FingerID

A New Security Model Based on Fingerprint Recognition for Personal Learning Environments (PLEs)

Sara Jeza Alotaibi
Learning Societies Laboratory
University of Southampton
Southampton, UK
sja2g09@ecs.soton.ac.uk

Dr. David Argles
Learning Societies Laboratory
University of Southampton
Southampton, UK
da@ecs.soton.ac.uk

Abstract— **the current practice of password based security for PLEs in general and the Internet in particular is inadequate. The widespread authentication mechanism of username and password is out-dated, and does not meet current needs. Intruders and hackers have also learnt, and become more tech savvy. Besides, remembering a plethora of long passwords and passphrases, sometimes as many as 15 or 20, is cumbersome. This raises the need to introduce a better and more reliable authentication mechanism which is not dependent on a series of characters, but rather on a technology that is unique and only possessed by the individual. Similar services already exist, and they are good in some situations, but prove to be inadequate under other circumstances. In this paper, we propose a one-stop solution to eliminate all these problems, named FingerID. This solution will make the experience of access to distributed web accounts a more secure, accessible and usable one. This solution has been developed, tested, and proven. The findings of this paper will revolutionise the entire authentication mechanism on the web, and thereby enable the user access to distributed accounts at a single point.**

Keywords- security, federated access management, biometric authentication, personal learning environments

I. INTRODUCTION

The advent of the Internet has had a significant effect on human civilization [1]. Human efforts over many decades have made the Internet to be what it is today and to become an integral part of human life, at least in the developed world. A benevolent tool in the hands of the noble, the Internet is changing lives; but it can also be a spiteful weapon in the hands of the wicked.

Terrorism, money laundering, drug trafficking and gunrunning, coordinated through the Internet, are just some of the manifestations. Similarly, financial fraud, of this ingeniously orchestrated over the Internet, enables attackers to break into a security system and spirit away the money of their victims [2]. Phishing and Identity theft are some of the attacks that the 1.8 billion population of Internet users [35] must have come across.

As these evils occur, the need for the security also rises. Therefore, there is the need for improved security measures and authentication mechanisms so that intruders can be discouraged. A simple solution that might come to mind is to maintain the same username and password for all accounts maintained on the web. However, such an approach is never advised, since it increases vulnerability of information, and therefore makes it easy for the intruder to attack all web accounts [3]. A similar solution is to keep easy passwords [4], but this approach also makes intrusion more achievable for malicious users. On the other hand, long and complex passwords seem like a good solution, but it would ultimately prove to be impractical for Internet users to remember [5]. Studies have revealed that an average Internet user has to commit to memory as many as 15 such access control passwords[1]. Besides, the problem of weak passwords and the need to change them tends to deprive some of the advantages of the Internet, making it an arena of insecurity, susceptibility and cumbersomeness [3], [4]. This is an inconvenience, which compels every Internet user to live with it.

II. CURRENT ISSUES

A. Virtual Learning Environment

The unprecedented development of Information and Communication Technology (ICT) from the early Eighties revolutionized many fields of work and activity, including learning and education which has undergone radical changes. The coming of the Internet and the World Wide Web (WWW) introduced the concept of "learning anytime, anywhere and anyhow" [10]. Students and teachers could be geographically dispersed in what is termed a virtual classroom. Distance education was prefixed with 'online' to give what is now known as e-Learning.

VLEs are systems designed to support teaching and learning in an educational setting and allow them to access education resources from any computers that have Internet connections. Most of these systems are password-protected to offer a secure, closed environment and to prevent unauthorised third-party access. This authentication mechanism prevailed for many years, but the needs of the current times do not coincide with its application [7]. The current times require

[1] According to a survey carried out for this research earlier, it was found out that around 45% people from the chosen sample had over 15 online accounts on different online service providers.

greater convenience and enhanced security, simply because the intruder has become very smart and technologically savvy [6].

1) *Personal Learning Environments (PLEs)*

The PLE represents the next generation of e-Learning system, and refers to "an online learning environment where the student is able to customize his/her learning environment based on pedagogical and personal choices." [11]. A PLE is not an application in itself, but a new way of using the web or web2.0 for learning. PLE focuses on the individual, the learner is presented with learning resources based on individual interests, education level, attitude and cultural, social and other factors [12]. Two primary approaches have been identified for conceptualising and developing PLEs– with the PLE as an object i.e. an environment or a hub comprising all learning applications and tools; and with the PLE as a framework that integrates a variety of Web 2.0 tools according to the choice of the learner [13]. Web 2.0 and social software tools that are used to develop PLEs include blogs, applications such as del.icio.us, wiki, podcasting, videocasting, wiki facebook, etc.

PLEs offer distinct advantages over VLEs. PLEs can be used to pursue formal study even while being outside the realm of the educational institute; unlike VLEs, a digital record of the process of learning is conserved through the PLE by means of applications such as the Interactive Logbook (IL)[2] [14]; the learner is the owner and manager of the PLE; the PLE provides a social presence for the owner; and most importantly, PLE is designed for lifelong learning, while VLE is an imitation of the classroom with its set time period. It is now accepted that learning continues throughout life in different contexts and different settings, and efforts are on to access and certify informal learning by extending and recognizing PLEs [15]. In 2005, Scott Wilson proposed a future of the PLE as illustrated in Figure 1.

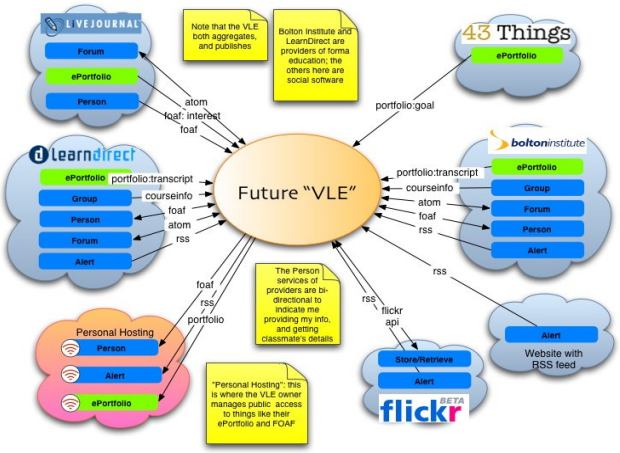


Figure 1. The Future of PLE[3]

As appealing as it sounds, VLEs and PLEs pose various threats, especially when exams are held online. There was a study held by King *et al*. in 2009 [40], which concludes that 73.6% of the students that were selected for the sample had the point of view that it is easier to cheat in an online environment rather than in a conventional one.

