PREVENTING HEALTH CARE WEB APPLICATIONS FROM SESSION HIJACK ATTACKS USING SESSION KEY AUTHENTICATION AND DISTRIBUTED SESSION ID

S. S. Manivannan and E. Sathiyamoorthy
School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India
E-Mail: manivannan.ss@vit.ac.in

ABSTRACT

Usage of health care web applications by network of hospitals and health care service providers are increases in the current technology world. Accessing the confidential healthcare information by doctors, patients over the wireless network is at the risk of information theft by various attacks. Most of the multispeciality hospitals situated in metropolitan cities, chief doctors are sending the prescriptions to the junior doctors over the internet after successful completion of the surgery. Individual session is created for each user to access the health care data in a web application. Hackers make use of sniffer tools to crack the session ID and hijack the session in order to steal the confidential data of the patients. In this paper, we have proposed the session key authentication method and distributed session ID to secure the medical data against session hijack attacks in wireless networks.

Keywords: session hijack attack, health care web application, wireless network, authentication, distributed session ID.

1. INTRODUCTION

Sharing the medical information with the use of latest communication technologies questions the confidentiality of the data. Most of the confidential data in health care applications are frequently hacked by powerful hackers. Deans, Doctors, patients and nurses can access the patient data over the wireless network. Insurance companies and health care service providers are using the same method of storing the medical information. Hackers use various hacking methods to steal the confidential data of the patient. Session hijack is a powerful attack which hijacks the session from web application users such as doctors, patients and nurses. Security requirements of healthcare applications are

(i) Confidentiality
(ii) Integrity
(iii) Availability
(iv) Privacy
(v) Authentication

Session hijacking is the technique of hijacking the web application session between trusted client and the target server. The types of session hijacking are

(i) Session theft: It can be done by installing proxy server. It's the primary type of Session hijacking. It is similar to man in the middle attack, where attacker gets in the middle of the session and capture information such as session ID, sequence number, IP address, port number…etc. The attacker convinces the server as legitimate client and it can alter, delete the information. The attacker often breaks the connection between the client and server.

(ii) Cookie theft: when an authenticated user login in with his username and password in a face book account. The face book will provide a cookie for the authenticated user. The rest of the communication relies on the cookies for identifying the authenticated user. If the attacker steals the cookie then he will start accessing the session with that cookie.

(iii) Brute force attack: the non legitimate user use brute force technique and tries all possibilities of session id until the exact match is found. If the user clicks some link which open another site. The attacker finds the session id in that URL.

1.1 Steps to execute session hijacking attack

a) Attacker is placed in between the legitimate client and target server.
b) Trace the packet flow.
c) Sequence number is predicted.
d) Disconnect the session with legitimate client.
e) Take over the active connection with target server.

1.2 Modes of Session Hijacking

Session Hijack can be executed in 3 different modes such as Active, Passive and Hybrid. The following Table-1 compares the 3 modes of session hijack attack.

Table-1. Session Hijack modes.

Active	Passive	Hybrid
The non legitimate user identifies the active session between legitimate client and server and then takes over the session and also pretend to be legitimate client thereby communication occurs.	The non legitimate user identifies the session but just watch the traffic flow between legitimate client and server.	Combination of active and passive attack.
Session replaced by non legitimate client.	Session monitored by non legitimate client.	The non legitimate user keeps listening to active session and then takes over the session when needed.
The attacker uses client side scripting tool. The attacker tears down the connection between legitimate users sequence number need to be predicted before tearing down connection.	Sniffers are used by attacker to gather the details of legitimate client to logon later as legitimate client.	

2. LITERATURE SURVEY

Kalyani, Mohammad and Hong have discussed the secure architecture for healthcare wireless sensor networks. The architecture consists of Patient Monitoring Network (PMN) that monitors the patient mobility. Key generation and agreement is used to provide the authentication of the node in Wireless Sensor Network. Two tier authentications is used. In the first tier, authentication and encryption is done. In the second tier, registration is done.

Kuo, Lo, Wu, Yang and Horng have presented the analysis of health care system using smart card based authentication. The presented CLCC scheme contains four phases of authentication such as Registration Phase, login phase, verification phase and password modification phase are used to provide the strong authentication mechanism for health care providers such as doctors as well as patients.

