Research Article

International Journal of Advanced Computer Research, Vol 6(23)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2016.623031

The implementation and investigation of securing web applications upon multi-platform for a single sign-on functionality

Hsien-Yu Lee* **and Nai-Jian Wang**
Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan

Received: 19-February-2016; Revised: 18-March-2016; Accepted: 20-March-2016

Abstract
Nowadays, the world is moving toward mobilized communities as the development of internet and web applications. Almost all of the daily activities and transactions can be done through the internet. Web applications become trends as e-business and e-commerce systems continue to make our lives easier and better without our noticing. These web applications were developed from various frameworks, programming languages and platforms etc. over the internet. Computer technology is a time saving and quality improving revolution. When the enterprise will build up the vision of computer digitalization, i.e. hosting e-Enterprise engineering, cloud platform or information systems integration, etc. Under the web world, the single sign-on (SSO) concept was invented as problem-solving method about one login as you go authorized systems. In other words, web securities are confronting some challenges under the networked era of the emergency web. Therefore the SSO functionality based on multiple platforms and web enabling technologies is put forward and it also secures web applications developed from diverse programming. The proposed method of secure login utility is created as an obvious solution to the general functionality of SSO. Hereby, we also will reveal two application instances of the secure login utility to implement the idea of SSO realized in the enterprise systems.

Keywords
Security, Single sign-on, Web programming, MD5.

1.Introduction
Single sign-on (SSO) is a session or user authentication process that permits a user to enter one name and password in order to access multiple applications. To verify that the users for all applications, they have been given the rights and eliminate further prompts when they are in a particular session during the process of switching applications [4]. Single sign-on (SSO) is a property of access control of multiple related sources, but independent software systems. Based on this property, a user logs in with a single ID and password to obtain access to a connected system or the other systems without having to use a different user name or password. In [5], what are the benefits of SSO? The benefits of SSO apply to many areas: 1) User experience: the most obvious benefit is that users can move between services securely and continuously without having to specify their credentials every time.

*Author for correspondence

2) Security: provide the user credentials directly to the central SSO server, not the actual service that the user attempts to access and save, 3) Resource savings: IT administrators can save their time and resources with a central web access management services. To comprehend Enterprise Single Sign-On (SSO) [6], it is useful today to observe the three types of Single Sign-On services available: Windows integrated, extranet (web SSO), and an internal network (Server-based Intranet). Enterprise Single Sign-On provides services to store and transmit encrypted user credentials across the local and global internet. SSO always stores the credentials in the database. Because SSO provides a generic single sign-on solution, applications and adapters can use SSO to safely store and transmit user credentials across a variety of environments. Users do not always remember different credentials/passcodes for different applications/platforms. Therefore, we proposed the solution focused on web SSO applied upon a multi-platform method. In 1991, MD5 message-digest algorithm was designed by Ronald Rivest to replace an earlier hash function, MD4 in 1990 [1], [2]. The MD5 message-digest algorithm is widely used a cryptographic hash function producing

a 128-bit (16-byte) hash value, typically expressed as a 32-bit hexadecimal numbers in text format. MD5 has been used for a variety of cryptographic applications, and is also commonly used to verify data integrity [13]. In the following section, we are going to use this concept to propose the method of Secured Login Utility (SLU) <Universal Authenticated Key Generator, Captured User IP Address> and implement these applications/components in Java, .Net, PHP and BCD WebSmart ILE, about IBM As/400 Web System, and so on.

The key issue we are concerned (considered) is: Single Sign-On, it means that users can login only once and access to multiple functionality websites. Privacy, resources, integrity and segregation belonging to one user cannot be accessed by unauthorized users, cannot be tampered during transfer, and deeply considering about both global and local resource usage rules. Upon this key issue, we simply and easily adopt MD5 [2] message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number (stored in the field of AUTKEY(32)). We realized the Secure Login Utility – Universal Authenticated Key Generator by using Java and AS/400 CL/RPG. The utility will create a unique, authenticated key (stored in AUTKEY (32)) based on the MD5 algorithm in every real-time login action, and the server will also automatically capture this user's unique IP address (i.e. 216.28.219.238).

