VOL. 11, NO. 2, JANUARY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

AN INNOVATIVE SECURITY ARCHITECTURE AND ALGORITHM FOR SOCIAL NETWORK SERVICES

S. Thiraviya Regina Rajam[1] and S. Britto Ramesh Kumar[2]
[1]St. Joseph's College (Autonomous), Trichy- 2, India
[2]Department of Computer Science, St. Joseph's College (Autonomous), Tricy-2, India
E-Mail: srajicic10@gmail.com

ABSTRACT

Social Network Services (SNS) play a vital role in today's communication. There is a need to ensure the security, effectiveness, usability, friendliness and accuracy mechanisms in SNS. In this paper an innovative Security Architecture and Algorithm for Social Network Service (SAASNS) is proposed. SAASNS System has been developed and implemented to provide web-enabled community SNS. The results are tested for community user authentication and access to services as well as to measure system response time with respect to the user.

Keywords: security, effectiveness and usability.

INTRODUCTION

Social networks like facebook, twitter, linked in and google+ have different security measures, rules, regulations and policies. Earlier security for user is not up to the mark. In facebook if a person wants to share any content it is publicly available in social network and every one see it even if he shares only with his friends if his/her friend likes it then it is to all the friends in his list can see it. So privacy and security is not there. Public Key Cryptography (PKC) can provide secure communication in Social Network Service (SNS). PKC is recently playing an essential role in electronic banking and financial transactions. Though several PKC algorithms are available for encrypting the data. Elliptic Curve Cryptography (ECC) is one of the best public key techniques for its small key size and high security. In this work Elliptic Curve Diffie Hellman (ECDH) for key exchange, signed with Elliptic Curve Digital Signature Algorithm(ECDSA) key for identity verification, AES - 128 for encryption, and the SHA-2 hash function in an Hash Message Authentication Code(HMAC) for message authenticity algorithms.

REVIEW OF LITERATURE

[Youssef, 2014] described general Social Network Services (SNS) architecture. The architecture of the virtualization layer is composed of four modules with interaction signals between the modules as in the original SNS architecture. The virtualization layer operation is consisting of data extraction, data cleansing unit, data abstraction or transformation unit, data federation unit, and cache memory1.According to Williams [Williams, 2010]the architecture of Social Network Services contains(i) a set of binary relationship types,(ii) asset of users, represented by individual user profiles, (iii) a set of mechanisms for exchanging information, such as message boards, email, and wall posts, (iv) and a set of search functions, to locate user profiles2.Luigi *et al.* (2012)described the possible architecture that included the functions of a social network and simulated the characteristics of social network structure. The author detailed an overview of the processes related to SNS activities, namely new object entrance, service discovery and composition, new object relationship establishment, and service provisioning3.The model for social stream, a social network framework was described by [Tapiador *et al.* 2012], in which the activities were based on two super types called actor and object. Actor is the first super type for any social entity defined in the Social Network Services (SNS). Object is the second super type introduced by social stream's architecture which represents every entity that could be the object of an actor's action and thus appearing in activities' timelines4.Datta *et al.*(2010) proposed a Distributed Online Social Network (DOSN) architecture model with the objective of protecting users' privacy. The concept of the model was based on two simple assumptions: decentralization and cooperation between friends to facilitate the implementation of a secure, privacy preserving SNS5.Aravindhu *et al.* (2014) introduced an architecture called WARNING BIRD, for detecting and blocking of suspicious Universal Resource Location (URL) in SNS6. He *et al.* (2011) introduced crawling architecture and the database to store crawled information from foursquare. The authors outlined three levels of attack: cheating via Global Position Service (GPS), automated cheating, and use of venue profile analysis to assist cheating7.Shehab *et al.*(2012) presented social network application authentication architecture. The proposed social network application architecture includes three interacting parties namely the user, social network server, and the third party application server8.Khoshgozaran *et al.* (2009) proposed Private Buddy Search (PBS), architecture to enable private spatial queries in social networks. The authors introduced the concept of group keys and secure server side indexes enable users to efficiently and privately query their peers in a social networking services environment 9. Constantinescu *et al.* (2011) proposed an authentication model based on multi Agent System Architecture for social networks. The system architecture includes two related components such as Master Agent (MA) and Super Agent (SA) 10. The remainder of the paper is organized as

follows. In section two provides summary of connected work. Methodology described in section three. In Section four explains security algorithm. In section five performance details are delineated. In section six details the results and discussions. Section seven concludes this paper.

