ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Novel Approach for Enhanced Single Sign-On Authentication to Provide Better Security

Garima Kumrawat[1], Amit Agrawal[2]

M. Tech. Student, Department of CSE, Medi-Caps Institute of Science and Technology, Indore, India[1]

Asst. Professor, Department of CSE, Medi-Caps Institute of Technology and Management, Indore, India[2]

ABSTRACT: Today's Internet world, mostly internet services are based on the single server system and use the password identity authentication to offer application service for the users; in this the user must enter the credentials (ID and password), before requesting to login in any application service. It is enormously hard for any user to remember so many different IDs and passwords, so the single sign-on (SSO) scheme has been proposed by providing Single-tier authentication which is relies on username and password for accessing the registered services but it is not sufficient to secure from some well-known attacks like brute-force attack, replay attacks, etc. so a solution to this issue; we come up with Two-factor authentication using single- sign on access of registered services. Two-factor authentication security relies on the username and password as well Smart Card. The main focus of this paper is to propose Single Sign- on (SSO) based Smart Card authentication technique.

KEYWORDS: Single Sign-On, Security and Authentication, Encryption and Decryption, Smart Card.

I. INTRODUCTION

In traditional web application during creation of the account we suppose to enter user name and password with some security questions. This data get saved in database. Next time when user wants to access his account he needs to specify his login name and password. Entered login name and password get compared with one saved in database. If entered login name and password matches with database then only user will get access to his web application. Here purpose of security questions is to retrieve the password when you forget. But problem of this system is anyone can steal the password.

For making more secure authentication model, the researcher came up with two-tier authentication (also known as two-factor authentication). This new technique leads to less probability of breaking the authentication system which provides more security. The two-tier authentication technique uses two or more verification process to verify the user.

II. SINGLE-SIGN-ON

SSO can be defined as a user experience of logging in just once and being able to navigate across many applications seamlessly without a need to enter credentials for each application [1]. It is very common for organizations to have many applications running to take care of different business functions. SSO makes it easy for the users to login once and be able to access all the applications they can, reducingthe need for users to remember a plethora of logins and passwords.

The following is a brief description of a few important concepts of SSO.

- **Authentication:** The process of verifying the user's identity, making sure that the user is who he claims to be. This can be based on login & password combination or Smart card, biometrics, etc.
- **Authorization:** The process of verifying whether a user is privileged to access a particular resource.
- **Credentials:** Credentials are the details provided by a user during the process of authentication into an application. They can be login and password, fingerprint, smart card etc.
- **Domain:** A domain is a logical group in an organization with a unique name that is the part of host names used on the intranet/Internet. For example, abc.com is the domain name in myhost.abc.com.

- **Protected Resource:** It is a resource the access of which is not open to everyone. A user needs to go through authentication and authorization before accessing a protected resource. It can be a URL on the Internet or intranet, a client to an application, a folder on a server, etc.
- **Cookie:** A cookie is a ticket given to a user's browser as a result of successful authentication and it contains data to indicate authentication and authorization information. The actual contents of a cookie may vary depending on the application. After having a cookie, if the user browses to a different application that is a part of SSO, the cookie is presented by the browser to the application in lieu of credentials, for directly logging into the application. Then for accessing the resources if the user is authorized, he will be able to do so.

There are two types of cookies.

- **Per session cookie:** The cookie is retained in volatile memory of the user's computer and is valid only till the end of the current session. As soon as browser is closed, the cookie is destroyed.
- **Persistent cookie:** When you check the box for "Remember my password" or "Log me in automatically "or a similar one in the login page of a web site then a cookie is stored on your hard drive. This is a persistent cookie and the server that sets the cookie specifies its life. So, its contents are not destroyed when the browser is closed and will remain available between sessions, till expiry.

Single sign on has currently become referred to as reduced sign-on (RSO) since over one style of authentication mechanism is employed per enterprise risk models.

For example, in an enterprise exploitation SSO [2] computer code, the user logs on with their id andPassword. This gains them access to low risk info and multiple applications like the enterprise portal. However, once the user tries to access higher risk applications and data, sort of a payroll system, the only sign up computer code needs them to use a stronger kind of authentication.

This could embrace digital certificates, security tokens, good cards, bioscience or combos then cassowary.