One of the main challenges facing the security of the e-learning environment is to ***authenticate students*** so that no unauthorised individuals are permitted to upload submissions or access information, respectively [41]. Some other problems faced during e-learning are double submissions from the same students [42], and e-learning not being held in supervised locations, which therefore enables the individual to access unauthorised areas, etc. [43]. Moreover, students typically have to sign-on to multiple e-learning systems, necessitating an equivalent number of sign-on dialogues, each of which may involve different usernames and verification information.

2) *Single Sign-On and User- Authentaction in PLEs*

Authorisation preceded by authentication plays a crucial role in providing security amongst PLEs [15]. Therefore, most of the existing systems are faced with managing user accounts within each of the multiple e-learning systems to be accessed in a co-ordinated manner in order to maintain the integrity of security policy enforcement.

Single sign on system will provide a security assertion token to e-learning systems using a protocol like SAML, Liberty Alliance, WS Federation or Shibboleth [44]. Then, this SSO software receives the token, checks it, and then allows the students to access e-learning services without having to sign on [44].

However, not much work has so far been carried out to replace the conventional form of authentication of username and password on single sign on systems. The current practice of password based security for PLEs in general and the Internet in particular is inadequate. The widespread authentication mechanism of username and password is out-dated, and does not meet current needs. Intruders and hackers have also learnt, and become more tech savvy. Therefore, Chou [39] describes various techniques which may prove to make the authentication process stronger and more secure. These techniques have been categorised into three types:

- The first technique is based on the knowledge of the user; therefore, it is present with him only. A select few examples include password, secret question, PIN, etc.
- The second technique is personally held (owned) by the user, or is otherwise in use by him. A few examples include smart card, mobile device or security token.
- The third technique is the trait which is naturally possessed by the user or is inherent in him. These kinds of authentications are those which are classified as biometric, and which cannot be possessed by another person since they are unique in every individual. A few examples include palm prints, fingerprints, retinal image, face gestures.

[2] A suite of mobile tools for multimedia note-taking, knowledge sharing, learning management and personal development planning.

[3] <http://zope.cetis.ac.uk/members/scott/blogview?entry=20050125170206 >

This authentication mechanism prevailed for many years, but the needs of the current times do not coincide with its application [7]. The current times require greater convenience and enhanced security, simply because the intruder has become very smart and technologically savvy [6].

Many applications have been developed in the past with the objective to improve the security, accessibility and usability on single sign on systems in VLEs; some of these have been analysed in the table 1 on the basis of the three chosen criterion.

TABLE I. SUMMARY OF COMPARISON WITH SIMILAR APPLICATIONS

Current Applications	Level of security	Level of accessibility	Level of usability
OpenID	✓ [17]	✗ [23]	✗ [24]
Shibboleth	✓ [16]	✗ [25]	✗ [25]
OAuth	✓ [44]	✗ [27]	✓ [26]
Liberty Alliance	✗ [29]	✗	✓ [30], [31]
Microsoft Passport	✗ [34], [33]	✓ [18], [19]	✓ [20]

With the help of the Table I, there is now the need for Internet users to break the relation between long passwords and their obligation to remember it [8]. Moreover, it can be stated that no software or application has so far been established which matches the features and innovation that can be witnessed by the usage of our proposed system. Therefore, the research revolves around the objective to make the maintenance and log-in process more secure, usable and accessible for the internet user. Thus the research question is as follows:

'What is the procedure to enable web users to access distributed systems on one accessible, usable and secure platform?'

Both existing systems and our proposed systems were evaluated against the criteria of Security, Accessibility and Usability. Accordingly, an idea was generated which would fundamentally alter the entire authentication mechanism; replacing memorised passwords with fingerprint data. This laid the foundation for FingerID - a service to maintain multiple web accounts with the user's fingerprint.

One of the most important tools in PLEs is social networking tools [12]. For this, we began with the concept of a service that would maintain web accounts for the user rather than the user going through the ordeal. Other e-learning tools—for example, LMSs [4], MLEs [5] and other education services— will be taken as a goal for the future by implementing the same model.

[4] Learning Management Systems

[5] Managed Learning Environments

III. PROPOSED SOLUTION

Computer technology has improved so much that natural features are now being used for authentication. Nature has made every individual unique, the clue to which can be had through eye coloration, fingerprint, palm print, voice, facial image, DNA signature and so on [7]. Since early days, fingerprint is being used as an important proof of an individual's identity. It is readily available, convenient to use and at the same time unique providing "accuracy, size, cost, performance and proven track record" [9], [7]. These natural characteristics are termed 'biometrics', and the systems that make use of such features in terms of providing access to respective users are known as biometric authentication systems [9]. The solution presented in this paper takes these inherent advantages of fingerprinting into account and offers a system of authentication for the Internet users which is more easily managed and more secure.

A. Our Proposed Solution: FingerID

FingerID provides the user with the facility to maintain multiple web accounts from a single source without the concern of having to remember multiple credentials. It is also a common practice to give away differing information on the web and to then forget which information has been revealed to which website. This makes information vulnerable and difficult to update. FingerID solves this problem by making itself the single source where information of the user will be maintained. Any updates or deletions can be achieved effectively, and one can effectively keep track of what information is sent out on the web. Moreover, Internet users are faced with the tedious process of filling out registration forms at every new account or subscription to a service on the web. FingerID provides the service of filling out the forms by giving the respective service provider with the user's credentials.

