Improved User Authentication Process for Third-Party Identity Management in Distributed Environment

Kashif Nisar[1] Shamsuddeen Bala[2]

AbubakarAminu Mu'azu[3] Ibrahim A. Lawal[4]

Abstract

Third-party identity management user authentication process using single sign-on (SSO) in distributed computer networks requires modification as the process of authenticating user to log into relying party (RP) resources by either identity provider (IDP) or hybrid relying party (HRP) depend always on the authentication of user logins. In this research an algorithm is proposed to authenticate user only once by recording and encrypting user credential with one-way hashing algorithm (SHA2), this simplifies user subsequent logins into relying party by confirming user credentials without other authentication by IDP or HRP. Authentication time and response time continuous time plot of the proposed algorithm was plotted with respect to the arrival time of users in which we show the relationship of authentication time and response time with random arrival rate of users.

Keyword: Single Sign-On, Third-party, Identity management, Distributed networks

1 Introduction

Internet of everything is the current world of innovations, by making everything virtually available on the World Wide Web. The need to manage data easily and securely is the main interest as compared to managing memory space which is no longer an issue (Elgendy & Elragal, 2018). This makes it pretty much easier for people to access dazzling array of online resources at any point in time, anywhere around the globe with the few clicks of the mouse button and/or from their mobile devices (Wada & Tanaka, 2014). However, gaining access to many resources requires login credentials (username and password) and sometimes one time password (OTP) (David et al., 2008). For the obvious reason of security, it is improper to be using single password for accessing resources on line. Same login credentials for accessing different applications/ resource provide the need for single sign-on (SSO) (B. Li et al., 2004).

Identity provider (IDP) authenticates and authorise user to have legal right to access relying party (RP) resources, RP is a party of which user access its resource after authentication by IDP (Vapen, Carlsson, Mahanti, & Shahmehri, 2016).However, some RPs are hybrid relying parties (HRPs) in that they act as both IDPs and RPs at the same time. This makes their third-party identity management to be authenticated and to authenticate other RPs. Yet, other RPs are been authenticated by HRPs and IDPs (Vapen et al., 2014).Distributed networks are designed

[1] *University Malaysia Sabah, Jalan UMS, Kota Kinabalu Saba h, Malaysia |kashif@ums.edu.my*
[2] *Umaru Musa Yar'adua University Katsina, Nigeria |Shamsuddeen.bala@umyu.edu.ng*
[3] *Umaru Musa Yar'adua University Katsina, Nigeria |abubakar.muazu@umyu.edu.ng*
[4] *Bayero University Kano, Kano Nigeria |ialawan.it@buk.edu.ng*

as integration of different components assembled together from different independent security domains (Radha& Reddy, 2012). Sensitive information access must be secured and private and the functionality of the system must be to the desired standard, with seamless operation process. Millions of RPs are using different IDPs for their SSO while others act as both IDP and RP (hybrid) at the same time (Vapen, Carlsson, Mahanti, & Shahmehri, 2016).

Internet access login is very essential in the contemporary World Wide Web, hence the need to have secure, well-functioning SSO configuration that has privacy to ascertain as well as the desired security for using one login to access different resources at any time while online, without malicious attack to the login credentials (J. Li et al., 2019)(Wassermann et al., 2019)(B. Li et al., 2004). Although many researchers have examined several aspects of SSO particularly in the areas of security, privacy, and functionality among others (e.g. Beer Mohamed, M. I., Hassan, M. F., Safdar, S., & Saleem, M. Q., 2019; Vapen, Carlsson, Mahanti, & Shahmehri, 2016; Heijmink, 2015; Science & Cao, 2014; David, Nascimento & Tonicelli, 2008 etc.), studies on authentication in Third-Party Identity Management (TIM) appear to be grossly inadequate. This research therefore aims to develop an algorithm geared towards redesigning the authentication process in TIM in order to eliminate the overhead in the authentication process for both IDPs and Hybrid Relying Parties (HRPs)

This paper therefore aims to develop an algorithm geared towards redesigning the authentication process in third-party identity management (TIM) in order to eliminate the overhead in the authentication process for both IDPs and (HRPs). Especially when user is authenticated for the first time there is no need for subsequent authentications, user credentials will be encrypted in one-way hashing algorithm (SHA2) (Beer Mohamed et al., 2019), user credentials will be use to validate subsequent logins by login directly into an RP with the stored credentials.