Jungchae, Byuck Lee and Sun K.Yoo have narrated the data protection wearable health care devices. The presented Advanced Encryption Standard (AES) framework is used to provide strong authentication and security for wearable devices in sharing the electronic health records. The wearable devices supported by AES framework provide the real time encryption using electrocardiogram.

Ahmed, Huaiguo Fu has explained the distributed learning clustering of health care data. The presented distributed learning local clustering algorithm works in distributed environment instead of centralized environment. The dlc algorithm partitions the medical data vertically. The protocol is encrypted using homomorphic encryption and the protocol prevents the colluding attacks. Majidi, Mobarhan and Parchinaki have discussed the key management techniques for secure patient monitoring in Wireless Sensor Networks. Hybrid key management combines the RSA encryption system and Elliptic Curve Cryptography system to secure the medical data in wireless Sensor networks. The results proved that hybrid key management techniques consumes less energy when compared to other key management techniques to secure the health care data in wireless sensor networks.

Rui Zhang and Ling Liu have described the security model for health care application cloud. The presented Electronic Health Record (EHR) security reference model is used to collect and integrate the medical data in the secure manner. EHR model is also used to encrypt the health care data and allow the specific health care users to access the medical data securely over the cloud environment.

Danan, Shiping chen, Surya Nepal, Rafael calvo and Leila Alem have discussed the method of sharing the health care data in the cloud environment. The developed cloud computing application is used to monitor the patients remotely. The secure data sharing protocol is used to share medical data between health care providers and patients in the cloud environment.

Ongxing Lu, X.Lin and X.Shen have developed the Secure and Privacy preserving Computing (SPOC) framework.

For mobile healthcare emergency. The SPOC is used to process the personal health information with less disclosure of privacy using user centric privacy access control and privacy preserving scalar product computation (PPSPC). The simulation results proved that the SPOC framework is effective and highly reliable in mobile healthcare emergency.

Jun Zhou, Z.Cao, X.Dong, X.Lin and A.V Vasilakos have presented the method of securing mobile healthcare social networks. The presented distributed architecture is used to provide the security and privacy for health care data in M-healthcare social networks. The counter measure are discussed to prevent the data injection attacks, mobile compromise attack, privacy attack of data attacks and Target oriented compromise attack in mobile health care social networks.

Suhair Alshehri, S.P. Radzi szowski and Rajendra K.Raj have discussed about securely accessing the healthcare data in cloud environment. The Cipher text policy Attributed based Encryption (CP-ABE) is used to encrypt the health care records based on the user's credentials.

Kevin, Emil, Smith and Nick have described about the limitations, requirements and security models with respect to web client authentication. The interrogative adversary, who is able to compromise the system by adaptively querying the website, the presented secure client authentication scheme uses the set of hints to make the client authentication system resistant against the interrogative adversary. By incorporating SSL cryptographic protocol in the authentication scheme, the system becomes resistant against active adversary.

Yang, Wang and Liu have discussed about the drawbacks of the SIP authentication security mechanism which is based on HTTP Digest Authentication. Off-line password guessing attack and server spoofing are the main security problems that need to be solved. To overcome these problems they presented a new scheme for secure authentication based on Diffie Hellman concept which possesses the features of discrete algorithms.

Karthikeyan, Ricardo, Fournet and Andrew have discussed two major specifications WS-Trust and WS-Secure Conversation that provide mechanisms to establish secured session by using shared security token called security context token between the communicating parties. These specifications overcome the inefficiency in WS-Security which provides security to SOAP traffic only at the message level instead of at the required session level.

Luke Murphey has discussed the methods of web-based authentication and the areas where authentication faces failure and how to address those failures. User authentication is one of the most critical part in the web application. User authentication failure is not only due to technical issues but also due to lack of good policy and user education. Good program design, policies and people are essential in the development of secure authentication for web based applications.

Aytunc and Ibrahim have presented a new approach for secure SIP authentication based on Elliptic Curve Cryptography (ECC). ECC technique has advantages like smaller key sizes and rapid computations as compared to Public Key Cryptography at the same security levels. They also made comparisons between Diffie-Hellman and ECDH approaches and found that ECDH requires less number of dynamic instructions and execution time.