The scope of this research is based on key principles: (1) background literature review and concurrent studies; (2) a live project for the development of the solution; and (3) field-testing. This is supported by hard techno-economic analysis, which ensures that the solution is commercially viable. Many solutions languish in the dark tunnels of academic history and gather dust for not being commercially viable; therefore, the present study encompasses the entire gamut of the subject surrounding the problem. These constitute a critical review of the literature, development of a solution as a live project, inclusion of the requirements of everyday Internet users, field-testing the models, and techno-economic feasibility analyses.

FingerID involves the human element from two aspects: fingerprint scans are taken from humans and the human interaction with the system to utilise the service. Therefore, an innovative HCI theory has been adapted for the research study whereby there is an amalgamation of scientific research with design research. The following figure exhibits how scientific research and design principles can be integrated into one model:

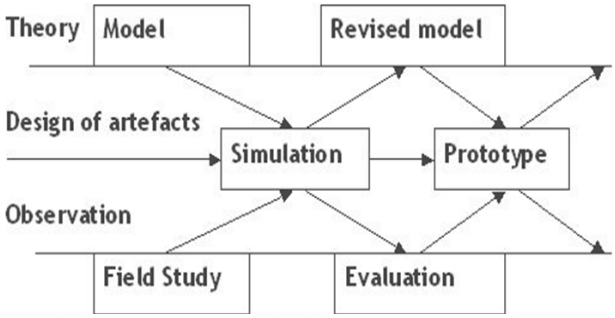


Figure 2. Integration of Scientific and Design Research [36]

As can be seen from the figure, artifacts tend to influence the simulations or prototypes, and thus the models are subject to change due to these influences [36]. Therefore, the research findings should be a combination of theoretical data analysis as well as observations from real life experiences and users. This approach has been used for FingerID to deduce the level of security, accessibilty and usability that is desired by the internet users when they access their web accounts.

1) Development and Research Methodology

One of the earliest frameworks is the waterfall model. The waterfall model was selected owing to its structured approach, proven record and simplicity. The waterfall model fits the development methodology of FingerID, since it comprises five phases[6], and each phase is dependent on the completion of its preceding phase [37].

Initially, a first research questionnaire was formulated in order to gather basic information and prospects of the application. The initial research questionnaire was helpful in terms of identifying the functional as well as non-functional requirements of FingerID. Then, three research questions were formulated and, correspondingly, a set of three hypotheses were developed based on three criteria of accessibility, usability and security. These hypotheses were field-tested by the Research methodology that contains two main entities:

- Lab testing
- User Survey.

Lab testing is defined as the amalgamation of semi-automated tools and manual evaluation which is performed by an expert. Along with lab testing, the user survey proved to provide beneficial data for the research study. Quantitative and qualitative data were collected from representatives of people with disabilities and others concerning how they interact with FingerID in terms of security, accessibility and usability. For this purpose, an empirical operational model was developed and the results were analysed with the use of suitable statistical instruments.

[6] Requirements, Design, Implementation, Testing and Maintenance.

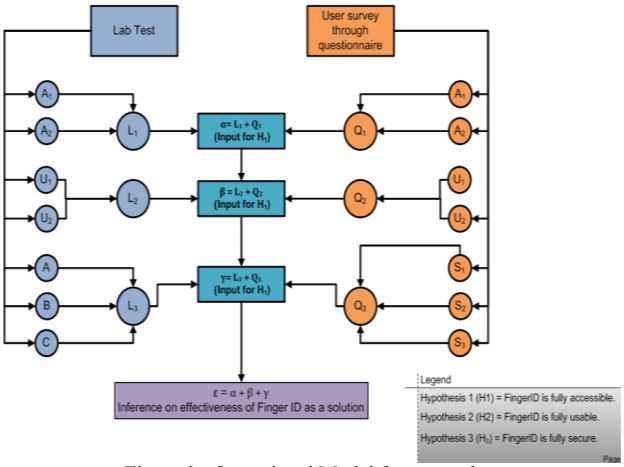


Figure 3. Operational Model for research

IV. ANALYSIS

A. Initial Questionnaire

The initial questionnaire which was developed for FingerID was filled out by participants for one month so that more respondents could be included in the survey. The questionnaire was made available on the internet from July 26, 2010 to August 26, 2010; notably, the survey comprised only 10 questions[7].

The sample of the questionnaire comprised 189 participants, who varied in terms of age and gender. There were some individuals who were disabled whilst some were not. The research was carried out in an opportunistic manner, and the questionnaire was made available in the form of an online advertisement on Facebook, Disable World Website[8], etc. The respondents of the advertisement filled out the questionnaire and increased the sample of the survey.

The results of the questionnaire show that approximately 55% of the participants were women whilst the rest were men. The age group data show that the majority of participants was between 21-25 years of age, and then 26-30 years. 25% of the participants in the sample were disabled. The results of the level of experience of the participants show that 30% were experienced, 50% were intermediate, and only 20% were new on the web. The typing skills result of the participants show the following figures: 20% were equipped with fast typing skills, 50% considered themselves to be normal typists, whilst 30% were slow typists. The input devices that the participants were most acquainted with include a mouse, and fingerprint scanner came second on the list. 50% of the users had fingerprint scanners on their laptops whilst the other half of the sample did not have this facility. It was found that social networking sites and email sites are the most popular amongst the general internet users, and most web accounts are held there. The second last question on the questionnaire was a

[7] <http://qtrial.qualtrics.com/SE?SID=SV_7NInQmVL928SDQM>

[8] Disability Community for Persons with Disabilities and Health Conditions, <http://community.disabled-world.com/>

very important one, as it helped to establish the average number of accounts held by internet users; the results show that the highest rank on the list was 38%, which represented the number of people who have more than 15 accounts on the web. The last question inquired about the number of users who forget their usernames and passwords. 27.2% participants strongly agree with this statement, 36.6% people agree with this statement, and the rest either disagreed or showed neutral response. The results of questions 9 and 10 are given below:

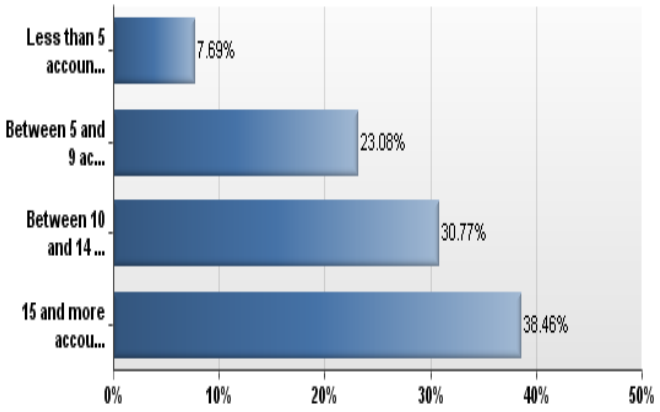


Figure 4. Result of Question 9: "How many accounts you have on the Internet?"

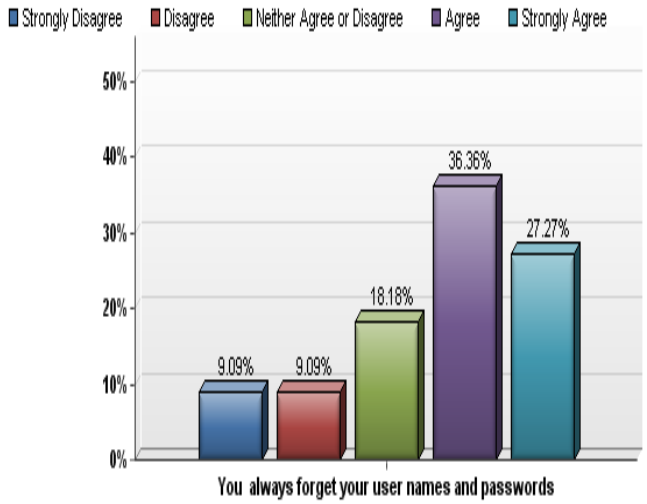
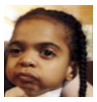


Figure 5. Result of question 10: "You always forget your username and passwords?"

B. *Personas and Scenarios*

Personas revolve around the concept of assuming fictional users for a diverse testing approach. These users are intended to have real needs and tasks. This approach might help to address the factors that may have been ignored in the questionnaires.

Sandra Steven



Sandra is an undergraduate student in engineering courses at The Open University[9] *and has been visually impaired since she was 20 years old. She has always loved logging on to the web and interacting with her friends via email for sharing studying materials. Ever since she has become disabled, she has restricted her time on the web to the instances when she is accompanied with someone to help her. Although guidelines and standards have been made to make websites accessible for the disabled, general accessibility rate of sites is still very low. FingerID will provide her with a solution and make the process of accessing her web accounts more usable and accessible. The decrease in the colour saturation and large font size better facilitate vision for her weak sightedness. Screen readers can also be used with FingerID that will provide her easy access to her required functions.*

Mohammed Ahmed

Mohammed is a retired army officer and often logs on the web to check his web accounts to stay connected with educational groups to develop his various skills. It is very difficult for him to remember all the credentials, usernames and passwords at his age, and desires a service that would eliminate the need to remember passwords and usernames. He has suffered from the undesirable instance of getting his web accounts hacked because one password was kept for several accounts. FingerID will provide him with the security that he desires for his web accounts and will make him avoid the need to memorize multiple credentials for his web accounts.

C. *Functional and Non-Functional Requirements*

Functional requirements outline the main objective of the research study. The functional requirements are categorised with respect to the priority of each, i.e. some possess high priority whilst others have low priority. Those with high priority are necessary to be fulfilled for the success of the research. On the other hand, Non-functional requirements specify the attributes pertaining to the quality of the system rather than the functionality. The tables below show these requirements;

TABLE II. FUNCTIONAL REQUIREMENTS

Functional Requirement	Priority
A service to enable the users to log-in to multiple web accounts.	High
The user is able to add or delete web accounts that are registered under FingerID	High
A summary page is available to the user showing him an update of all his accounts.	High
Email notifications about any activity, i.e. new message, etc. on any account of the user that are registered under FingerID.	Moderate
Personalized image option is available with each user account.	Low

[9] <http://www.open.ac.uk/ >

TABLE III. NON-FUNCTIONAL REQUIREMENTS

Non-Functional Requirement	Priority
Extensive help and instructions are available on the site in the form of text and videos to help the user.	High
Sufficient bandwidth is arranged to provide good service to numerous users at the same time.	High
There exists a reliable and efficient system for backup purposes.	High
A visible and attractive appearance and layout is given to the site to facilitate usability and accessibility.	High
Safeguarding of passwords and other personal information.	High

D. *Use Case Diagram*

As previously stated, the FingerID System comprises two fundamental parts: website and software. The website helps the user to add his account information on the web, and the software allows him to register his fingerprint. The case diagram shows all these functions in the form of interaction between the actor and the application, as is shown in Figure 6. The following are the functions that have been shown in the use case diagram;

- Website:
  - Register at FingerID website: A new user registers his fingerprint in the database of FingerID to become a user.
  - When the user forgets his password on the FingerID website, a new password can be sent to him after necessary authentication has been carried out.
  - The following functions can be performed on different websites: add/delete/update/select information of the user in the web account.
- Software:
  - Registers the user on FingerID service.

V. DESIGN

A. *Four-Tier Architecture*

FingerID has a four-tier architecture comprising the following tiers: client, interface, control and distribution. All these tiers are developed and implemented for the purpose of this dissertation. The architecture provides the framework of the application which serves as the base for the centralised access of web accounts and fingerprint authentication system.