III. TWO-FACTOR AUTHENTICATION

Two-factor authentication has emerged as an alternative way to improve security by requiring the user to provide more than one authentication factor, as opposed to only a password. The most commonly used authentication factors in two-factor authentication are [3]:

- Something user know (as a password).
- Something user have (as a secure device with a secret key).

There are three major techniques for authentication:

- **Password based authentication:** The oldest and simplest method of authentication for accessing the resources in which user has to provide a password which is only known to the user.
- **Challenge-Response authentication:** In this technique, users have to prove that they know the secret without sending it to the service provider. The challenge is any time stamp value which is sent by the service provider and user applies a function on challenge to send response to the service provider.
- **Zero-Knowledge authentication:** In this technique, the user does not disclose anything that might take a chance to the confidentiality of the secret. The user proves to the service provider that they know the secret without disclosing it to the service provider. User and service provider exchanges some messages to each other for authentication. After exchanging these messages, service provider somehow knows that the user knows the secret.

Single-tier authentication can be implemented using one these techniques, but still single-tier authentication is not enoughto secure the resources of the service providers because this technique is suffering from many security attacks like, brute-force attack, insider attacks etc. For making more secure authentication model, the researcher came up with two-tier authentication (also known as two-factor authentication). This new technique leads to less probability of breaking the authentication system which provides more security. Thetwo-tierauthentication technique uses two or more verification process to verify the user.

By taking the two factors in the similar authentication protocol together possibly will increase the security because the intruder needs to break two protections.

In this way the Smart card based authentication is most suitable and commonly used two-factor authentication mechanisms.

The most common example of two-factor authentication is bank ATM, or debit cards. One factor is the ATM card ("something the user has"). The second factor is the PIN of the ATM ("something the user knows") [3].

A smart-card based password authentication scheme includes a server and a client. At first, in registration phase server generates the smart card which is containing the user ID and initial password to the client and for every client thisphase is performs only once. Later on, in login phase client sends authentication request which containing user name and password, server verifies this and also asks for additional details. After entered the required details user authentication is verifies if it is correct user can successfully access the applications of servers. In this phase, various kinds of attacks are possible in the communication channel between client and server. Attackers can eavesdrop messages and even modify, insert or remove messages into thechannel.

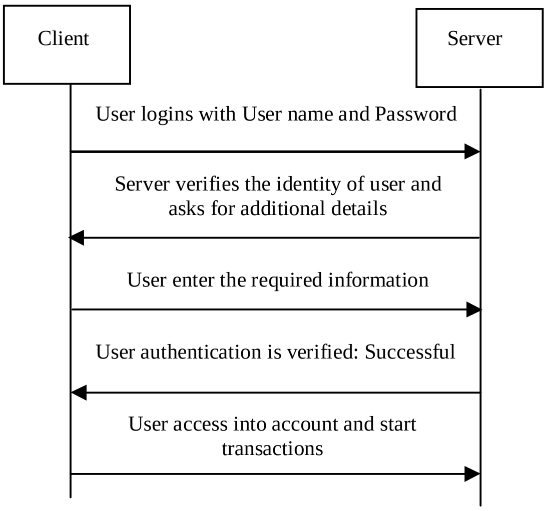
Client
Server
User logins with User name and Password
Server verifies the identity of user and asks for additional details
User enter the required information
User authentication is verified: Successful
User access into account and start transactions

Fig. 1: Two-Factor Authentication Process

Mostly all the websites and online services are now-a-days implementing multi-step authentication to provide security to their customers. More recently, an increasing number of service providers like Google, Face book, Drop box, Twitter, LinkedIn etc. have also begun to provide their users with the option of enabling Two-factor authentication; this is motivated by the increase in number of hackingpasswords.

There are various authentication techniques included a user's password, personal information numbers (PINs), digital certificates using public key infrastructure (PKI), one-time passwords (OTP) or other type of 'tokens', biometric identification, and other as well as various authentication factors like shared secrets, tokens and biometrics are available to provide the secured authentication.

In this paper we proposed the SSO with smart card authentication technique where we use a pen drive smart card which is easy to use and convenient for security purpose.