3. OVERALL SYSTEM ARCHITECTURE

The following Figure-1 shows the proposed architecture for the super specialty hospital. Nowadays patients will be going to the hospitals only for the critical cases such as minor surgery or major surgery. Most of the super speciality hospitals allow the patients to communicate with the doctors with the help of hospital web application.

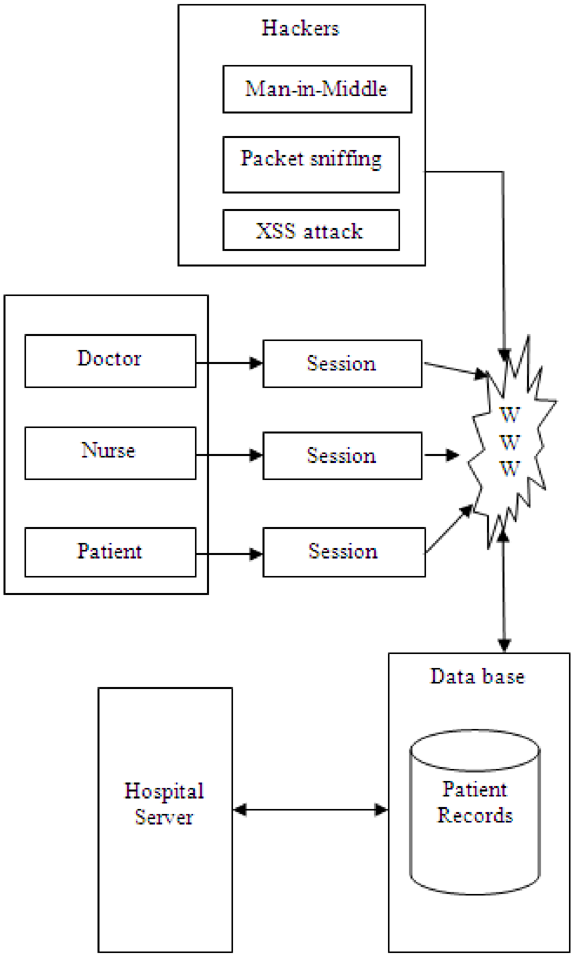

Figure-1. Architecture of super specialty hospital.

Patients can login to their web session using http protocol and interact with the doctors in the hospitals for the diseases that can be treated with the help of tablets alone. Also the hospital web application allows the patients to send their medical reports online to the respective doctors.

The following medical reports can be sent to the doctors:

a) Blood test report
b) Blood Pressure Chart
c) ECG report
d) Audiogram Test
e) Scan Reports
f) X-Ray reports

When the patients are sending their personal medical reports to their doctor, doctor can see the reports and prescribe the medicines over online. Some of the persons who want to destroy the health of the patients; they can sniff the web application session between the patient and doctor. They can completely observe the web session content and they can alter the medicines prescribed by the doctors using the session hijack attack.

Patients think that he is interacting with doctors but actually he was interacting with attackers. This kind of session hijack attacks is severe and can destroy the health of the patients. The proposed architecture prevents the session hijack attacks.

4. METHODOLOGY

Patients, doctors and nurses can login to their session using their login credentials such as user id and password. In order to prevent the stealing of patient credentials by the attackers, a session key is generated using session key generation algorithm and that session key will be sent to the patient mobile number. The patient has to validate the identity by entering the session key into the hospital web application.

4.1 Session key generation algorithm

The following algorithm implemented in java is used to generate the session key.

```
package session;
importjava.util.Random;
publicfinalclassRandomGaussian {
        publicstaticvoid main(String[] args) {
RandomGaussiangaussian = newRandomGaussian();
double MEAN = 100.0f;
double VARIANCE = 0.05f;
doubledd=gaussian.getGaussian(MEAN, VARIANCE);
int y=(int)dd;
double z=(dd-y)*1000000000;
intzd=(int)z;
System.out.println("Gaussian session key "+zd);
  }
private Random fRandom = new Random();

privatedoublegetGaussian(doubleaMean,
doubleaVariance){
returnaMean + fRandom.nextGaussian() * aVariance;
  }
}
```

After the client is authenticated by the web server using session key, the web server splits the whole session ID into three parts and send it to the client in 3 times. Client may be patient or doctor or nurse.

4.2 Distributed session ID generation

The following distributed Session ID generation algorithm is used to generate the whole session ID and send it to the client in 3 parts.