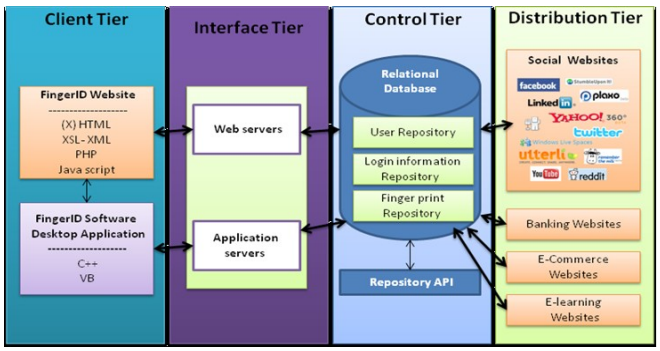


Figure 6. 4-tier architecture of FingerID

B. *FingerID Flowchart*

FingerID System has the following flowchart that highlights the main process of the system:

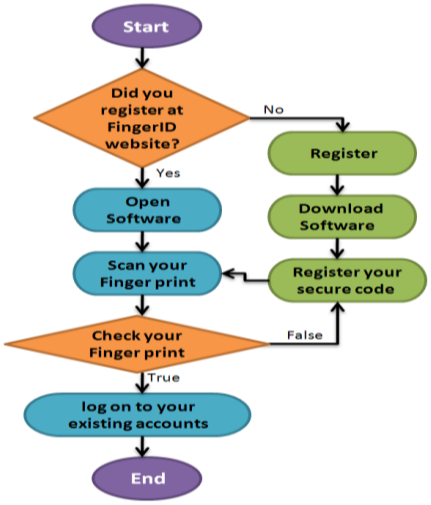


Figure 7. FingerID Flowchart

The FingerID system has been programmed to request the user's fingerprint scan for registration purposes when he is a new user to the system. Following the user registering to become a member, he can then gain access to multiple web accounts under one service. The registration process of the user will only take place once, and later scans will be used to verify the user to provide him access to his web accounts.

C. *FingerID Token Exchange Description*

FingerID token exchange description diagram is given below:

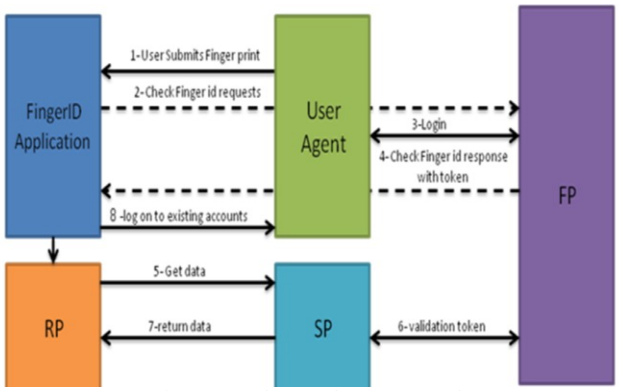


Figure 8. Token Exchange Protocol

The entities in Figure 9 have the following meanings [38]:

- **RP (Relying Party)[10]:** This entity is responsible for acquiring the identity of the user. The main objective of RP is to verify the user so that he can gain the desired access.
- **User Agent:** This is typically a web browser. The user in this component is defined as the individual

[10] "A Web application that wants proof that the end user controls an Identifier, and requests identity data associated with the end user" [38].

who has a digital identity and who participates in the exchange of data with the aid of the client software.

- **SP (Service Provider):** SP is responsible for providing the service to the verified users. This verification is achieved with respect to a token issued by the FingerID provider (FP).
- **FingerID Provider (FP):** This serves as a FingerID authentication server that transmits confirmation to RP about the possession of the identifier by the user.

D. *User Design Interface*

The user interface of FingerID has been designed such that it is attractive, usable, consistent, and able to facilitate the movement between different screens. Existing popular websites have also been analysed for the key features that make them a preference for the user.

In the early stages of the development of FingerID, a paper prototype was designed in order to gather the feedback of general internet users. This exercise proved to be helpful in terms of improving the design of the application, and further helped to evaluate the user interface of FingerID. The sample of the paper prototype testing included students and faculty members from University of Southampton, UK. Then, the computer prototype involved the development of software as well as website prototype. The computer prototype for FingerID System was developed and made available online[11].

VI. IMPLEMENTATION

The implementation phase of any project revolves around the development of the system with respect to the design which is formulated following extensive analysis. Notably, regular monitoring activities are advisable for the implementation phase in order to ensure that the end-product is close to the design of the system. In this case, monitoring activities will ultimately ensure that the focus areas of accessibility, usability and security are being given utmost attention, and that the designs of FingerID software and website are being followed. Essentially, good scripting practices have also been adapted, such as commenting so as to make the code understandable and maintainable.

As previously highlighted, the FingerID System comprises two main parts: website and software. The hosting of the website is carried out on a dedicated web server running on Windows XP with PHP 5.3.1 and MySQL 5.1.4. The IDE of Adobe Dreamweaver has been selected in order to develop PHP, CSS and XHTML content. This environment has been chosen because of its highlighting feature, which makes the content more visible and readable. The highlighting function also helps in the identification of common syntax errors. SQL workbench has been selected in order to create and manage the database schema. It provides a GUI which offers the user a graphical representation of the database.

The software developed and tested on a computer installed with Windows XP, VB.Net 2008 and Microsoft Access. FingerID requires fingerprint scans of the user from the finger printer hardware; therefore, various necessary libraries are required in order to make the program interface compatible to most available brands of fingerprint hardware. The library used for this purpose is provided by Fingerprint SDK and is called GrFinger Fingerprint Recognition Library. After the development of the software, a set-up program has also been developed, which enables a smooth installation of the application[12].

VII. TESTING AND EVALUATION

Testing can be considered as one of the most important phases in the development process of any system or application. The testing activities of FingerID have been based on the research hypotheses and the three focus areas—accessibility, usability and security—throughout the process of accessing web accounts. These hypotheses were field-tested by two means: (1) lab testing to test accessibility, usability and security; and (2) user satisfaction. For this purpose, an empirical operational model was developed and the results were analysed with the use of suitable statistical instruments. The testing tools as well as the results have been discussed in detail in the future papers.