IV. RELATED WORK

In [2] authorsdefined that proposed method can increase the protection for the card. Authentication is only true at present point in time and its strong point is also depend on other external factors, because of this there is no form of authentication is up to the mark. Whether the authentication is enough for the business need; the user’s confidentiality is improved, the user controls any release of personal information.In [3] authors describes the authentication factors of two factor authentication mechanism and also gives the description of the techniques of the authentication and the basic difference between single tier and multi-tier (two factor) authentication. In [4]authors established a unified database of persons concluded the single sign-on project construction. They combined the isolated system that is suitable for the customer and also for the manager. For achieving the synchronization of information among databases in the construction of Digital Campus, Enterprise Service Bus was also used. In [5] authorsexplained the technical requirements and functions of an SSO application that would run on the existing bank application. The primary concern of the banking industry is to secure transaction and authentication through additional research and effective data and information security techniques.In [6] authors explained that Single-sign-on is a new method thereby increases the network's usability and at the same time centralizes the organization of relevant system parameters. Unfortunately, they show that Ren's scheme is suffering from unforgeable attack they proposed in this paper. In this, without a legal ID anyone can clear the verification phase. Finally, they give the equivalent revise. In computer networks Ren's scheme was very well-organized Single-sign-on solution for authentication. So, it is a kind of open problem to improve Ren's scheme and make it protected in the standard model. In[7] authors used trusted computing platform for performing the operation like user authentication, data verification. In their system they use three ways protection schemes in which first used Diffie Hell-man algorithms for key exchange algorithms for the AES encryption algorithms. Digital signature is responsible for the authentication and used SHA as a hashing algorithm for computing the signature and AES as encryption algorithms.Authors of this paper proposed and implemented digital signature algorithm for authentication purpose and used AES algorithm for encryption of data. So, they observed their system is more secure than previous system. In [8] authors provide security using the key management and encryption technology. Encryption basically is the method to turn information into unintelligible format using different algorithm. The key management is a method with which uses special encrypted keys to access all the data. This paper shows how data is encrypted and keys are generated for application using AES algorithm, also says only the secret key would be encrypted with this algorithm and the encryption and decryption process will be more efficient and needless to say it would be less time consuming and memory deficient.

V. PROPOSED ARCHITECTURE OF SINGLE SIGN- ON WITH SMART CARD AUTHENTICATION TECHNIQUE

The proposed architecture for SSO with smart card authentication a new system is prepared using the traditionally available SSO techniques.

Proposed scheme uses two phases of authentication for authenticating the user. The first phase of authentication is done by username and password, and the second phase is using the pen drive as smart card for authentication.The proposed work defined an identification base Single Sign-On (SSO) determination for organizations to improve the protection.

The proposed approachwill use smart card as identification based authentication mechanism while keeping underlying architecture of Single Sign-On (SSO) as base.

As current technology changes, this is expecting these smart cards to turn into more crucial to data security in day-to-day life. The rising need for secrecy and advanced data security is indicative of amarket shift in how people protect themselves when visiting websites on the internet.

The organization of traditional methodologies for obtaining Single Sign-on with smart card is given using figure-2. The architecture mentioned above contains four main Components-

- Client
- Application Server
- SSO Server
- Pen Drive(used as smart card)

The main components of proposed architecture are described as under-

(i) Client - A client send authentication request through client browser to the application server (Client Browser is a software application for retrieving, presenting and traversing information resources on the World Wide Web (WWW)).

(ii) Application Server- Application server is a program that generates & transmits responses to client requests for web responses usually web pages (HTML documents, linked objects, images etc).

(iii) SSO Server- SSO server checks for the valid cookie in the client browser & if it exists then allows user to access the services of application server without going through the normal authentication process.

(iv) Pen Drive: Pen drive is a mass storage device which is used to storethe data like files, movies, songs etc.

The working process completed in three sub parts Registration, Login & SSO phase.

- **Registration Phase**: In registration phase firstly user send the registration request which containing user name, password with an USB option to the SSO server. After this server generate and send smart card which is saved in pen drive.At this stage encryption is performed.

- **Login phase:**After registration in login phase, user fills user name and Password thensystems checks user name and password in database are same, if match is found then server check the smart card on user disk if smart card is found server decrypt smart card and compare it to server copy, if match found then authentication is successful and server generate a cookie in client browser for other application access.