METHODOLOGY

This paper mainly focuses on providing end-to-end security architecture with the support of authentication, access control policy, confidentiality and privacy using Public Key Infrastructure (PKI). This paper is also extended by developing a new algorithm of the proposed Architecture. The proposed Architecture for SNS is depicted in Figure 1. The entities of the architecture are described as follows.

Community Users (CU)

The community users are sending user id, designation, etc. during the registration process over the mail. During the signup, the user is validated with user id and email id which is already sent by the authorities for acknowledging them as valid users. The invalid request made by other users is simply discarded.

Host Community Infrastructure (HCI)

The Host Community Infrastructure (HCI) helps to provide various technical supports such as processing the credentials, end to end connectivity and maintenance of community services. The determined functionalities of the HCI are devised and set aside into four servers namely HCI Firewall, Secure Gateway Community Server (SGCS), AAA Server and Database Server.

HCI Firewall

The HCI Firewall prevents the incoming and outgoing network traffic. HCI Firewall establishes a barrier between a trusted, secure internal network and other service providers' networks. Once the request is made by the user, service request is sent to the Secure Gateway Community Server (SGCS).

Secure Gateway Community Server (SGCS)

SGCS protects the external and internal threats and it filters the user requests and analyzes http and ftp transfers for any trace of malicious threats. Once the request is received by the SGCS, it initiates the user session by verifying the user identity by using AAA server for authentication. The SGCS establishes the secure communication with the respective community for availing the services using Enhanced Elliptic Curve Cryptography (EECC).

Secure Authorized Community Server (SACS)

Secure Authorized Community Server is responsible for providing the requested services rendered by the user. However, both SACS and SGCS establishes secure communications to transmit the service messages using Public Key Infrastructure (PKI) and EECC.

Social Community Services (SCS)

The system provides an interactive environment for the social collaborations. The social community services include chat, message, news feed, notification, events and share.

AAA Server (AAAS)

AAA Server is the central unit of the proposed system which is responsible for authenticating user credentials, authorizing user activities and accounting for the users' log.

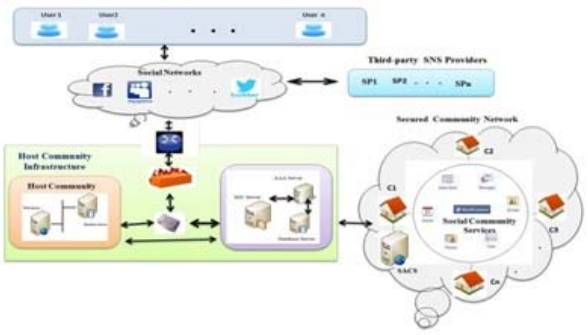

Figure-1. Proposed security architecture for social network services.

1). Authentication, Authorization and Accounting Server (AAAS)

a. Authentication Manager receives the decrypted plain text from USM and verifies the user credentials such as UID and PWDS in consultation with the database manager. Authentication Manager establishes the user session if the user is valid or denies otherwise.

b. Authorization Manager prepares a list of access policies by referring two databases called, RoleDB and PrivilegeDB when the user is well authenticated. The access policies are defined as a Role Based Access according to the community hierarchy. The access policies differ from one another, since services offered by the system are not common to all. The access policy has the details of information on what services the corresponding user can avail and what privilege the user has got. The policies are then forwarded to the SACS.

c. Accounting Manager creates a log of user session like login and logout time, user personal data modification, number of attempts made, track changes and requested pages and so on.

Database Server

SCSF Database Sever holds the SGCS personal information of the registered community users such as userid, passwords, name, date of birth, mobile number, division, designation, profession and email. These data are stored for the purpose of building dynamic community groups within the network.

SECURITY ALGORITHM FOR SECURITY FRAMEWORK FOR SOCIAL NETWORK SERVICE (SFSNS) ARCHITECTURE

User or Gateway Server Authentication Algorithm (UGSAA)