VIII. COMPARISON WITH SIMILAR APPLICATIONS

The security of user information on the web has been an area of interest and concern for many years. The consequences of vulnerability of data are so intense that users and organisations both take extensive measures and spend a great deal of their resources making their information safe. Many applications have been developed in the past with the objective to improve the security, accessibility and usability on the Internet; some of these have been analysed here on the basis of the three chosen criterion. The idea behind isolating these criteria was to enable a robust comparison of the applications' features, benefits, advantages, and disadvantages, which would eventually lead to the framing of the research questions. These criteria are:

A. *Security*

Username and passwords are usually kept simple by Internet users so that they can be remembered easily; this makes intrusion and password cracking much simpler for the intruder. Another bad practice which has been observed is that people tend to use the same password for multiple accounts, which thereby enables the intruder to gain access to more information and utilise such data for malicious purposes.

There are a lot of applications and systems that tried to solve these issues. One of the most significant applications is OpenID; that is a fast and convenient way of accessing multiple web accounts and to avoid the tedious task of remembering information for all accounts separately [21]. The user registers at OpenID with a username and password, and

[11] <www.fingerid.6te.net>

[12] More information about Installation instructions as well as the user manual please visit; <http://www.fingerid.me/GetHelp.php >.

their credentials will then be used by OpenID to provide access to the desired web accounts. The username and password is knowledge-based, and only known to the user. The same information will be maintained in all of the web accounts, which also enhances the security of information [17]. Additionally, the Shibboleth system is high secure application, but it focused on the access and identity management of an organisational set-up, rather than random Internet users. It is a standards-based system which provides single sign-in on the Internet for access to organisational data or licensed resources. It implements the aspect of security by commonly found federated identity standards. The standard—which is followed the most by them—is OASIS' Security Assertion Markup Language (SAML). This provides further privacy to access on the web by giving the power to the browser user and the home web page so as to control the flow of information sent out to each application [16]. Moreover, some secure services revolve around the distributed sharing of data, and do not provide any log-in facilities for any website or web account such as Open authorisation (OAuth); which is a platform through which users can share their private data (pictures, videos, bank accounts, etc.) with users on other websites without revealing their usernames and passwords to anyone [22]. The authentication mechanism of the owner of the account is based on the username and password, and therefore it is knowledge-based like OpenID. The visitors who view the permitted data cannot view any other data, and access to the owner's private data does not require the owner to reveal his credentials therefore security level is good [44].

However, some existing systems are not highly secure; even though they comprise extremely important and private data relating to the individual. One of these applications is liberty alliance; it is focused and concerned with establishing a global network where customers, vendors and governments can perform online transactions whilst ensuring privacy and security [28]. The level of security is not very good in the case of Liberty alliance. The nature of the information—i.e. credit card details—is far too important to be shared with so many websites. Essentially, the user will be connected with a liberty alliance associated website even if he doesn't realise this is the case. Ultimately, the sharing of information, to a great extent, increases the chances of its misuse [29]. An other application is Microsoft Passport that advertises the fact that business owners can enhance their business by incorporating Windows Live ID service on their websites; in this way, the users will be able to log-in automatically at the business owner's website and will thus increase their traffic [32]. Through the Internet there is a hacking tool available for Microsoft Passport which poses a threat to its security. This indicates that strong security measures have not been implemented. If a user logs-in at Hotmail to check email, he might not realise but he has provided access to his Passport wallet for the next 15 minutes without the need for any verifications. An intruder might subsequently use this time to gain access to any of his MSN accounts without his knowledge [33], [34].

All these security issues raise the need to introduce a high secure authentication mechanism that is FingerID. The access to the web accounts which is given after the fingerprint scan matches with the registered print in the database. All the fingerprint scans are saved at a centralised point and is not accessible to any application other than FingerID. Fingerprints are an individual's unique characteristic, which therefore cannot be possessed by anyone else. Additionally, FingerID uses various types of security tools that are Secure Web Services, TimeStamp and SSL Certificate. Data and fingerprint templates are encrypted to enhance the security of the system.

B. Accessibility

Several problems have been identified through research over the years regarding accessibility. Later, some tools and methods were stated and have been proposed by different organizations to make the websites and software applications more accessible. However, the level of accessibility for a lot of systems is not commendable. For example, the users at OpenID have complained about the frequency of visual images and graphics used to verify whether a human is making the entry [23]. Such graphical content proves to be difficult for disabled individuals. Besides, disabled people will experience difficulty in utilising the features on the Open authorisation (OAuth) website and authenticating themselves to gain access owing to the username and password authentication mechanism [27].

Nevertheless, No evidence has so far been established that would indicate that Liberty Alliance and the Shibboleth system have taken measures to provide accessibility to their users. Therefore, it cannot be stated that they are accessible to less able users [25].

On the other hand, Microsoft Passport has made provisions which enable disabled people to use websites without difficulty [18]. Microsoft Shared Computer Toolkit has great features to facilitate accessible navigation and log-in process for a windows user. This toolkit has been integrated with Microsoft Passport, thereby provides accessibility to the disabled user [19]. However, this service is only limited for the websites where Windows Live ID service is incorporated. Notably, this is a significant limitation, since not all websites are equipped with this service. Microsoft Passport has incorporated commercial benefits within its service; on the other hand, FingerID does not offer any commercial benefits so far, since the product is very new. Besides, FingerID requires no entry of password at log-in; therefore, it would be very useful for disabled people. Fingerprint scanners are widely available nowadays, and even present in laptops; therefore, users will have no problem in utilising the services offered by FingerID.

C. Usability

Usability is a very important factor that measures the quality of a user's experience when interacting with websites or systems. Even though a lot of organizations proposed usability principles, there are a lot of systems and applications not meet the usability demands of the current times. For

instance, the usability level of OpenID still requires further enhancement, since users face major issues and confusion when performing desired functions [24]. Notably, user experiences have been studied and indicate that Shibboleth lacks usability since usability is limited to organisational use and cannot be used for general Internet users since they will need to get organisational credentials to get access [25].

