Using Fingerprint Recognition in a New Security Model for Accessing Distributed Systems

Sara Jeza Alotaibi, Mike Wald, David Argles
Learning Societies Laboratory, University of Southampton, United Kingdom

Abstract

The security threats to the personal information of Internet users raise the need for improved security measures and authentication mechanisms of username and password so that intruders can be discouraged. Another problem faced by modern-day Internet users is that they are required to maintain a long list of passwords for their web accounts - maybe 15-20 accounts. Therefore, 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. However, there are some secure services that revolve around the distributed sharing of data, and do not provide any log-in facilities for any website or web account with high level of security, accessibility and usability. This paper presents an answer to all these problems in a single solution, named FingerID, by focusing the theoretical background of the subject and an in-depth review of the literature available on various aspects of security provisions used in the industry for distributed systems. During the course, the objective is to identify clear criteria which would enable robust comparison between FingerID and various similar applications available in the market.

1. Introduction

The advancement of technology and multi-faceted information system, as has ushered in a hi-tech futuristic era in the history of the Human race, it has also indulged in cryptic criminological affairs. This has necessitated a supremely secured, safe and sophisticated identification and access control methodologies thus strengthening screening specifications to protect sensitive information with a vision to shield the international online users and web community against any covert intervention and activity. Phishing and Identity theft are some of the attacks that most online users of the 1.8 billion-population of Internet users [35] must have come across. Thus in the foreseeable future the law abiding web users and internet facilitators can plan to build up a more protected networked society by the introduction of revolutionary human identity recognition systems.

Another hitch that humans have inherited from the use of the Internet is the maintenance of the great number of accounts held by the Internet users. A survey was carried out through a previous research study regarding the number of accounts held by Internet users. The sample of the questionnaire comprised 79 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[1]. The respondents of the advertisement filled out the questionnaire and increased the sample of the survey. The question concerning the number of accounts provided different choices: less than 5 accounts; less than 10 accounts; less than 15 accounts; 15 accounts and more. The results of the survey revealed that 44% (highest rank) of Internet users have more than 15 web accounts. Such an Internet user will face great difficulty in remembering log-in details for his web accounts, along with the personal details that are given.

This unique personnel identification model can be based on broadly three factors, namely, introduction of single web identification, implementation of biometric especially fingerprint distinguisher and unique recognition identifier for each and every online account holders and internet users through the very unique FingerID system with high level of security, accessibility and usability.

The paper is structured in the following manner; Firstly, the theoretical background of the subject, including a brief overview of the distributed systems comprising concepts, definitions, components, architecture, advantages and disadvantages of such systems are explained in *Section 2*. Then, a new system, FingerID, has been proposed, as outlined in *Section 3*. This is followed by a critical review of theoretical information and an extensive evaluation of similar software applications in the market in *Section 4*. Finally, *Section 5* concludes the report with a research question, summary and results.

2. Theoretical Background

[1] It was made available from April 5, 2010 to May 5, 2010 at <http://qtrial.qualtrics.com/SE/?SID=SV_7NInQmVL928SDQM&SVID>.

2.1. Distributed systems

The ubiquitous computers which are seen in every household, office and every part of the market are not simply interconnected but are rather a part of a distributed set-up executing a collection of protocols to coordinate the actions of multiple processes [36], [37].

2.2. Concepts and definitions

A study of the underlying concepts of a distributed system has provided somewhat differing perspectives from academia, the industry regulator, and business organisations associated with distributed networks. One of the earliest definitions of a distributed system was proffered by Enslow in 1978, who specified that a distributed-data-processing-system[2] needs to have five properties: multiplicity, physical distribution, unity of system operation, system transparency, and cooperative autonomy. More recently, in 2009, academicians Yan [38] and Steen [39] separately defined a distributed system as 'a piece of software that ensures a collection of independent computers that would appear as a single coherent system to its users'. Somewhat different from Yan and Steen's definition, Rao [41] defines a distributed system to be 'one in which components communicate and coordinate their actions only by passing messages to other's components in the network'. On the other hand, Google, a giant search engine operator, operating extensively and successfully in a distributed system, defines it as, 'an application that executes a collection of protocols to coordinate the actions of multiple processes on a network, such that all components cooperate together to perform a single or small set of related tasks' [37].

Irrespective of the varying perceptions between academia and the industry which have been introduced over the years, there appears to be consistency amongst all concerning the key characteristics and the ultimate goal of a distributed system. The two key characteristics of a distributed system are, firstly, the differences of various system components and the way in which they communicate with each other are transparent to users, and secondly, applications and users have the freedom to interact consistently and uniformly, irrespective of the location and time of the interaction [38]. Steen [39] identified that the goal of a distributed system is to make resources available with transparency, openness and provision for scalability within the system.