Algorithm: distributed session ID generation

```
i)    input set A =  digits , alphabets
ii)   input set S = { *, @ , $, %, &, # }
iii)  Session key = $S_K$
iv)   If ( $\text{client}_{input}$ ) = $S_k$
then
Client login = success;
Else
Client login = fail;

v)    $\text{Session ID}_{gen}$=  { (0-9) | (a-z) | (A-Z) | (S) }
vi)   Splitting the session $\text{ID}_{gen}$ in to 3 parts
vii)  $C_m$= $\text{SID}_{gen}$ /2
where $c_m$ is the middle character of $\text{SID}_{gen}$

viii) If ($C_m$= integer)
assign integer=$C_m$
else
$C_m$= flooring($C_m$)
$\text{SID}_{mid\_part}$ = {$C_{m-6}$+….+$C_{m-1}$}+$C_m$+($C_{m+1}$+…$C_{m+6}$}
$\text{SID}_{left\_part}$= {$C_1$+$C_2$+…+$C_{m-7}$}
where $C_1$ = first character of $\text{SID}_{gen}$
$C_2$= second character of $\text{SID}_{gen}$
$\text{SID}_{right\_part}$= $C_{m+7}$ +…..+ $C_n$
where $C_n$ is the last character of $\text{SID}_{gen}$
Server sends $\text{SID}_{left\_part}$, $\text{SID}_{mid-part}$,  $\text{SID}_{right\_part}$
Client receives $\text{SID}_{left\_part}$, $\text{SID}_{mid-part}$,  $\text{SID}_{right\_part}$
Client concatenates the 3 parts of SIDgen
Client transfer the data to server
Client log off the session
```

Whenever the client is receiving the session ID from server, attacks such as packet sniffing, Man-in-the-Middle attack and Cross Site Scripting attacks are executed to capture the session ID.

4.3.1 Packet sniffing

Wireshark tool is installed in the client machine and content of the session such as Session ID, packet header and packet data are captured.

4.3.2 Man-in-the-Middle attack

a) Attackers login to the session
b) Attacker uses sniffing tool
c) Attacker send the RST and FIN packet to the client
d) Client gets disconnected
e) Attacker take over the session

4.3.3 Cross Site Scripting (XSS) attack

(i) create the malicious java script
(ii) inject the java script in to the web page of the Created web application
(iii) steal the private data between client and web server

5. RESULTS AND DISCUSSIONS

In order to test the proposed system in real time the sample web application www.chennaisuperspeciality.com is created. Separate login is created for patient, doctor and nurse. Whenever the patient or doctor enters in to their web session, web server generates the session ID and splits in to 3 parts and sends it to the client. Client integrates the session ID and communicates with the server. The following Table-2 shows the sample session keys generated by the session key generation algorithm.

Table-2. Session keys.

S. No.	Session number	Session key
1	Session 1	32267582
2	Session 2	24190361
3	Session 3	75617096

The following Table-3 shows the generated whole session ID and 3 parts of the session ID.

Table-3. Generated Session IDs.

Session	Generated Session ID	SID part1	SID part 2	SID part 3
1	7692abc@@32ghj%%323345*BZX&&&&581324	7692abc@@	32ghj%%323345*	BZX&&&&581324
2	88934%%%klmn@@@CMNgbh07###009ghtl@@yy	88934%%%	klmn@@@CMNgbh07	###009ghtl@@yy

Web server generates the variable length session ID ranging from 36 characters to 68 characters. Generated session ID has been spitted to 3 parts. SIDmid_part will have the length of 13 characters as constant for all the sessions. But the SIDleft_part and SIDright_part will have variable length of characters for each and every session based on the total length of the session Id generated by the server.

5.1 Results of attacks

10 number of sessions, 20 numbers of sessions and 30 number of web sessions are created between the patient and doctor. Packet sniffing, Man-in-the-middle attack and cross site scripting attacks are executed. The results are tabulated.

When the patient is interacting with doctor, Packet sniffing attack is executed and the results are recorded in the Table-4.

Table-4. Results of packet sniffing attack.

