plain Session ID and Encrypted Session ID

No	plain Session ID (Length=92)	Encrypted Session ID
1	13B1F75CD8026ACB057 E037471A93C699B7E37 38107E71F109D9888B14 593f12e1cf999f58dede5d b9bd87c578ec	QgA7Xe6IDFI6pFqFxC11Zz3LmYd9x0I KyChFk27tYDyrSj59QwcTv76A+y9NSR CJWIhP6j2fUOYThjog2HpScaUNjltaLr2 PFsQ4G0gixR27f0FS0IzPiGIS/gV6bOGg KGQ3Mw==
2	38C8FFD13BF55A33E2 DDEE751F04601D89AF B06DA2DD8819C149354 B792657a11398b5b340b5 5465d451a74af342	2gIvbhKJDFJRWfZ3ESEtBbF5pnGwbah Rc0oH8xKVV2XnWG8WTGuv9ElaJUw APu7V5vPbaAaMJ38coRUvUXwFVSZZ/ tlt97LCvcVHPbjYcqwBDAn3tZLT0xrAH tL7V1yIQ704Uw==
3	85170F3AE1E52434739E 2587256F5C9F4BF4B912 BD5606DBDA716A75A4 B9f4a276b054fc84518e45 86a8f790d10	cAPlLyKJDFKm52dBdIUj5MePw/0VN1 1k+WEfkImirEGHFuEgAC/qn8s6uN0dW KKF6ClC94Xg9OBBakyPGC/hsUlL5/9+ 1S9naBJKeraUeSTlSBrdgfO3iUsbBM1G 2mqFrIxCmA==
4	1F6F15E9D28E5149B052 94FD65897CE28E98FB8 D0C7442C781EACE1FB B9265c530f4ffd3843da11 2cab046118799	MwNL50OJDFK4mhYesSvBbhV3HVJ6n 6BfFLgL2CCWN9qzwyVSJoKxfreomGQ vA/v6IxHBxRjt+gECrRqieVowVfzz/QW G5Wwl+YEg4CCxa/eP2ECbuV

The following Table.4.4 shows the attack results of 92 character encrypted session ID.

Table.4.4 Attack results of 92 character encrypted session ID

No	Metrics	92 characters encrypted Session ID		
		10 sessions	20 sessions	30 sessions
1	Number of unique session IDs generated	10	20	30
2	Number of session IDs attacked	0	1	1
3	Number of session IDs prevented	10	19	29
4	Session Hijack Prevention Rate	100 %	95 %	97 %

The attacks such as packet sniffing, man-in-the-middle attacks and brute force attacks are executed to capture the Session ID. In order to test the integrity of the session ID, 10 numbers of sessions, 20 numbers of sessions and 30 numbers of sessions are established between the client and the server in the created web application.

For each and every session, the number of session IDs captured and the number of session IDs prevented are tabulated in Table.4.4. The table shows that 92 character encrypted session ID is having 100 % session hijack prevention rate for 10 sessions, 95 % for 20 sessions and 97 % for 30 sessions.

4.9.2 212 CHARACTERS ENCRYPTED SESSION ID

The web server generates the 212 characters session ID and encrypt the 212 character session ID using Secret Key Sharing algorithm. The encrypted session IDs of the 4 web application sessions are shown in the Table.4.5