On the other hand, evidence shows that OAuth has a good level of usability concerning its features and pages. Users navigate with convenience and perform the required functions without any problems [26]. Moreover, Liberty Alliance offers great usability to its users [31]. Liberty Alliance is known to bridge fixed and mobile networks as well as provide great usability to its users [30]. Furthermore, Microsoft Passport has taken steps to ensure that their website possesses a commendable level of usability. One such example is that of a standard followed by them whereby 'all Passport enabled sites should possess sign-out buttons'. This sign-out button should enable the user to sign out of not only that specific site but all other associated Passport-enabled sites to which a user is currently logged in. Another one of their standards is that the colour of the buttons on the site should be such that they are easily visible [20]. Furthermore, our proposed system, that is FingerID, offers great usability to its users since it enables them to avoid the redundant entry of password and usernames at every log-in. Once the user has logged in FingerID, he can easily access all the web accounts in one place.

IX. Summary and Results

Learning is a lifelong process, even though conventional educational systems did not truly acknowledge the fact in the way in which they worked. Closed structured learning is gradually giving way to informal learning in which the individual learns throughout a complete lifespan if so desired. However, the authentication mechanism of these existing systems based on usernames and passwords that are out-dated, and do not meet current needs. Therefore, this raises the need to initiate a better and more reliable authentication mechanism which is not dependent on a series of characters, but rather on a technology that is unique and only possessed by the individual.

The extensive study of the existing applications and relevant literature enabled understanding of the requirements of accessing web accounts with security, accessibility and usability. These three criteria were determined as the areas in which the hypotheses were tested, and thus results were concluded.

FingerID is an efficient and reliable alternate to the conventional authentication mechanism of username and password. FingerID authentication is multi-factored in terms of three authentication techniques:

- Knowledge-based factor: Secure code is sent to the user when he registers on FingerID.
- Ownership-based factor: Cryptographic data, such as biometric data or fingerprint minutiae.
- Inherence-based factor: The fingerprint scan of the user is saved in the database and used upon every instance of authentication.

On the other hand, FingerID aims to promote the convenience for the Internet user since he will not have to remember multiple passwords for a multiple number of accounts. FingerID has been developed with the objective of improving the process of log-in in the user's web accounts. The biometric that has been selected is fingerprint in order to enable greater convenience for everyone.

X. Conclusion and Future Work

The username and password authentication mechanism no longer serves the current times of increasing identity thefts and intrusion activities. The authentication mechanism which can serve the need of the existing times is to have a mechanism that relies upon unique characteristics that cannot be stolen. Fingerprints seem to be the most applicable solution to the above mentioned concern of security breach.

There are many guidelines available for ensuring usability, accessibility and security on the web; however, it is noteworthy to state that not many websites abide by such guidelines. FingerID aims to change this and to provide its users with an application that caters to all of these required areas. Accessing the web can be a tedious task for a person with a disability and others if the websites are not accessible and usable. Accessibility, usability and security guidelines have been tested on the FingerID website and browser by means of numerous activities. Such activities have been discussed in detail in the future papers. In general, FingerID has been evaluated on the basis of these several guidelines and a user survey. The results from both of these forms of evaluations bear the conclusion that FingerID is an accessible, usable and secure way of accessing web accounts. The system is live, and a user community has been established[13].

The username/password authentication mechanism is no longer fit for purpose. In this paper, we propose a cost effective, convenient and secure authentication-solution to the everyday users throughout the world for undertaking secure dealings over the Internet. The study envisions of worldwide application of the solution such as VLEs and PLEs. It visualizes seeing Internet users happily authenticating their identity in a hassle free manner and going about doing their activities in a secure environment without the fear or trepidation of loss of identity and money.

The chosen Fingerprint SDK for Windows will be later tested with artificial fingerprints in order to judge whether the system is threatened by any fake inputs. In the case of failure of the chosen software, new compatible software will be selected from the available products in the market.

FingerID will authenticate the user on the basis of his fingerprint scans. Other biometric authentication methods—for example, palm prints and face gestures—will be taken as a goal for the future. Another aim of the project is to encourage further research and development on the subject.

[13] Details can be found at <www.fingerid.me>.

REFERENCES

[1] B. Starr, Helium, "Groundbreaking inventions of the 20th century", *Helium*, 2010.

[2] Z. Tian, N. Xu, W. Peng, "E-Commerce Security: A Technical Survey," iita, vol. 2, *Second International Symposium on Intelligent Information Technology Application,* IEEE Xplore, China, 2008, pp.956-960.

[3] D. Argles, A. Pease and R. J. Walters, "An Improved Approach to Secure Authentication and Signing", *Advanced Information Networking and Applications Workshops, AINAW '07, 21st International Conference*, IEEE Xplore, Niagara Falls, Canada, 2007, pp. 119-123.

[4] D. Denning, "Protecting Public Keys and Signature Keys," *IEEE Compute Society,* IEEE Xplore, vol. 16, USA, 2006, pp. 27-35.

[5] V. Gligor, "A guide to understanding covert channel analysis of trusted systems", *Technical Report NCSC-TG-030, National Computer Security Center*, USA, 1993.

[6] Science News, "Smart Methods for Detecting Computer Network Intruders", *Science Daily,* 2002.

[7] Z. Riha and V. Matyas, "Biometric authentication systems", *FI MU. Report Series, FIMU-RS-2000-08*, 2000.

[8] J. M. Williams, "New security paradigms", *Proceedings of the 2002 Workshop on New Security Paradigms*, Virginia Beach, Virginia, 2002, pp. 97-107.

[9] M. McGinity, "Staying connected: Let your fingers do the talking", *Communications of the ACM*, vol. 48, no. 1, 2005, pp 21-23.