2.Objectives–computer digitalization

During the past two decades, in virtue of the web has evolved into a global environment, addressing applications that range from simple, small-scale to complex large-scale enterprise applications distributed over the internet. Enterprises and companies are using the web to do business processes for their employees, to communicate with their partners and vendors, to integrate their back-end databases and information systems, and to perform all kinds of e-Commerce transactions. The most important one of the key benefits is that the programs, softwares, systems, and platforms will be well-maintained. The enterprise adopted computer technologies before the past three decades. Since then, the enterprise has gone step by step to apply Customer Relationship Management (CRM) and Supply Chain Management (SCM) systems, obtaining Electronic Data Interchange (EDI), Office Automation (OA), internet, Engineering and now Cloud Engineering, i.e. e-Commerce, e-Business, e-Marketplace, e-ERP and other information systems. And totally use computer to handle all purchasing and contracting business. The enterprise's digitalization that connects administrative sections into the ERP system, e-Commerce systems and information systems and so on covers all kinds of use in a company. Therefore, there is an integration request between these enterprise information systems. In other words, these systems confront a challenge about a major authorization processing problem under the networked era of the emergency web. Hereby, we proposed the solution focused on web SSO applied upon a multi-platform method - Secure Login Utility.

3.Designs and implementations for a single sign-on functionality

3.1The algorithm for secure login utility

In *Figure 1*, we illustrate the algorithm of the work and it for Secure Login Utility is depicted in order from top to bottom as below.

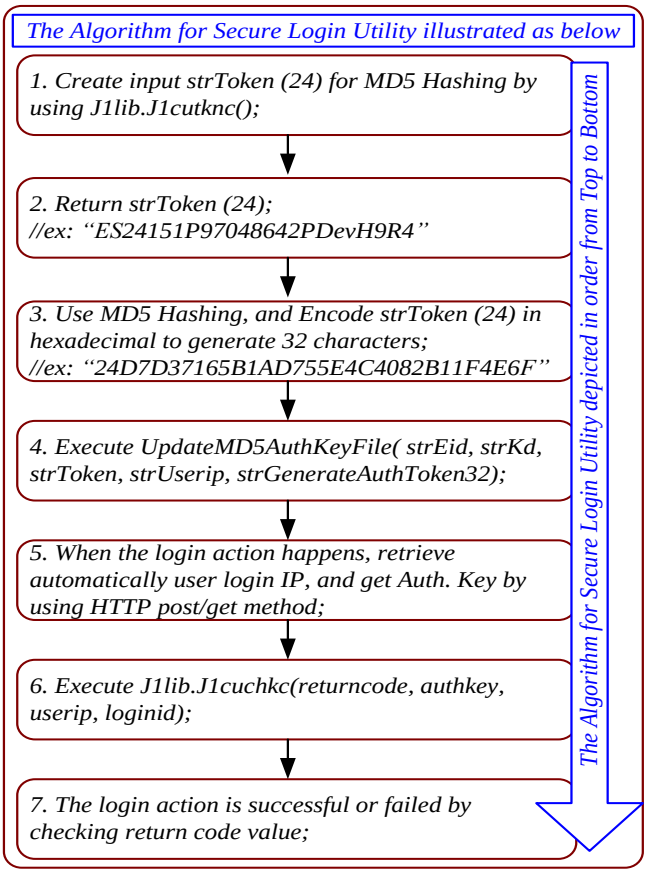


Figure 1 An illustration of the algorithm for secure login utility

3.2The secure login utility-universal authenticated key generator

We realized the Secure Login Utility – Universal Authenticated Key Generator by using Java and AS/400 CL/RPG. The utility will create a unique, authenticated key (stored in AUTKEY (32)) based on the MD5 algorithm in every real-time login action, and In Appendix's *Figure 8* outlined the implementation sample codes for Secure Login Utility - Universal Authenticated Key Generator by using Java and AS/400 CL/RPG program.

3.3Captured the user's IP address automatically

The server will also automatically capture this user's unique IP address (i.e. 65.216.158.152). According to the combined authorizing and auditing of both a unique, authenticated key and a unique IP address, we will secure all of login users until then logout systems. Although the IP address can be tampered by Hijacking during login, the generated authenticated key cannot be modified.