User Authentication prevents unauthorized access of the system from unknown users. The SFSNS architecture is designed to validate users through series of verifications that include the traditional User Identity (UID) with password (PWD)(two factor Font Alpha Numeric(FAN)password and Shape Csode password). After verifies the UID and PWD, Elliptic Curve Cryptography(ECC) encrypts those information using the generated Skey and forwards encrypted UID and PWD and digital signature to the gateway server. The server decrypts the hashed users data using Skey and verifies it using aAdvanced Encryption Standard(AES) key with the database look up. The AES decrypted UID and PWD retrieved from database is checked with gateway server decrypted UID and PWD for client, gateway authentication. Algorithm 1 depicts for client or gateway server authentication.

```
Algorithm for CSAutN(UID, PWD)
{
// Client Side
While (attempt <= 3 times)
{
Get (UID, PWD) [FANPWD and Shape Code; // User
enters UID and Passwords];
Skey=Equate ECC through obtained user's private key,
extracted server's Public key
MD= hashing (UID&PWD) using SHA-2 algorithm;
EMD= encrypt (MD using Skey);
CSAutNDS=sign (EMD using client private key);
CSAutNM= copy (UID & PWD);
CSAutNEM= encrypt (CSAutNM using S key);
Send CSAutNDS and CSAutNEM to the gateway
}
//Authentication SGC Server Side
//Search and validates the user's request from user profile
database;

Skey=Equate ECC through Obtained server private key,
Extracted user's Public key
CSAutNS= decrypt(CSAutNEM using SGCS S key)
CSAutNP= de-sign(CSAutNDS using client public key);
MD= decrypt(CSAutNP using S key);
NMD=hashing (CSAutNS) using SHA-2 algorithm;

A=Split (CSAutNS(UID))
AESKey=key associated with A;
DB:UID=decrypt (A's UID from SGDB using AESKey)
DB:PWD=decrypt (A's PWD from SGDB using AESKey)
If(DB:UID==CSAutNS:UID&
DB:PWD==CSAutNS:PWD)
{
Client & SGCS server authenticated;
If (MD== NMD) then
{
Message integrity is ensured;
}
SGCS sends homepage to the user;
}
Else
        Send error message for invalid user;
        Forward login failure message via email;
        }
```

Algorithm-1. Client or gateway server authentication.

Algorithm 1 depicts for client or gateway server authentication.

Gateway or Secure Authorized Community Server Authentication algorithm (GSACSAA)

The security algorithm for secure communication between the gateway and secure authorized community server. Once the gateway server recognizes a community user as valid, then communicates with the corresponding authorized community server of the user for granting the communication services as per the users role and policy. Using ECC algorithm the communication between the gateway server and authorized community server is done in a secure way. Gateway server forwards the encrypted UID and signed to the SACServer. The SACServer starts by decrypting the received data by Skey. After decrypted, to ensure message integrity the decrypted message digest is mapped with the digested UID which is generated by the SAC server. Algorithm 2 depicts for Gateway or Secure Authorized Community (SAC) Server Authentication

```
Algorithm for SGAutN(UID)
{
// SGCS
{
Get UID; // Gateway forwards UID to SAC Server;
Skey1=Equate ECC through Obtained it's private key,
Extracted SAC Server's Public key
MD1= hashing (UID) using SHA-2 algorithm;
EMD1= encrypt (MD using Skey1);
CSAutNDS1=sign (EMD using SGCS private key);
CSAutNM1= copy (UID);
CSAutNEM1= encrypt (CSAutNM1 using Skey1);
Send CSAutNDS1 and CSAutNEM1 to SAC Server
}

/Authentication SAC Server Side

Skey1=Equate ECC through Obtained SAC Server's private
key, Extracted SGC Server's Public key
CSAutNS1= decrypt (CSAutNEM1 using SGCS Skey1)
CSAutNP1= de-sign(CSAutNDS1 using SGCS public key);
MD1= decrypt(CSAutNP1 using Skey);
NMD1=hashing (CSAutNS1) using SHA-2 algorithm;
A=(CSAutNS1(UID))
AESKey1=key associated with A;
DB:UID=decrypt (A's UID from SGDB using AESKey1)
If(SGDB:UID==CSAutNS1:UID)
{
Client & SGCS server authenticated;
If (MD1== NMD1) then
{
Message integrity is ensured;
}
SACS assigns role and policy to corresponding user;
}
Else
        Send error message for invalid user;
}
```

Algorithm-2. Gateway or secure authorized community (sac) server authentication.

PERFORMANCE RESULT FOR THROUGHPUT ANALYSIS

The purpose of this test is to have an understanding if the system's performance and determining the scalability, where the number of concurrent users is set as variable. Jmeter tool is used to calculate the mean response time, standard deviation time and throughput time (refer Table-1 are calculated to measure system response time with respect to the user).

Table-1. A summary of test results.

Test	Mean Response Time (in msec)	Standard Deviation (in msec)	Throughput No. of Request (in sec)
1	4	0	0.25
2	6	5	1.66
3	6	3	3.3
4	7	2	4.28
5	7	8	5.71
6	7	11	7.142857143
7	8	19	12.5
8	9	21	22.22222222
9	11	20	27.27272727
10	18	22	22.22

Table-2 shows significance of the scale of 1 to 300 users, the system seems to exhibit a linearly growing mean response time. The slope of the curve is starting to reduce between 300 to 400. This is quite natural that every system reaches the level of load where the single user starts to degrade dramatically. Figure-2 shows the performance result for throughput.