2 Review of Related Work

All the way through the design of our proposed algorithm previous related works were visited. Beer Mohamed, Hassan, Safdar, & Saleem (2019), proposed an adaptive security architectural model for federated identity management in cloud computing as Service Oriented Architecture (SOA) for software as a service (SaaS). Their architecture was implemented and tested in a large-scale identity enterprise computing environment, where they compared their model with a vendor security and security layer performance in which their model out performs the vendor security and the security layer performance. In their model algorithm was incorporated to encrypt credential using MD5 hashing algorithm and SHA2 but we choose SHA2 alone due to some drawbacks of MD5 as presented by (hashedout).

In 2016, Vapen, Carlsson, Mahanti and Shahmehri used landscape overview of which sites act as SSO RPs and how different Classes of RPs select their IDPs. They collected data sets using both manual identification and large-scale crawling which they used to identify current state of third-party identity management landscape but class-based analysis was only used to characterize the third-party IDPs landscape. They apply the following method. First, during data collection, they identify RP-IDP relationships and other site characteristics for selected sample websites. Second, they classify the sampled site along four dimensions (primary services, popularity segment, geographic region, byte/link volume). Third, they used hypothesis testing to identify website classes more likely to act as RPs. Use of popular sites as IDPs is dominant because these already have a large number of users with active accounts. In addition, in many cases, these sites may already access to large amounts of personal information that could help the RP improve their personalisation and service.

Jensen, Marsh, Dimitrakos, & Murayama (2015), adopted mathematical representation modelling and analysis of different requirements of federated identity management to develop a frame work that can formally express trust in federated identity management and how such expression can be used to analyse and evaluate trust qualitatively and quantitatively. In our work, we reduce the circuit of trust they applied in their modelling analysis as in section 3.

3 Architectural Model for User Authentication Process

The process of authenticating users in third-party identity management (TIM) needs modification, this leads to a new way of authenticating user once with a design of an improved authentication algorithm and development of smart security architectural model. The Smart security architectural model has three parts as in Figure 1 these three parts are; (1) user authentication services, (2) smart security engine, and (3) broker managing services.

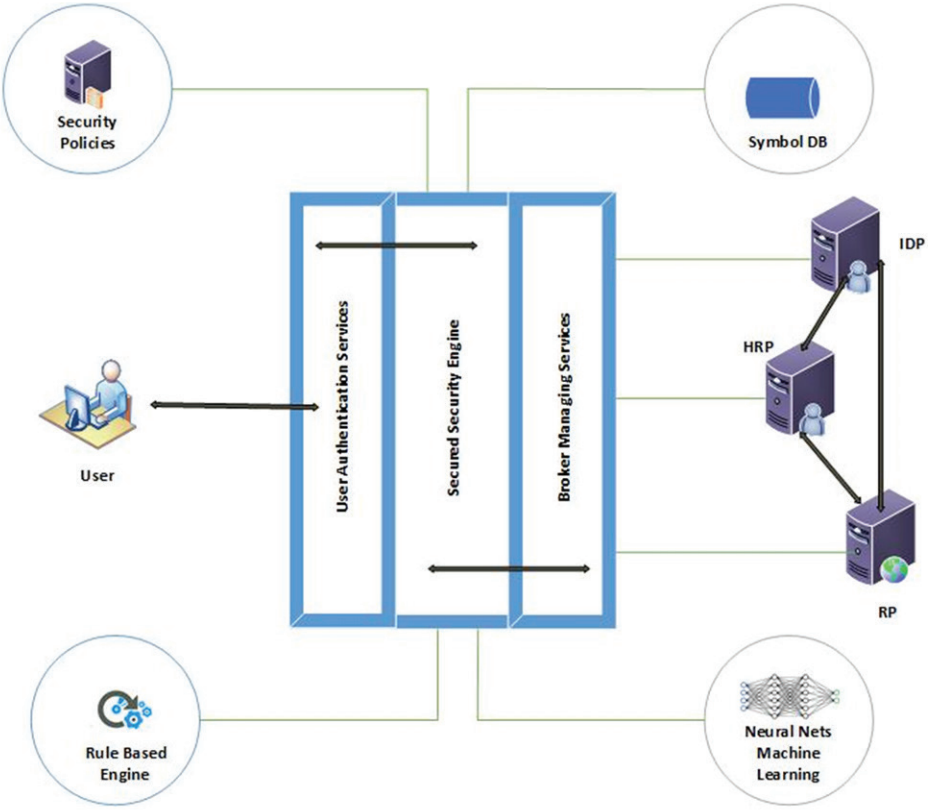


Figure 1: Proposed Model

User authentication services, this part of the Model is responsible for authenticating users, when they send their requests to login into an RP, user request is send to the IDP via broker managing services and the smart security engine is to validate the user credentials before forwarding it to RP for resource access by user.