No.	Packet sniffing attack	No of Session IDs captured		
		10 sessions	20 sessions	30 sessions
1	Number of unique session IDs generated	10	20	30
2	Number of session IDs captured by attacks	0	0	0
3	Number of session IDs prevented from attacks	10	20	30
4	Session Hijack Prevention Rate	100 %	100 %	100 %

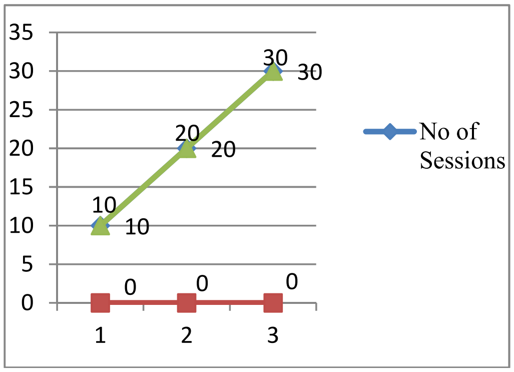

Figure-2. No of session IDs prevented (Packet sniffing).

When the patient is interacting with doctor, Man-in-the-Middle attack is executed and the results are recorded in the Table-4.

Table-5. Results of Man-in-the-Middle attack.

No.	Man-in-the-Middle attack	No of Session IDs captured		
		10 sessions	20 sessions	30 sessions
1	Number of unique session IDs generated	10	20	30
2	Number of session IDs captured by attacks	0	0	0
3	Number of session IDs prevented from attacks	10	20	30
4	Session Hijack Prevention Rate	100 %	100 %	100 %

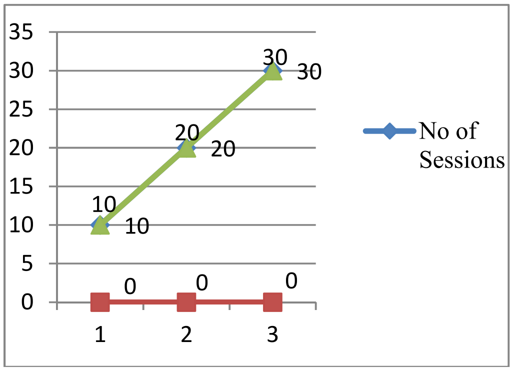

Figure-3. Number of session IDs prevented (MIM attack).

When the patient is interacting with doctor, Cross Site Scripting attack is executed and the results are recorded in the Table-6.

Table-6. Results of Cross Site Scripting attack.

No.	Cross site scripting attack	No of Session IDs captured		
		10 sessions	20 sessions	30 sessions
1	Number of unique session IDs generated	10	20	30
2	Number of session IDs captured by attacks	0	0	0
3	Number of session IDs prevented from attacks	10	20	29
4	Session Hijack Prevention Rate	100 %	100 %	97 %

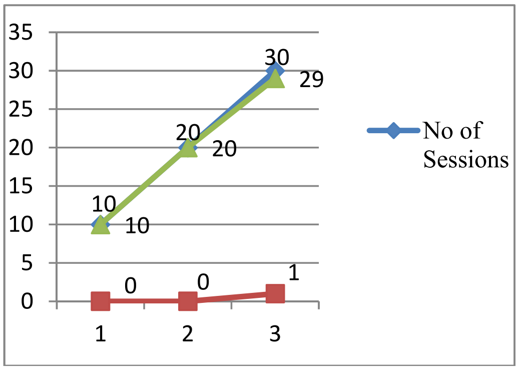

Figure-4. Number of session IDs prevented (XSS attack).

5.2 Session Hijack Prevention rate

From the results of Table-7, it was observed that the proposed system has the session hijack prevention rate of 100% against packet sniffing attack, 100 % against man-in-the-middle attack and 97% against Cross Site Scripting attacks.

The following Table-7 shows the session hijack prevention rate for packet sniffing, man-in-the-middle and cross site scripting attack.

Table-7. Results of Man-in-the-Middle attack.

No.	Name of the attack	No of Session IDs prevented		
		10 sessions	20 sessions	30 sessions
1	Packet Sniffing attack	10	20	30
2	Man-in-the-Middle attack	10	20	30
3	Cross Site Scripting attack	10	20	29

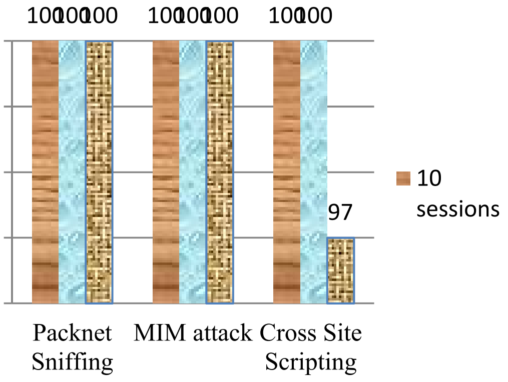

Figure-5. Session Hijack prevention rate.