3.4Designed table SQL layout

Hereby, we provide the designed table SQL layout, detailed in *Figure 2*.

```
--   Version:                 V7R1M0 100423 ------------  AS/400 table SQL layout
--   Generated on:            02/07/16 20:36:55
--   Relational Database:     FPGD10
--   Standards Option:        DB2 for i
CREATE TABLE J1LIB.J1LOGIN (
     LOGIND CHAR(25) CCSID 37 NOT NULL DEFAULT '' ,
     KD CHAR(1) CCSID 37 NOT NULL DEFAULT '' ,
     SYSID CHAR(8) CCSID 37 NOT NULL DEFAULT '' ,
     AUTKEY CHAR(32) CCSID 37 NOT NULL DEFAULT '' ,
     USERIP CHAR(16) CCSID 37 NOT NULL DEFAULT '' ,
     TOKEN CHAR(24) CCSID 37 NOT NULL DEFAULT '' ,
     GENTMSTAMP FOR COLUMN GTMSTP      DECIMAL(13, 0) NOT NULL DEFAULT 0 ,
     CONSTRAINT J1LIB.Q_J1LIB_J1LOGIN_PK_00001 PRIMARY KEY( AUTKEY ) ) ;
LABEL ON COLUMN J1LIB.J1LOGIN
(    LOGIND TEXT IS 'LoginId code' ,
     KD TEXT IS 'Kind code' ,
     SYSID TEXT IS 'System id' ,
     AUTKEY TEXT IS 'MD5 Authent key' ,
     USERIP TEXT IS 'User IP' ,
     TOKEN TEXT IS 'Input string for MD5 Hashing' ,
     GENTMSTAMP TEXT IS 'Generate time stamp' ) ;
```

Figure 2 The designed table SQL layout in IBM AS/400

3.5Some results of creating token for authenticated key

a. Randomly create token stored in TOKEN(24) field.
b. Use MD5 Algorithm to generate authenticated key stored in AUTKEY (32) field.
c. Check for the login user's authenticated key and IP address.
d. Finish verifying the login action and return the flag of true or false.

Figure 3 shows the results of creating token for authenticated key.

	KD	SYSID	AUTKEY	USERIP	GENTMSTAMP
900	2	9999	ES11068P5639961827GvbBca	72.24.175.5	1160207165737
901	2	9999	ES11068P060327GvsPwD4867	72.24.175.5	1160207165754
902	2	9999	ES11068P54842127GwIvCF39	72.24.175.5	1160207165818
903	2	9999	ES11068P159427GxS1YL1450	72.24.175.5	1160207165928
904	2	9999	ES11068P0673173327H1TIuk	72.24.175.5	1160207170029
905	2	9999	ES11068P71827H1i71A90047	72.24.175.5	1160207170044
906	2	9999	ES11068P552827H1vNdn2826	72.24.175.5	1160207170057
907	2	9999	ES11068P8827H2CRT8405316	72.24.175.5	1160207170112
908	2	9999	ES11068P327H2h7k49765053	72.24.175.5	1160207170143
909	2	9999	ES11068P3927H2vENG426570	72.24.175.5	1160207170157
910	2	9999	ES11068P663405527H39ZB05	72.24.175.5	1160207170208
911	2	9999	ES24630P5927HIoqVp210467	172.21.132.86	1160207171850
912	2	9999	ES24630P87827HJ0QAf43649	172.21.132.86	1160207171909
913	2	9999	ES24630P74427HJM6HP65770	172.21.132.86	1160207171922
914	2	9999	ES52089P2927HJf3Qi975770	50.128.143.81	1160207171941
915	2	9999	ES24630P138327HKjWhI6996	172.21.132.86	1160207172045
916	2	9999	ES11028P1635089627HLm6K3	72.24.245.21	1160207172148
917	2	9999	ES11028P8527HXw0WI424073	72.24.245.21	1160207173358
918	2	9999	ES10463P33827HdMyl764685	172.21.129.122	1160207173922
919	2	9999	ES11052P212676827Hp80vt7	172.17.12.29	1160207175107
920	2	9999	ES11052P327Hp8Grq0566312	172.17.12.29	1160207175107
921	2	9999	ES24630P358627Hr9gsA3534	172.21.133.152	1160207175308
922	2	9999	ES24630P527HvJLDj5034463	172.21.133.152	1160207175719
923	2	9999	ES24594P27Hx9TGx04668835	172.21.133.152	1160207175908