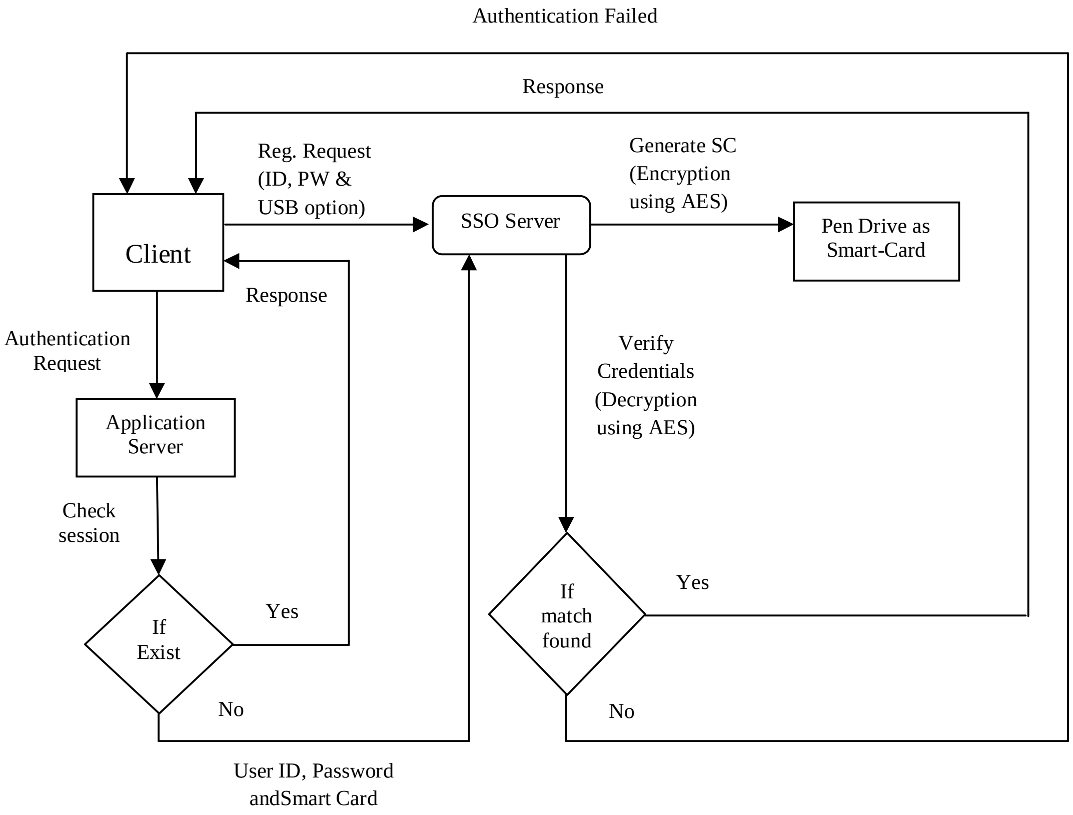

Fig.2: Proposed Architecture of Single Sign- On with smart card authentication technique

- **SSO Phase:**We combining this two factor authentication mechanism with the SSO technique for this user send request for application access, if user already logged in, in other application then server check the session, if it is not null and valid then server provides application access to the user otherwise user again need to perform login process. For all requested applications this steps performs repetitively.

VI. PROPOSED ALGORITHM

There are different types of terminologies used in algorithm to describe the implementation of proposed system. The flow of a system divided into two phases, one is ‘Key Generation ‘and second is ‘To Encrypt and To Decrypt’.

A. Encryption Algorithm

(i) Key Generation

The following steps are used to generate the key

- Generate the AES key using Key Generator.
- Initialize the key size.
- Generate the secret key.

(ii) To Encrypt and To Decrypt

- Create a cipher by specifying the following parameters //Algorithm name -AES

- Initialize the Cipher for Encryption.
- Encrypt the file.//Declare /Initialize file
  //Convert the input array to file
  //Encrypt the byte using do Final method
- Calculate the encryption time.
- Decrypt the file. //Initialize a new instance of cipher.
  //Decrypt the cipher bytes using do Final method.
- Calculate the Decryption time.