Table.4.5 212 character plain Session ID and Encrypted Session ID

No	plain Session ID (Length=212)	Encrypted Session ID
1	5E3602C889EA285A8E4C107 ABAAF726B858D6B6E31C0D 331D7BEC19EAF79E7755CA 729C7B0C7FAD9FEFFBD0DF 078DABC31C25982861DCFA 24FA6495BD9AE4F5D3DAEF 8324509A3B9700F997E11FFD 5C16DBFFF4CD1025CFCCC1 Ac4fbbc05a93e3518151277c6b 2e09bd0	RQMQBJqJDFJa+V9tyRkR+i8DDJV52 0lkbYyZM8ghRbDtvX3B6tW6W7wyJ5 dy6RGPjXwZpvJt2bTSLTNU0zCAzata Qu3SeYx5eYxgURx/Xk4CO0HW752lz e9mF2kmeWSg42QuT6gWdmmLr4GV mL0SzJ0TrGpUQeFEhksFoZPmzOkday gNp5awq5bOLkDgliYNX2LHrPiivOjyg qzw67EyNmQXRQN8Vuypm+I5uQqS3 35L9QmrRevfqbNpCIGugUNDwfGrQB jngG81jhZw2qCq0FDgdMG2h9Q0EBqi Tg==
2	7C3096D9EEADB2917F00320 2AED4CDBF52B8D0644E5E AA3238C66249A277269696F C106346D8A4316ACBBE1326 596134F4E5ED8FA1EBF017D C70B1DCC82C6ED2704E8E2 04DDFACCB760B3D26C4B97 81BB24C3B2A795145A4C9A Dcd7942012e8b304760f752e11 d74f4af	5QH7fbKJDFIvyR7oj7yDXLWx8pOUF pO78u79d4KpWdiYG0YIZY9HTLtOW /Xo4g6jfFTWaDHbQ2Zyw6kU1Cm9Rl enHdyGOGI60GeN4w78JCIsxxfKvBW 1bRevkENs7nyhvVpf9PjDFvK/UxWLS vS6xDFr3ZxiGv/eUcAAcNINXsdYzK WfyEc07YzAn81QGCxWeH/cTK7fOb mv0iEYxPlpt9IS3QD9mhkqDNs/Jb6Sk njQXd31dpCCpdiYbcUFRR9s2OV2cA +2dIabm/Ugk/j93QU5T/9ezIL+gHbflw= =
3	E7BEA07AE7E335297EEAB1 F53FBD78896500D7CF1C3FF 276775688F9A048FDF857C77 99ADACA56BB0700EA2EE3 FDFF18B3DA6F12EDEE35C6 71F93C8980F8F3154C3FA063	HAIk8cKJDFLSK1e3r+OVlC3XwUJljx CwDXuyQpL9Sg507NpeG+/whEFlVA biA3P2ffBnx+UjBXFoEYnNxpD91Cyz Qb9HlVkwVLszYo6JE3bW3dCMV7+6 cg2Mg5lMeXmHsAMAArMnDE7ehIx V6R3gy6aaYNBDBt7ttTRSj22FGBaLU

	A7581AA95BDFD7B7A2E537 9CC672E265617743EEA42E3a 2a3b156a16f19f6867dff42b8d3 f4a	Vt9yAS8Bl/x2kZiNFiyu0NBJ8Lm83qef oDtifidH1AE7mAr+GGKvoOFR9qsMs uO344VgfyU1AgYMrV9LHr+/g/tno+5u sH30SNoiFdhbjYmmXNs/3KHNQKpM A==
3	361295DE73EEB0D9CDF763 BB6A53728DEC9BAA08E3E7 EE2D2A47DCFD9A889A90A E6E24A0841A9FEBD70EA75 074309C1D6498F6547A3E19F 70A240DC73BB5E0651FB071 BA2FA98DBBD4B6D56303E3 8D480FF8A4E9312DD9A3D9 90b666817e9c1ba30bc2fc4698 3061229a	swK8O9WJDFJ/NE1+P4jtpjenwKIJoW gpe+tH6TKj+gmsTM2FQDrI9QLB7P6 wP/jz07TyqdqYqbH/Ec7/kf+ufanCiVlB +hCTDEBIJyqqh7JMxx/rqxl9oV05qVA 7MkFUq7QIsm9A72yTTSOwMDm9Vf 8R8Rg7nzjB29NIfZrcYn3sMPI4sSpu/K wpkWWjmhxyFA1B2ihHD0mrTBOkuv v+QJ201a3odaF2T6cCK1ycYgXGcYyP wnm1RXimr9jegCO8+jIbb8CN0VMvru HFEBONWVKoTcIpslM1ap52Tw==