Figure 3 Some results of creating token for authenticated key

3.6Two application instances of the secure login utility

In order to verify the feasibility and practicality of the theory and method in this paper, the Secure Login Utility – Universal Authenticated Key Generator method which is developed by the author's web group has been built and now is running in the enterprise. In the following *Figure 4* and *Figure 5*, we are going to use this concept to implement and realize the proposed method applying on two applications developed in the Java Struts framework (https://www23.fpcusa.com/PsnWeb/logon.do) and WebSmart ILE (http://wd10.fpcusa.com:8010/pppublic/xlpp/VPPIRREL2.pgm?task=Open Enrollment Summary Reoprt2&TKN=xxxxxx) respectively. According to our realizations, the IP address can be tampered by Hijacking during login, the generated authenticated key cannot be modified. In 2013, there was an attack by Xie Tao [3] to break MD5 collision resistance in 2^{18} times. In virtue of the server's techniques and programming skills, they could resist amount of trial by Hijacking in a second. Hence we have successfully secured the protection upon the Secure Login Utility. Currently, we can't discover any methods or ideas to decipher this secure utility.

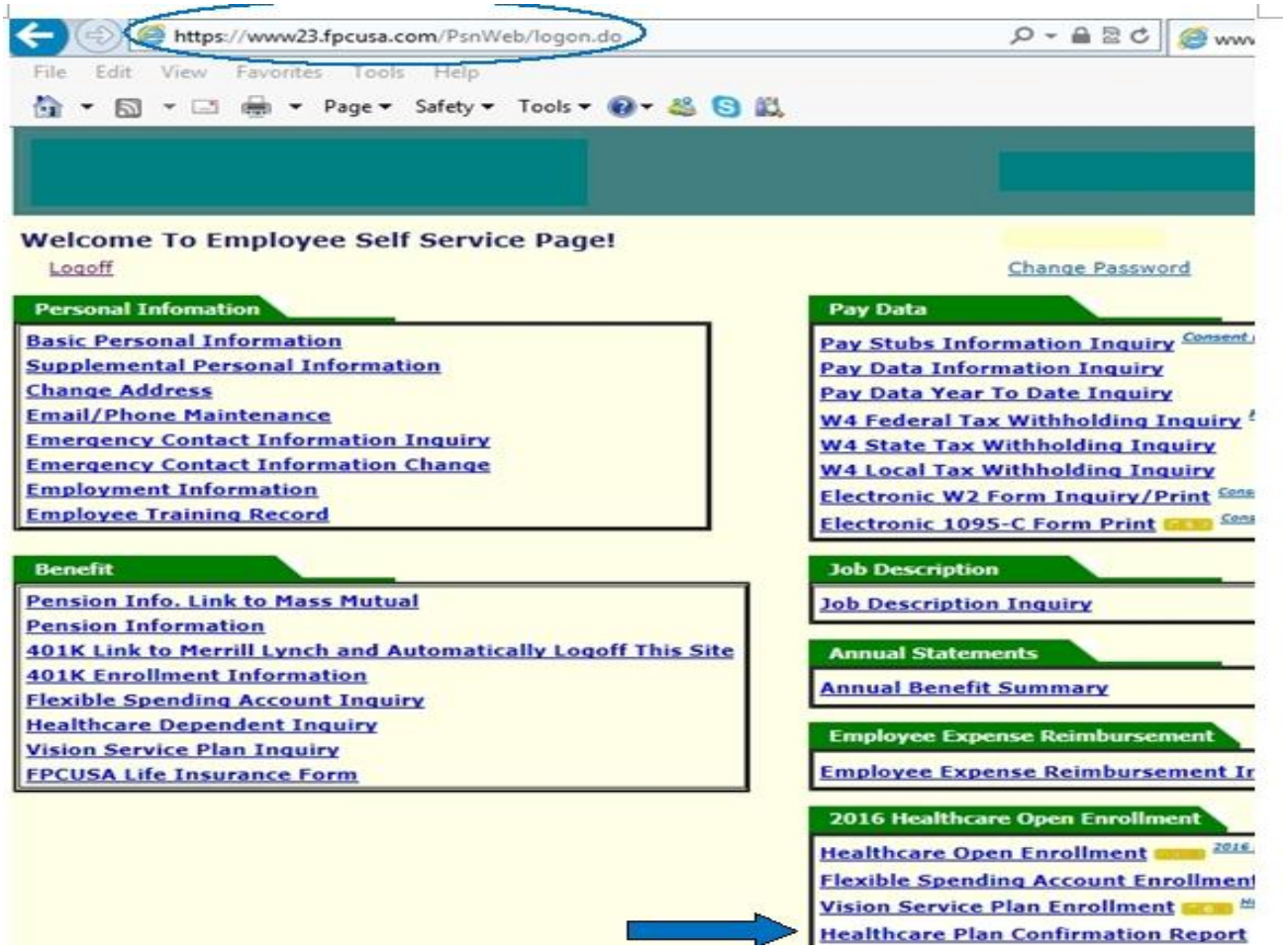
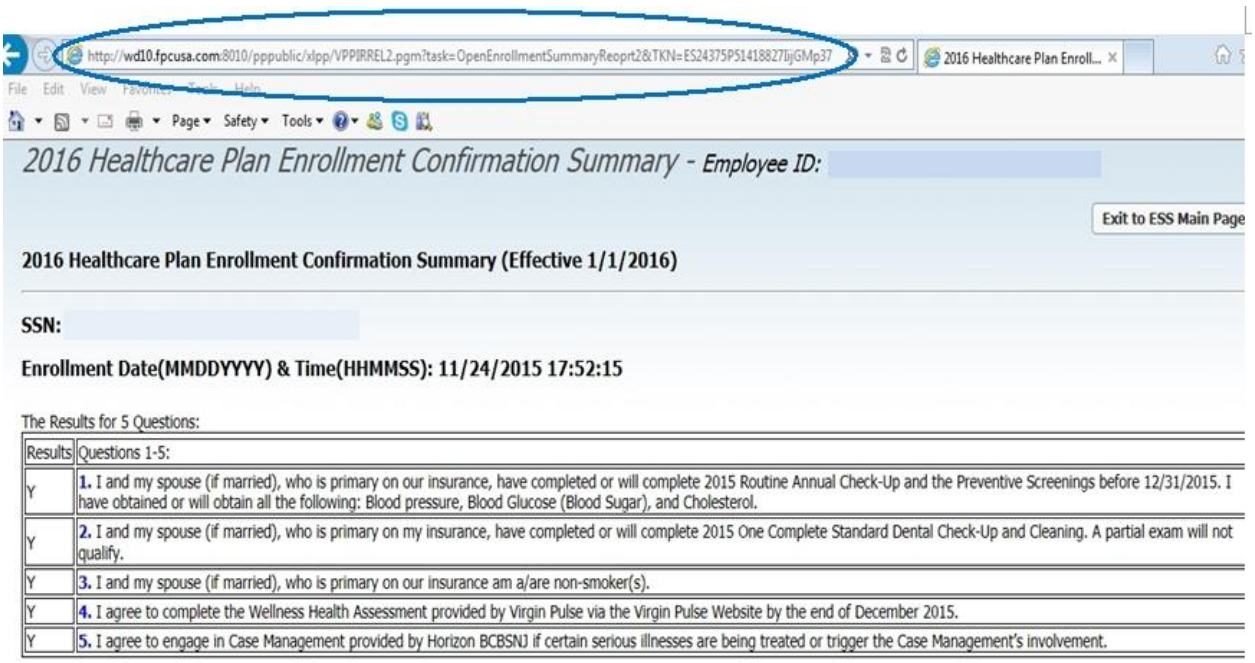


Figure 4 Employee self service–the look of output pages developed in Java

3.7The design is beneficial to web information systems

Why the design is such beneficial [7-12], hereby, we justify it by illustrating two detailed figures which are representative many Sign-On in *Figure 6* and Single Sign-On (SSO) in *Figure 7* respectively. In *Figure 6*, we indicate the regular application of many login functionalities upon multi-platform from diverse web programming. Another *Figure 7*, it exhibits the beneficial application of a Single Sign-On functionality upon the same conditions. Obviously, there is only one difference whether the enterprise should adopt the SSO for their web systems and users or not.