The smart security engine (SSE) serves as a central point between user authentication services and broker managing services. When user send a request to login into RP whereby user will be authenticated by IDP via SSE, then SSE will allocate the user with an access token and record user credentials together with access token in symbol table. SSE encrypts user details in one-way encryption format using secured hashing algorithm version II (SHA2) for subsequent logins without any other authentication. Therefore henceforth user will be able to login into any relying party authenticated once with the login details of the IDP that authenticates the user.Broker managing services is an inter-mediator between the SSE and the IDP, HRP, and RP. Broker accept user request via User Managing Services and interact with either RP and IDP, or RP and HRP for authentication.

Mathematical trust relationship of third-party identity management for identity providers (IDPs) and hybrid relaying parties (HRPs) are modelled as: $u_i \in u_{f_i}$, $RP_i \in RP_{f_i}$, $HRP_i \in HRP_{f_i}$, $IDP_i \in IDP_{f_i}$, $f_i \in TIM$, $i \in \{1,2,.....,n\}$. $u_i \xleftrightarrow[FT]{DT:fi} RP_i$ user (u_i) has direct trust relationship (DT) with the Relaying Party (RP_i), and is fully trusted (FT) by the (RP_i); $u_i \xleftrightarrow[FT]{DT:fi} HRP_i$ user (u_i) has direct trust relationship (DT) with the HRP_i , and is fully trusted (FT) by the RP_i ; $u_i \xleftrightarrow[FT]{DT:fi} HRP_i$ Relying Party (u_i) has direct trust relationship (DT) with the HRP_i , and is fully trusted (FT) by the HRP_i ; $RP_i \xleftrightarrow[FT]{DT:fi} IDP_i$ Relying Party (RP_i) has direct trust relationship (DT) with the IDP_i , and is fully trusted (FT) by the as inspired by (Jensen et al., 2015).

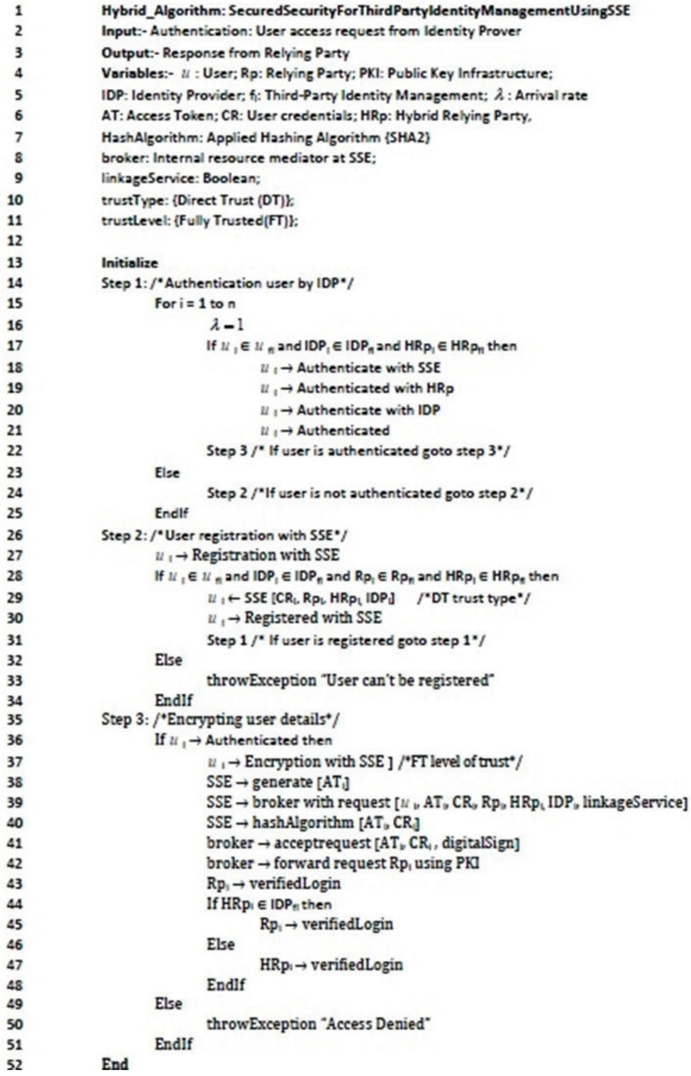
Thus, the circuit of trust (COT) is reduced to direct trust relationship (DT) only and the trust level is reduced to fully trusted (FT) only. In this research other level of trust, semi trusted (ST), not trusted (NT), and restricted but trusted (RT) were eliminated due the nature of the proposed architectural model, for the level of trust indirect trust (IT) is also eliminated according to what (Beer Mohamed et al., 2019) suggested. Trust relationship between User, RP, HRP, and IDP is expressed as:

$$\left(u_i \xleftrightarrow[FT]{DT:fi} RP_i\right)\left(RP_i \xleftrightarrow[FT]{DT:fi} IDP_i\right) = \left(u_i \xleftrightarrow[FT]{DT:fi} RP_i IDP_i\right) \quad (1)$$

$$\left(u_i \xleftrightarrow[FT]{DT:fi} HRP_i\right)\left(RP_i \xleftrightarrow[FT]{DT:fi} HRP_i\right) = \left(u_i \xleftrightarrow[FT]{DT:fi} RP_i HRP_i\right) \quad (2)$$

A Proposed Algorithm User Authentication Process

The proposed algorithm is designed in such a way that, when user want to access RP resources it will start with authentication step, i.e. step 1 if user is not registered by SSE user will not be authenticated. Therefore user should go to step2, registration step user will be registered in a symbol table and will be given an access token and directed to step 3, encryption step in this step user credential and access token will be encrypted using one-way hashing algorithm (SHA2) from then user details cannot be accessed unless when user want to login back for subsequent logins SSE will verify user details when the user entered his credentials to confirm the user access token for allowing user to access RP resources or HRP resources as the algorithm is designed to allow IDP and HRP to authenticate user only once i.e. for the first time, and IDP can also authenticate user to access HRP resources. Subsequent logins of user after authentication will be handled by checking user details encrypted if the access token of user is valid for the authenticating party i.e. IDP or HRP user is granted to login as illustrated in Figure 2.



```
Hybrid_Algorithm: SecuredSecurityForThirdPartyIdentityManagementUsingSSE
Input:- Authentication: User access request from Identity Prover
Output:- Response from Relying Party
Variables:- $u$ : User; Rp: Relying Party; PKI: Public Key Infrastructure;
IDP: Identity Provider; $f_i$: Third-Party Identity Management; $\lambda$ : Arrival rate
AT: Access Token; CR: User credentials; HRp: Hybrid Relying Party,
HashAlgorithm: Applied Hashing Algorithm {SHA2}
broker: Internal resource mediator at SSE;
linkageService: Boolean;
trustType: {Direct Trust (DT)};
trustLevel: {Fully Trusted(FT)};

Initialize
Step 1: /*Authentication user by IDP*/
        For i = 1 to n
                $\lambda - 1$
                If $u_i \in u_n$ and $IDP_i \in IDP_n$ and $HRp_i \in HRp_n$ then
                        $u_i \rightarrow$ Authenticate with SSE
                        $u_i \rightarrow$ Authenticated with HRp
                        $u_i \rightarrow$ Authenticate with IDP
                        $u_i \rightarrow$ Authenticated
                Step 3 /* If user is authenticated goto step 3*/
        Else
                Step 2 /*If user is not authenticated goto step 2*/
        EndIf
Step 2: /*User registration with SSE*/
        $u_i \rightarrow$ Registration with SSE
        If $u_i \in u_n$ and $IDP_i \in IDP_n$ and $Rp_i \in Rp_n$ and $HRp_i \in HRp_n$ then
                $u_i \leftarrow$ SSE [$CR_i$, $Rp_i$, $HRp_i$ $IDP_i$]     /*DT trust type*/
                $u_i \rightarrow$ Registered with SSE
                Step 1 /* If user is registered goto step 1*/
        Else
                throwException "User can't be registered"
        EndIf
Step 3: /*Encrypting user details*/
        If $u_i \rightarrow$ Authenticated then
                $u_i \rightarrow$ Encryption with SSE ] /*FT level of trust*/
                SSE $\rightarrow$ generate [$AT_i$]
                SSE $\rightarrow$ broker with request [$u_i$, $AT_i$, $CR_i$, $Rp_i$, $HRp_i$ $IDP_i$, linkageService]
                SSE $\rightarrow$ hashAlgorithm [$AT_i$, $CR_i$]
                broker $\rightarrow$ acceptrequest [$AT_i$, $CR_i$ , digitalSign]
                broker $\rightarrow$ forward request $Rp_i$ using PKI
                $Rp_i \rightarrow$ verifiedLogin
                If $HRp_i \in IDP_n$ then
                        $Rp_i \rightarrow$ verifiedLogin
                Else
                        $HRp_i \rightarrow$ verifiedLogin
                EndIf
        Else
                throwException "Access Denied"
        EndIf
End
```