The attacks such as packet sniffing and man-in-the-middle attacks are executed to capture the Session ID. In order to test the integrity of the session ID, 10 numbers of sessions, 20 numbers of sessions and 30 numbers of sessions are established between the client and the server in the created web application. For each and every session, the number of session IDs captured and the number of session IDs prevented are tabulated in Table.4.6

Table.4.6 attack results of 212 character encrypted session ID

No	Metrics	212 chars encrypted Session ID		
		10 sessions	20 sessions	30 sessions
1	Number of unique session IDs generated	10	20	30
2	Number of session IDs attacked	0	0	0
3	Number of session IDs prevented	10	20	30
4	Session Hijack Prevention Rate	100 %	100 %	100 %

Table.4.6 shows that 212 character encrypted session ID is having 100 % session hijack prevention rate for 10 sessions, 100 % for 20 sessions and100 % for 30 sessions.

4.10 PERFORMANCE ANALYSIS

The following Table.4.7 presents the number of sessions IDs prevented by the attacks for 32, 92 and 212 characters encrypted session ID.

Table.4.7 Number of Session IDs prevented

No	Metrics	No of session IDs prevented		
		10 sessions	20 sessions	30 sessions
1	32 characters encrypted session ID	9	18	28
2	92 characters encrypted session ID	10	19	19
3	212 characters encrypted session ID	10	20	20

The Fig.4.4 shows the number of Session IDs attacked for 32,92,212 character encrypted session ID

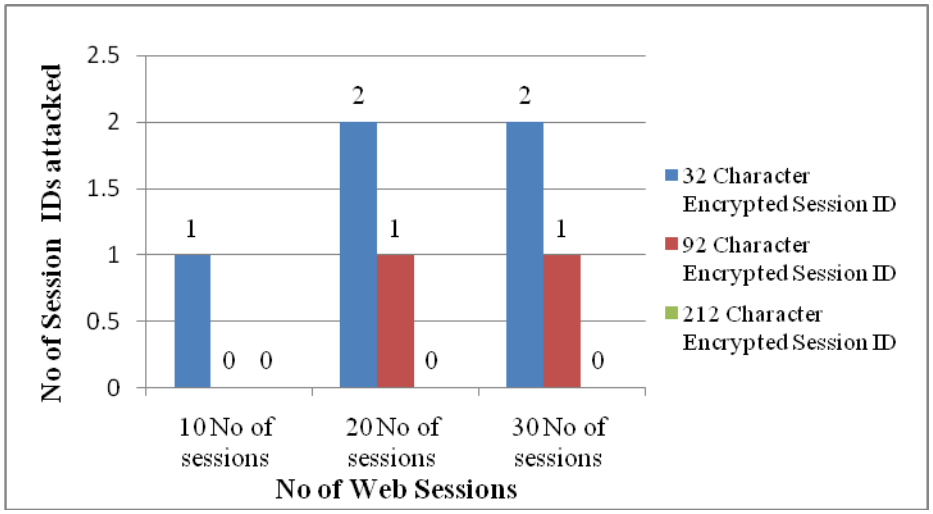

Fig.4.4 No of Session IDs attacked for 32,92,212 character encrypted session ID

Encrypted Session ID generation time is measured for the 32, 92 and 212 character encrypted is tabulated in the Table.4.8

Table.4.8 Encrypted Session ID generation time

No	Length of the encrypted Session ID	Encrypted Session ID generation time
1	32 character	40 ms
2	92 character	115 ms
3	212 character	265 ms

4.11 COMPARISON OF SESSION HIJACK PREVENTION RATE

Session Hijack Prevention Rate is measured for the proposed encrypted session ID and the prevention rate is compared with existing systems such as Unique Session ID presented by Lanxiang Chan, Dan Ferg et al. (2009), TCP state analyzer given by Bazara Barry and Anthony Chan (2007) , Received Signal Strength (RSS) discussed by Xiaobo Long and Biplab Sikdar (2010) , ARP Table discussed by Mark Lin, SANS Security Institute (2005), Secure Authentication and Key Agreement presented by Fengjiao Wang Yuqing Zhang (2008) and One way Authentication discussed by Jeffrey Cashion and Mostafa Bassiouni (2013). The following Table.4.9 shows the session hijack prevention rate