2016 Healthcare Plan Enrollment Confirmation Summary - Employee ID:

Exit to ESS Main Page

2016 Healthcare Plan Enrollment Confirmation Summary (Effective 1/1/2016)

SSN:

Enrollment Date(MMDDYYYY) & Time(HHMMSS): 11/24/2015 17:52:15

The Results for 5 Questions:

Results	Questions 1-5:
Y	1. I and my spouse (if married), who is primary on our insurance, have completed or will complete 2015 Routine Annual Check-Up and the Preventive Screenings before 12/31/2015. I have obtained or will obtain all the following: Blood pressure, Blood Glucose (Blood Sugar), and Cholesterol.
Y	2. I and my spouse (if married), who is primary on my insurance, have completed or will complete 2015 One Complete Standard Dental Check-Up and Cleaning. A partial exam will not qualify.
Y	3. I and my spouse (if married), who is primary on our insurance am a/are non-smoker(s).
Y	4. I agree to complete the Wellness Health Assessment provided by Virgin Pulse via the Virgin Pulse Website by the end of December 2015.
Y	5. I agree to engage in Case Management provided by Horizon BCBSNJ if certain serious illnesses are being treated or trigger the Case Management's involvement.

Wellness Program Participation: Yes

Plan Type: FPCCUSA New Plan

Figure 5 Employee healthcare enrollment–the look of output pages developed in websmart ILE