B. Algorithm for pen drive's security

```
Algorithm String check Removable ()
begin
fsv = FileSystemView.getFileSystemView();
// fsv is an object of file system view
        File [ ] roots = fsv.getRoots ();
        For i=1 to root .length
        {
        Write root [i]
// print all home directories
        }
Write (fsv.getHomeDirectory());
File [] f = File.ListRoots();
For i =1 to f.length do
{
If (fsv.getSystemDisplayName f[i]) = "pid_0024"
//0024 is my pen drive's serial number
Than
Return f[i]
else
Return "not found";
}
end
```

The given algorithm is about the pen drive's security where by using the unique serial number of the pen drive we can secured it from the smart card stolen attack. It is necessity condition that with the first factor of authentication (user name and user id) user has the correct pen drive which we used as second factor authentication so he can get the access otherwise the result shows not found the pen drive.

VII. SIMULATION AND RESUTS

Table 1 shown the proposed method prevent from various attacks on SSO application.Like password based Attack, Impersonation Attack, Against DOS Attack, Replay Attack, Credential Privacy Attack, Smart Card Stolen Attack. Proposed system is defining about the use of smart card (pen drive as smart card) mechanism which is protecting the existing system to this given attacks.

TABLE 1
Prevention from various attacks

Attacks	Bio-Smart Card [12]	Bio-Smart Card [15]	Smart Card [14]	Our Scheme
Password based Attack	Yes	No	Yes	Yes
Impersonation Attack	No	Yes	N.P	Yes
Against DOS Attack	Yes	Yes	No	Yes
Replay Attack	Yes	No	Yes	Yes
Credential Privacy Attack	No	Yes	N.P	Yes
Smart Card Stolen Attack	Yes	No	No	Yes

The proposed approach is compared with OTP & Finger Print recognition systems used for authentication on the basis of some dependency parameters like extra hardware needs, mobile network and failure due to third party mentioned on Table2. The value 1 represents 'YES' & value 0 represents 'NO'. In this table this is clearly shown that like OTP and Finger Print recognition systems ,proposed approach is uses the extra hardware (pen drive) but it is not dependent on mobile network and its results is also not dependent on any third party.

TABLE 2
Comparison of Proposed Approach

Dependency Parameter	OTP	Finger Print	Proposed Approach
Extra Hardware	1	1	1
Mobile Network	1	0	0
Failure due to third party	1	1	0

Figure 3 shows, the storage comparison of the proposed scheme with the relevant user authentication based on smart card. In order to show the comparison the X axis containsthe server storage and mass storage and Y axis contains the number of bits. As per shown in figure that proposed scheme uses additional hardware (pen drive) so the storage is more as compared to the existing method.

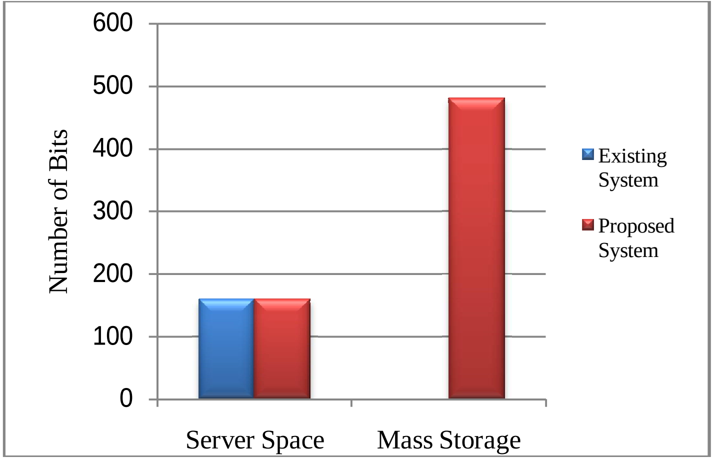

Fig. 3: Storage comparison of the proposed scheme

Figure 4 shows the encryption and decryption time of the user's information according to the different key size values like AES-128,AES-192 and AES-256.Here we take x axis as results of encryption and decryption and y axis shows the time (ms).