Table-2. Result of throughput.

Number of users	Throughput
1	0.25
10	1.66
20	3.3
30	4.28
40	5.71
50	7.142857143
100	12.5
200	22.22222222
300	27.27272727
400	22.22

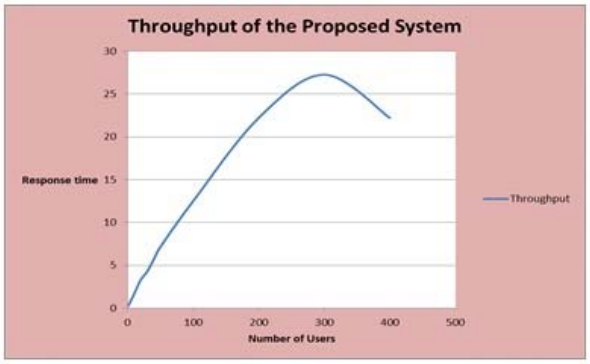

Figure-2. Performance results for throughput.

RESULT AND DISCUSSIONS

The main aim of this experiment is tested and found the performance result for throughput. To determine the scalability of the system, where the number of concurrent users are set as variable and found the result of throughput for each variable. The throughput of the proposed system falls under the mean time range from 11 to 18(Test 9 to 10) milliseconds. This is the expected response time of the server for any user request. However, the latency period can further be extended as the numbers of users are increased. The standard deviation is used to measure the variability of the dataset. If the data are very close to the mean, then the data is deviated only at small range. If the data is deviated more from the mean, then the data is dispersed at larger range. This criterion may also be considered for measuring the security. Test bed was established with the objective of testing the performance for all system at various security levels (user level, service level and data level).

CONCLUSIONS

This paper presents an innovative security architecture and algorithm for social network services and also aims at the provision of end-to-end security architecture that comprises authentication, access control policy, confidentiality and privacy using Public Key Infrastructure (PKI). The performance of the proposed architecture was tested using Jmeter tool, by means of calculating average response time, standard deviation time and throughput time. Test bed was established with the objective of testing the performance for all system at various security levels (user level, service level and data level).It was experienced that the proposed system was able to achieve a secured communication at all levels.

REFERENCES

[1] Youssef B. E. "Online Social Network Internetworking Analysis", International Journal of Next-Generation Networks, vol.6, pp.1-15, 2014.

[2] Williams J, "Social Networking Applications in Health Care: Threats to the Privacy and Security of Health Information", In: Proceedings of the

International Conference on Security in Health Care (SEHC'10), ACM, pp.39-49, 2010.

[3] Luigi A, Antonio I, Giacomo M, and Michele N, "The Social Internet of Things (SIoT) - When Social Networks meet the Internet of Things: Concept, Architecture and Network Characterization", Computer Networks, Elsevier Science Publishers, Vol. 56, pp. 3594-3608, 2012.

[4] Tapiador A, Diego C, "Social Stream, a social network framework", In: Proceedings of the International Conference on Future Generation Communication Technology (FGCT), IEEE, pp.52-57, 2012.

[5] Datta A, Sonja B, Le H and Thorsten S, "Decentralized Online Social Networks", In Handbook of Social Network Technologies and Applications, Springer US, pp. 349-378, 2010.

[6] Aravindhu, N., Arun, M., Yokes, T., Monoharan, M. and Sivasubramaniian S., "Authentication for social network from cautions URLS", In: Proceedings of the IEEE Transaction on Advance and Research in Computer and Communication Engineering (ARCCE), vol.3, pp.4915-4918, 2014.

[7] He, W., Liu, X., and Ren, M., "Location Cheating: A Security Challenge to Location-based Social Network Services", In: Proceedings of the International Conference on Distributed Computing Systems (ICDCS'11), IEEE, pp.740-749, 2011.

[8] Shehab, M., Squicciarini, A., Ahn, G. J., &Kokkinou, I., "Access control for Online Social Networks third party Application", In: Proceedings of the Elsevier vol.3, pp.897-911, 2012.

[9] Khoshgozaran, A., and Shahabi, C., "Private Buddy Search: Enabling Private Spatial Queries in Social Networks", In: Proceedings of the IEEE International Conference on Computational Science and Engineering, vol.4,pp.166-173, 2011.

[10] Constantinescu, N., and Popirlan, C. I., "Authentication model based on Multi Agent Systems Architecture", Mathematical and Computer Science, pp.59.68,2011.