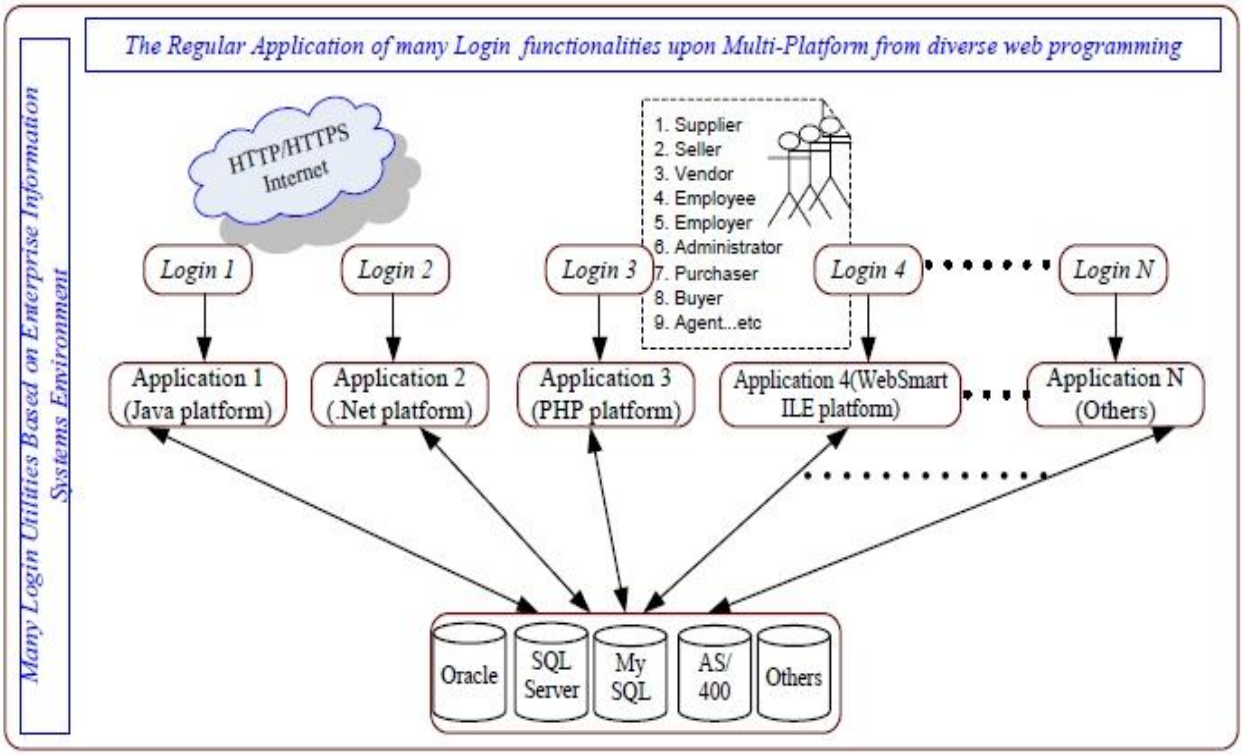


Figure 6 Many login functionalities upon multi-platform from diverse web programming

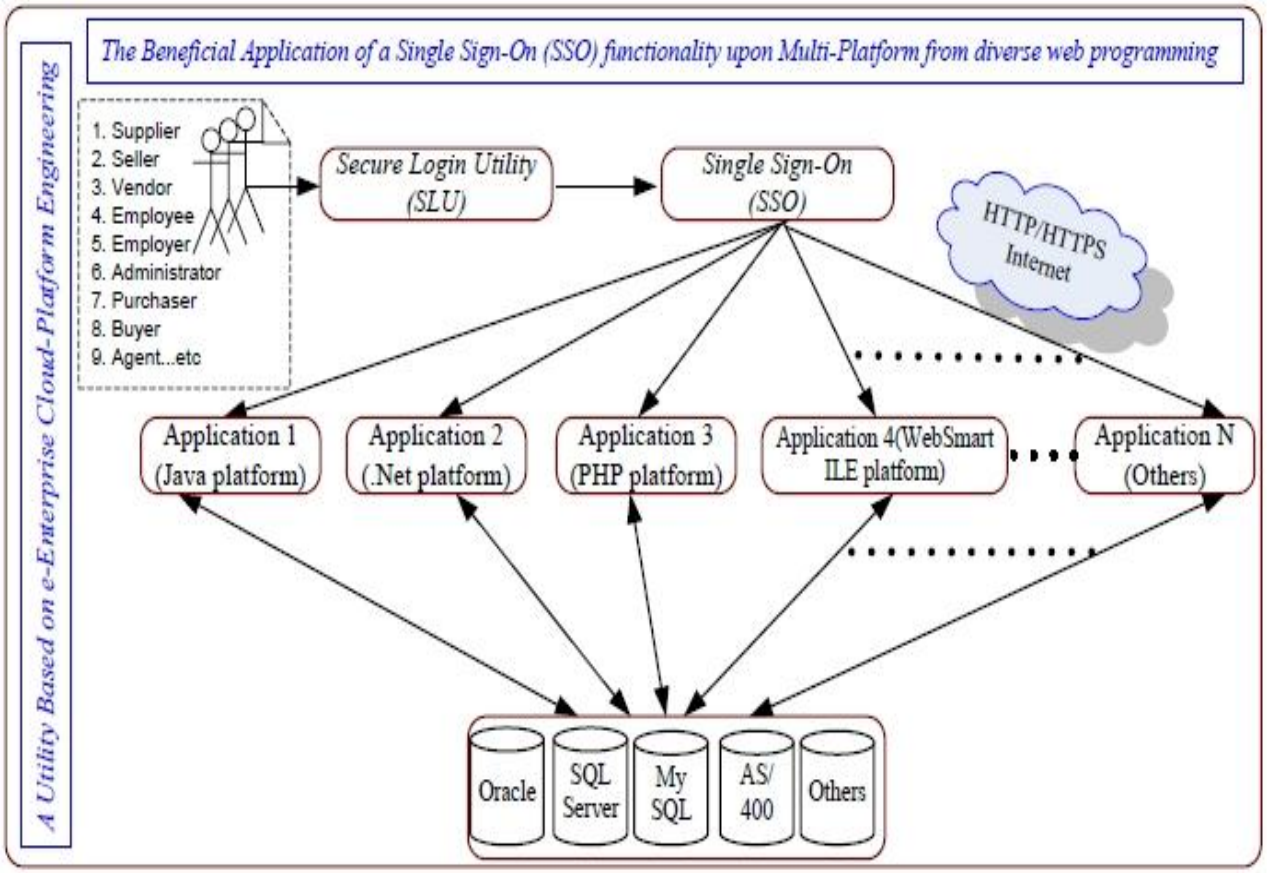


Figure 7 Single login functionalities upon multi-platform from diverse web programming