Table.4.9 Session Hijack Prevention Rate

No	Metrics	Session Hijack Prevention Rate		
		10 sessions	20 sessions	30 sessions
1	32 characters encrypted session ID	90 %	90 %	94 %
2	92 characters encrypted session ID	100 %	95 %	97 %
3	212 characters encrypted session ID	100 %	100 %	100 %

The results proved that 212 character of encrypted session ID is completely prevents the session hijack attacks. The following Fig.4.5 shows the comparison of session hijack prevention rate between the existing systems and 212 character encrypted session ID.

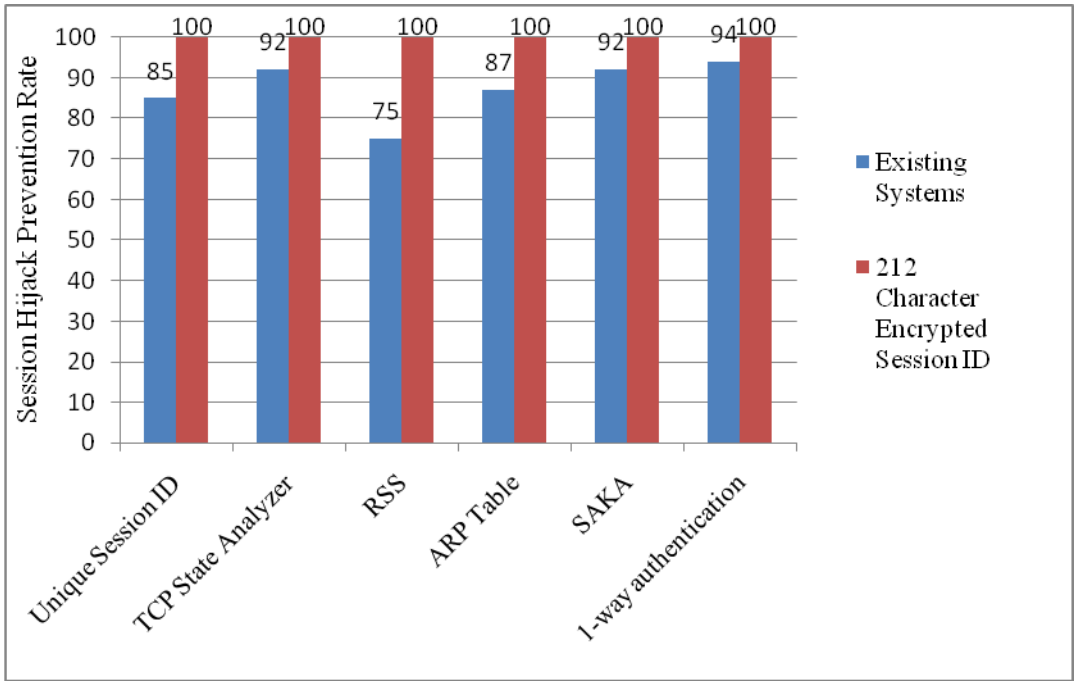

Fig.4.5 Comparison of Session Hijack Prevention Rate

Experimental results proved that 212 character encrypted session ID completely prevents the session hijack attacks in web applications.

4.12 SUMMARY

Web application security is more important for the systems that are connected to networks. Current web applications are weakly secured against session hijack attacks. The proposed the strong and encrypted Session ID is tested in three different cases of encrypted Session IDs of length 32 characters, 92 characters and 212 characters. The integrity of the session ID in a web application is tested by establishing 10 sessions, 20 sessions and 30 sessions between client and server. Experimental results proved that 212 characters of encrypted session ID completely prevents the session hijack attacks in web applications.