6. CONCLUSIONS

Web application plays an important role in the field of health care. Super specialty hospitals are using the web applications to communicate with the patients. Individual web session is created for each and every time for the client. In order to prevent the stealing of sensitive medical data of patients by session hijack attacks, we have proposed strong authentication using session key for the client authentication and distributed session ID for the sessions. The experimental results proved that distributed session ID completely prevents the session hijack attacks in wireless networks.

REFERENCES

[1] Kalyani Divi, Mohammed Raza Kanjee and Hong Liu. 2010. Secure Architecture for Healthcare Wireless Sensor Networks. Sixth International Conference on Information Assurance and Security. pp. 131-136.

[2] Kuo-Hui Yeh, N.W. Lo, Tzong-Chen Wu, Ta-Chi Yang and Horng-Twu Liaw. 2012. Analysis of an eHealth Care System with Smart Card based Authentication. Seventh Asia Joint Conference on Information Security. pp. 59-61.

[3] Jungchae Kim, Byuck jin Lee and Sun K. Yoo. 2013. Design of Real-time Encryption Module for Secure Data Protection of Wearable Healthcare Devices. 35th Annual International Conference of the IEEE EMBS. pp. 2283-2286, Japan.

[4] Ahmed M. Elmisery, Huaiguo Fu. 2010. Privacy Preserving Distributed Learning Clustering Of HealthCare Data Using Cryptography Protocols. 34th Annual IEEE Computer Software and Applications Conference Workshops. pp. 140-145.

[5] Mojib Majidi, Rokhsareh Mobarhan, Amir Hatami Hardoroudi, Abd Samad H-Ismail and Aidin Khodashenas Parchinaki. Energy Cost Analyses of key Management Techniques for Secure Patient Monitoring in WSN. IEEE Conference on Open Systems. pp. 111-115, Malaysia.

[6] Rui Zhang and Ling Liu. Security Models and Requirements for Healthcare Application Clouds. pp. 1-8, IEEE International Conference on Security.

[7] Danan Thilakanathan, Shiping Chen, Surya Nepal, Rafael Calvo, Leila Alem. 2013. A platform for secure monitoring and sharing of generic health data in the Cloud. Future Generation Computer Systems, Elsevier.

[8] ongxing Lu, Xiaodong Lin and Xuemin Shen. 2013. SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency. IEEE Transactions on Parallel and Distributed Systems. 24(3): 614-624.

[9] Jun zhou, Zhenfu cao, and Xiaolei Dong, Xiaodong lin and Athanasios v. Vasilakos. 2013. Securing m-healthcare social networks: Challenges, countermeasures and Future directions. IEEE Wireless Communications for e-health applications. pp. 12-21.

[10] Suhair Alshehri, Stanisław P. Radziszowski, and Rajendra K. Raj. 2012. Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption. IEEE 28th International Conference on Data Engineering Workshops. pp. 143-146.

[11] Kevin Fu, Emil Sit, Kendra Smith, Nick Feamster. 2001. Dos and Don’ts of Client Authentication on the Web. Proceedings of the 10th USENIX Security Symposium. Washington, D.C., USA.

[12] Chou-Chen Yang, Ren-Chiun Wang, Wei-Ting Liu. 2005. Secure authentication scheme for session initiation protocol. Computers and Security, Elsevier.

[13] Karthikeyan Bhargavan, Ricardo Corin, Cedric Fournet and Andrew D. Gordon. 2004. Secure Sessions for Web Services. ACM Workshop on Secure Web Services, Fairfax VA, USA.

[14] Luke Murphey. 2004. Secure Web Based Authentication. IEEE International Conference.

[15] Aytunc Durlanik and Ibrahim Sogukpinar. 2005. SIP Authentication Scheme using ECDH. World Academy of Science, Engineering and Technology. 8: 350-353.