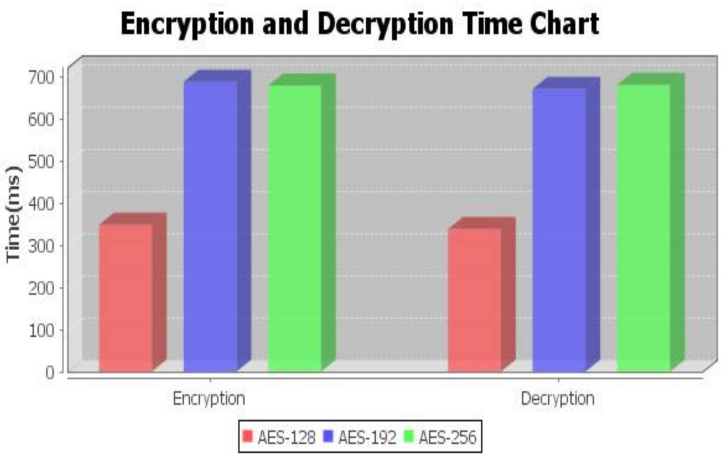

Fig. 4: Encryption and Decryption time Chart

VIII. CONCLUSION

The Proposed approach mentioned in this paper demonstrates a new authentication approach for authentication based on Smart card in the Single Sign- On application platform. Proposed approach gives better result compare to other methods. Thus we present a new idea for security.

This paper define a very convenient and easy to use approach which is provide security and user authentication, we use pen drive as smart card which is currently used so much and it is easy to use and also very convenient.

Introducing positive identification the protocol can authenticates the positive identification solely. Planned approach can use challenge- response technique to make sure the authentication of each server and therefore the positive identification. As trendy technology evolves, we tend to totally expect these hybrid sensible Cards to become a lot of essential to knowledge security in day-after-day life. The growing would like for obscurity and advanced knowledge security is indicative of a market shift in however users protect themselves once visiting websites on the net.

REFERENCES

1. Chin-Chen Chang, “A secure single mechanism for distributed computer networks,” IEEE Trans. On Industrial Electronics, vol. 59, no. 1, Jan 2012.
2. David J. Boyd,"Single Sign-On to the Web with an EMV Card",IEEE, 2008.
3. QiongPu“An Improved Two-factor Authentication Protocol”Second International Conference on Multimedia and Information Technology, 2010.
4. Jian Hu, Qizhi Sun, Hongping Chen,” Application of Single Sign-On (SSO) in Digital Campus”,IEEE 2010.
5. Sahana K. Bhosale,"Architecture of a Single Sign on (SSO) for Internet Banking", IET International Conference on Wireless, Mobile and Multimedia Networks, 2008.
6. Jianhong Zhang and XueLiu,"On the Security of An Identity-based Single-sign-on Scheme”,IEEE, 2010.
7. RituPahal and Vikaskumar “ Efficient Implementation of AES”,International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 7, pp. 290-295 July 2013
8. Hrushikesh S. Deshpande, Kailash J. Karande, Altaaf O. Mulani “Efficient Implementation of AES Algorithm on FPGA” Bimonthly International Journal PISER 11, Vol.02, Issue: January-February; Pages-170-175 ,2014 PISER Journal www.piserjournal.org
9. Divyajyoti and Ram kumar “Security Analysis and Performance Evaluation of an Enhanced Two-Factor Authenticated Scheme”International Journal of Computer Applications (0975 – 8887) Volume101–No.8, September2014.
10. Federal Financial Institutions Examination Council. Authentication in an internet banking environment. 2011.
11. Emiliano De Cristofaro, Honglu Du, JulienFreudiger, Greg Norcie, “A Comparative Usability Study of Two-Factor Authentication”, Cornell University Library, 31 January 2014.
12. A.K. Das, “Analysis and Improvement on an efficient biometric-based remote user authentication scheme using smart cards”, IET Information Security, vol. 5, no. 3, pp. 541–552, 2011.

13. Juan E. Tapiador, Julio C. Hernandez-Castro, Pedro Peris-Lopez, John A. Clark1 “Cryptanalysis of Song’s advanced smart card based password authentication protocol”, 11 Nov 2011.
14. W. Juang, S. Chen, and H. Liaw, “Robust and efficient password authentication key agreement using smart cards”, IEEE Trans. Ind. Electron, 15(6): 2551-2556, 2008.
15. YounghwaAn, “Security Analysis and enhancement of an efficient biometric-based remote user authentication scheme using smart cards”, Journal of Biomedicine and Biotechnology, 2012.