Figure 2: Proposed Algorithm

4 Implementation

The proposed algorithm in this research was implemented, where an exponential distribution was invoked for optimal performance of the algorithm operation. Random arrival time (t = λ) of users was used and authentication time (Ta) was compared against response time (Tr) for different arrival time to compare Ta of IDP and HRP against Tr of RP for users. The aim of reducing multiple authentication of user during login into RP resources by IDP and HRP for random users in order to know how they arrive and the relationship of the authentication time of the IDP or HRP and the response time of the RP. Random real values were generated for the authentication time for random users and their corresponding response time.

The arrival of users during authentication is random, there is need to use Exponential Distribution as inspired by (Haq et al., 2019)(Gupta et al., 2010).

Arrival pattern will be: 0≤ t_(0)<t_1<t_(2)<⋯ <t_n (1)

The stating time for queuing is assume to start at t = 0. The random variables are expressed as:

τ_k= t_k- t_(k-1, (k =1,2,3,…………….))τ_k=t_k-t_(k-1,(k=1,2,3,…………….)) (2)

Therefore the exponential pattern is: A[t]= 1-e^(-λt) (3)

The result in respect with λ = 1 ms is shown in Table 1. The result is presented graphically as in Figure 3 result was generated from random real values from 0 to 1.

Table 1: Proposed Algorithm Result

Users	Response Time (Seconds)	Authentication Time (Seconds)	λ (Mili-Seconds)
User1	0.0047835	0.0512164	1
User2	0.0318328	0.4579892	1
User3	0.0344461	0.646313	1
User4	0.0357117	0.793975	1
User5	0.0364413	0.807531	1

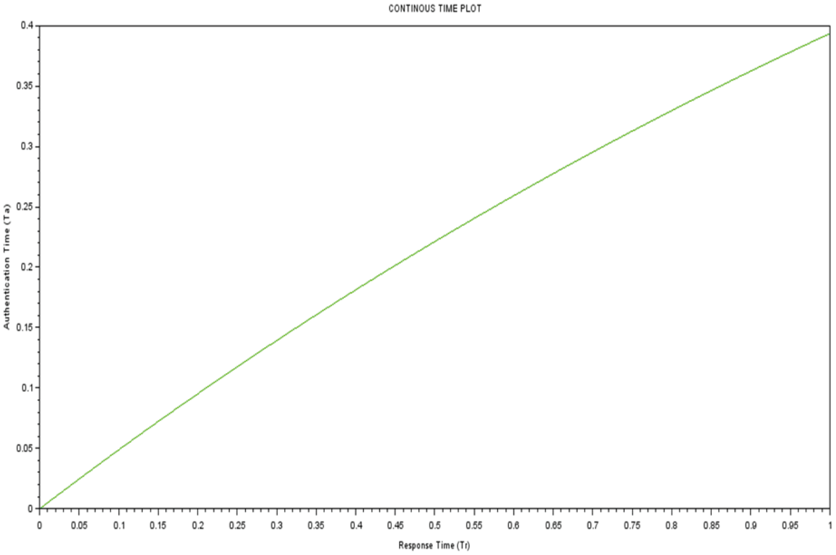


Figure 3: Proposed Algorithm I Result with = 1 ms

To know the difference of result plotted for authentication time against response time with respect to λ = 0.5 ms and λ = 0.1 ms for the proposed algorithms, their results is compared in figure 4.3 to showcase their difference. Therefore the arrival rate determines the authentication time of the Identity Providers (IDP) and Hybrid Relying Party (HRP) relationship with response time of Relying Parties (RP). Hence the high the arrival rate a better performance is recorded, whereas the lower the arrival rate a lower performance is recorded