[10] W.M. Petegem, "From Learning over E-learning to MyLearning", *In: ITI 2008 30th Int. Conf. on Information Technology Interfaces*,. IEEE Xplore, 2008, Cavtat, Croatia, pp. 27--30

[11] L. Kolas, A. Staupe, "A personalized E-learning Interface", *In: EUROCON 2007 The International Conference on "Computer as a Tool",* IEEE Xplore, 2007, Warsaw , pp. 2670—2675.

[12] X. Li, X. GU, "A Conceptual Model of Personal Learning Environment Based On Shanghai Lifelong Learning System", *In: 17th International Conference on Computers in Education*, Asia-Pacific Society for Computers in Education , 2009, Hong Kong , pp. 885—889.

[13] R. Kompen, R. Mobbs, "Building Web 2.0-based Personal Learning Environments – A Conceptual Framework", *In: Eden Research Workshop* , 2008, Paris.

[14] T. Chan, D. Corlett, M. Sharples, J. Ting, O. Westmancott, "Developing Interactive Logbook: A Personal Learning Environment", *In: IEEE International Workshop on Wireless and Mobile Technologies in Education (WMTE'05)*, IEEE, 2005.

[15] G. Attwell, "Personal Learning Environments - the future of eLearning?", *In eLearning Papers* ,2007.

[16] R. L. Morgan, S. Cantor, S. Carmody, W. Hoehn, K. Klingenstein, "Federated Security: The Shibboleth Approach", *Educause Quarterly*, vol. 27, no. 4, 2004, , pp. 12-17.

[17] T. DiVito, "OpenID: A Potential Authentication Technology", *Decision Line,* School of Business-Camden, Rutgers University, Newark, USA, 2008.

[18] S. Baklanov, "Security models in ASP.NET. Authentication", *XLineSoft*, 2005.

[19] D. Shinder, "How to Use Microsoft's Shared Computer Toolkit", *Window Security,* TechGenix Ltd, 2005.

[20] R. Oppliger, "Microsoft .NET Passport: A Security Analysis", *IEEE Computer Society Press*, Vol. 36, Issue 7, Los Alamitos, CA, USA, 2003, pp. 29-35.

[21] E. Bond, "Securing the Blogosphere through OpenID: Relying Parties, Unite", *AOL Developer Network*, 2007.

[22] J. Jackson, "OAuth 2.0 security used by Facebook, others called weak", *Computerworld Security newsletter*, IDG.net, 2010.

[23] B. Ferg et al., *"OpenID Authentication 2.0—Final", OpenID Community*, Dec. 2007; http://openid.net/_specsopenid-authentication-2_0.html .

[24] J. Zhou, "OpenID usability is not an oxymoron", *FactoryCity*, 2008.

[25] C. Joie, "Understanding Shibboleth- SLO Issues", *Internet2,* 2010.

[26] M. Engel, "MySpaceID Usability Testing", *Slide Share.net*, MySpace, 2009.

[27] "Accessibility issues of social Web", *W3C*, 2010; http://www.w3.org/WAI/PF/wiki/Social_Web#OAuth_Accessibility_Issues.

[28] A. Nghiem, *IT Web services: a roadmap for the enterprise*, Prentice Hall PTR, USA, 2003.

[29] P. Judge, S. Shankland, "Liberty - is usability compatible with security?", *ZDnet US*, July 2002; http://www.zdnet.co.uk/news/servers/2002/07/16/liberty-is-usability-compatible-with-security-2119220/

[30] T. Skytta, "Liberty Alliance Completes Two Projects Based on their ID-WSF", *Sun Security,* vol. 73, issue 5, 2004.

[31] H. Mikkonen, M. Silander, "Federated Identity Management for Grids," *icns, International conference on Networking and Services (ICNS'06),* USA, 2006, pp.69.

[32] "Use Windows Live ID for Your Web Site", *Windows Live ID*, 2006; https://msm.live.com/app/default.aspx

[33] W. Redmond, "Microsoft Passport: Streamlining Commerce and Communication on the Web", *Microsoft News Center*, 1999.

[34] K. Choo, "Issue report on business adoption of Microsoft Passport", *Information Management & Computer Security*, Emerald Group Publishing Limited, vol. 14, issue 3, 2006, pp. 218-234.

[35] Miniwatts Marketing Group, "Internet World Statistics", *World Internet Users and Population Stats*, 2009.

[36] W. E. Mackay, A. L. Fayard, "HCI, Natural Science and Design: A Framework for Triangulation across Disciplines", *DIS'97: Designing Interactive Systems* (August 18-20) ACM: Amsterdam, pp. 223-234, 1997.

[37] S. Casteleyn, F. Daniel, P. Dolog, M. Matera, "Engineering Web Applications",ISBN 3540922008, 2009.

[38] K. Farnham, "Augmenting OpenID: The OpenID Token Exchange Protocol", *AOL developer Network*, 2007.

[39] D. Chou, "Strong User Authentication on the Web", *Microsoft Corporation*, August 2008.

[40] C.G. King, R.W. Guyette, C. Piotrowski, "Online exams and cheating: An empirical analysis of business students' views", *The Journal of Educators Online*, vol. 6, issue 1, 2009.

[41] W. Huang, D. C. Yen, Z. X. Lin, J. H. Huang, "How to compete in a global education market effectively: A conceptual framework for designing a next generation eEducation system", *Journal of Global Information Management*, vol. 12, issue 2, 84-107, 2004.

[42] K. M. Apampa, G. B. Wills, D. Argles, E. Marais, "Electronic Integrity Issues in E-assessment Security", 2007.

[43] E. Marais, D. Argles, "Security issues specific to E-assessments", *8th Annual Conference on WWW Applications*. Conference proceedings, Bloemfontein, South Africa, 2006.

[44] Z. A. Khattak, S. Sulaiman, L. A. Manan, "A Study on Threat Model for Federated Identities in Federated Identity Management System", *Information Technology (ITSim), 2010 International Symposium,* IEEE, Kuala Lumpur, 2010.