4.Conclusions and recommendations

Internet and web applications, i.e. Cloud Computing, Semantic Web and e-Commerce have become several growing parts of our daily lives. No doubt, more opportunities are created to develop and deploy new web-based products and services. It is to say that it's impossible without automated web-based help. Even project managers and IT engineers shouldn't forget what have learned in their software engineering, programming and project management classes, they are expected to adopt new ideas and technologies as the evolving progress is getting mature. In this article, you will look at web security technologies over the internet that deeply affects to make up the enterprise business applications in a variety of different platforms and understood why companies/organizations such as ours might want to adopt and apply this method.

Web-based applications in the Cloud migrated from traditional ones benefit customers and the enterprise itself by providing application scalability and reducing hardware costs. Therefore web applications over the internet are involved within modern web topics and cloud computing to such an extent that the key issue of web security and Single Sign-On are considered. In other words, it's always up to the user in readiness for such security applications in the coming era of the emergency web.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] http://india.emc.com/emc-plus/rsa-labs/standards-initiatives/md2-md4-and-md5.htm. Accessed 03 February 2016.
[2] Rivest R. The MD5 message-digest algorithm.1992.
[3] Xie T, Liu F, Feng D. Fast collision attack on MD5. IACR Cryptology e Print Archive. 2013:1-12.
[4] https://wiki.evolveum.com/display/midPoint/Single+Sign-On+First. Accessed 03 February 2016.
[5] https://www.uoguelph.ca/ccs/security/internet/single-sign-sso/benefits. Accessed 03 February 2016.

[6] https://msdn.microsoft.com/en-us/%20en-us/library/aa745042%20%28v=bts.10%29.aspx. Accessed 14 March 2016.
[7] http://php.net. Accessed 14 March 2016.
[8] Budinsky F, DeCandio G, Earle R, Francis T, Jones J, Li J, et al. Websphere studio overview. IBM Systems Journal. 2004; 43(2):384-419.
[9] Haralabidis N. Oracle JDeveloper 11gR2 Cookbook. Packt Publishing Ltd; 2012.
[10] http://www.w3schools.com. Accessed 03 February 2016.
[11] https://www.bcdsoftware.com/iseriessupport/documentation/websmart/. Accessed 12 February 2016.
[12] https://www.bcdsoftware.com. Accessed 12 February 2016.
[13] http://www.asjava.com/core-java/java-md5-example/. Accessed 12 February 2016.

Hsien-Yu Lee, his academic research interests include web technologies/evolution, intelligent computing, and evolutionary algorithm application. His industrial specialties include web technologies (Java, .Net, PHP) realization, database design and application, object-oriented programming (C++, Java), and server techniques. He has published several articles in reputed international journals. In order to develop professional knowledge, enlarge diverse programming experience and increase project evaluation skills, Mr. Lee joins 10+ professional activities, these technical Journals certificated Reviewer/Editor listed several below - Studies in Engineering and Technology (SET), International Journal of Scientific Engineering and Technology (IJSET), International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), International Journal of Engineering Research & Technology (IJERT), ACCENTS Transactions on Information Security (TIS), International Journal of Advanced Computer Research (IJACR) and so on.
Email: ebilllee@gmail.com

Nai-Jian Wang is an associate professor in the Department of Electrical Engineering, National Taiwan University of Science and Technology, Taiwan. He got his master and PhD degree from the Department of Electrical Engineering, University of California, Los Angeles (UCLA), USA. His research interests include multimedia signal processing, digital design on FPGA, embedded system, intelligent computing and optimization, and computer vision.

Appendix:

Figure 8 Secure login utility–universal authenticated key generator by using Java and AS/400 CL/RPG