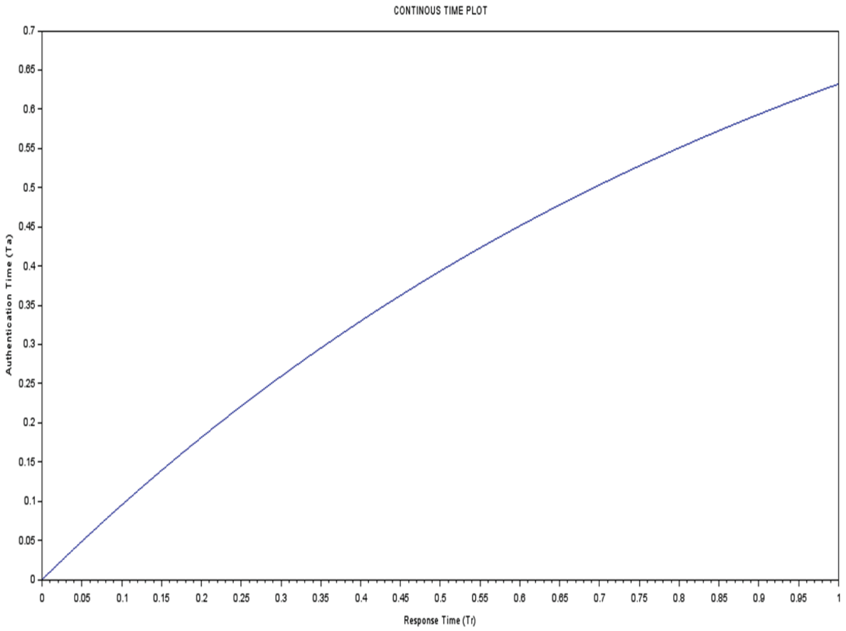


Figure 4: Proposed Algorithm II Result with λ = 0.5 ms

5 Conclusion

User authentication for Third-Party Identity Management is a phenomenon whereby user needs authentication from IDP and HRP for each login into RP resources. This paper have presented improved authentication process for third-party identity management in which the overhead of authenticating user at each login to access RP resources by IDP and HRP is reduced to single authentication as in the proposed algorithm. The user credentials are been encrypted using one-way hashing algorithm (SHA2) as depicted in the proposed model.

References

[1] Armando, A., Carbone, R., Compagna, L., Cuellar, J., & Tobarra, L. (2008). Formal analysis of SAML 2.0 web browser single sign-on: Breaking the SAML-based single sign-on for google apps. Proceedings of the ACM Conference on Computer and Communications Security, 1–9. https://doi.org/10.1145/1456396.1456397

[2] Beer Mohamed, M. I., Hassan, M. F., Safdar, S., & Saleem, M. Q. (2019). Adaptive security architectural model for protecting identity federation in service oriented computing. Journal of King Saud University - Computer and Information Sciences, xxxx. https://doi.org/10.1016/j.jksuci.2019.03.004

[3] David, B. M., Nascimento, A. C. a, & Tonicelli, R. (2008). A Framework for Secure

[4] Elgendy, N., & Elragal, A. (2018). Big Data Analytics : A Literature Review Paper Big Data Analytics : A Literature Review Paper. September 2014, 214–227. https://doi.org/10.1007/978-3-319-08976-8

[5] Gupta, A. K., Zeng, W. Bin, & Wu, Y. (2010). Probability and statistical models:

[6] Haq, M. A. ul, Usman, R. M., Hashmi, S., & Al-Omeri, A. I. (2019). The Marshall-Olkin length-biased exponential distribution and its applications. Journal of King Saud University - Science, 31(2), 246–251. https://doi.org/10.1016/j.jksus.2017.09.006

[7] Jensen, C. D., Marsh, S., Dimitrakos, T., & Murayama, Y. (2015). Trust management IX: 9th IFIP WG 11.11 international conference, IFIPTM 2015 Hamburg, Germany, may 26-28, 2015 proceedings. IFIP Advances in Information and Communication Technology, 454(December 2016). https://doi.org/10.1007/978-3-319-18491-3

[8] Li, B., Ge, S., Wo, T. Y., & Ma, D. F. (2004). Research and implementation of single sign-on mechanism for ASP pattern. Grid and Cooperative Computing Gcc 2004, Proceedings, 3251(2001), 161–166.

[9] Vapen, A., Carlsson, N., Mahanti, A., & Shahmehri, N. (2016). A look at the third-party identity management landscape. IEEE Internet Computing, 20(2), 18–25. https://doi.org/10.1109/MIC.2016.38

[10] Vapen, A., Carlsson, N., Mahanti, A., & Shahmehri, N. (2014). Third-party identity management usage on the web. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8362 LNCS, 151–162. https://doi.org/10.1007/978-3-319-04918-2_15