[2] A distributed system is a generic term that can be used for both; distributed data processing system or distributed computing system [38], [39], [41].

2.3. Components and architecture

Lee [42] summarised a distributed system as a combination of two important components: independent computers which appear to the user as a single coherent system, and a middleware that enables this perception. In a distributed system, the nodes tend to make use of the resources available to them [43]. Each processor has its own individual distributed memory. During the exchange of information, messages are passed between the processors [44]; this is fundamentally different to parallel computing where all processors have equal access to a shared memory. For the exchange of information, this shared memory is used to pass information between the processors [44].

Therefore, in a distributed system, each node becomes a subsystem, making a distributed system an amalgamation of multiple subsystems [43]. Three primary differences tend to exist in this theory. The differences are the distributed kernel, system size, and heterogeneity [36]. Firstly, ever since the concept of a single protected kernel ceased to exist, it took place over several nodes in the network [45]. Secondly, a centralised system may constitute several administrative domains, each of which having a set of specific responsibilities. The size of the summed-up system is much bigger than the individual components [46]. Finally, the security policy and operating systems in the distributed system may be different [47].

Yan [38] identified three primary types of distribution systems depending on the functional basis for which they are developed: distributed computing systems, distributed information systems and distributed pervasive systems. Notably, distributed systems are also often classified on the basis of design, which may include clusters [48], grids [49] and peer-2-peer networks [50].

2.4. Advantages and disadvantages

The goals that have been discussed above provide a distributed system with excellent features over a centralised system. Lee [42] summarised some of these features and included economics, speed, inherent distribution and incremental growth. The features listed by Nadiminti *et al*. [51] are consistent with those by Lee [42], except that the former has accorded 'functional separation' as the number one feature over speed. According to these views, a distributed system provides an excellent avenue for separation based on functionality/services provided, capacity and purpose of each entity in the system [51]. The large aggregate of microprocessors in distributed systems offer a better price to performance ratio than mainframes, thereby making it a much more cost-effective way to increase computing power. Besides, considering the

aggregation, a distributed system is more likely to have more computing power, thereby making it much faster than a mainframe's speed, which tends to drop due to load distribution. Since some applications are intrinsically distributed, under these situations, a distributed system is the best option. Moreover, owing to the inherent increased reliability goal embedded within a distributed system, if one machine crashes, the entire system does not fall, which is unlike the centralised system [52]. Demchenko *et al*. [45] argue that, because of the aggregation of multitude of subsystems, distributed systems provide considerable advantages and are more tolerant to failures. Perhaps the best feature of a distributed system over the centralised system is in its modular expandability, i.e. its capacity for incremental growth [53]. Nadiminti *et al*. [51] explained that due to existence of large number of personal computers, there arises a need for the users to collaborate and share information, which is a driving force by itself.

As nothing in the world is without a disadvantage, distributed systems also have a few disadvantages. The most commonly discussed issues include the security of the system and network problems. Perhaps the most important challenge for the distributed system is the provision of a secure environment where users can operate without fear or trepidation of losing their identity or resources. Bauer *et al.* [54] state that this is largely caused due to the dispersed nature of information. Gasser & McDermott [55] state that, once a user's password is altered, this information then circulates over a number of nodes, subsequently making it susceptible to attacks and eavesdropping by malicious intruders. Similarly, the network infrastructures of a distributed system may have various problems, such as load balancing, message loss, and so on. The challenge is to make the system efficient without jeopardising its overall performance [38].

2.4.1. Security in distributed systems. Security is a daunting challenge which was recognised early on in the evolution of the distributed system. Numerous studies have been undertaken with the objective to address almost all aspects of security of distributed systems bringing considerable insight into the problem.

The chief reason for insecurity in distributed systems is owing to its goal to make it open. Soshi & Maekawa [1] explain that, in an open distributed system, information and data are strewn all over the subsystems which it encompasses. Scott & Sharp [5] further observe that such data and information can be easily moved from location to location, and may even be replicated at different places, therefore making the data more susceptible to malicious attacks. This poses a serious challenge owing to the fact that, if security is compromised at one node, it then becomes very difficult to contain. Earlier, Popek & Cline [4] argue that the introduction of authentication protocols in the channels and encryption mechanisms on the network have not been able to contain security hazard. On the other hand, Hoa & Phoung [3] argue that the concerns of security can be controlled to a considerable extent by the use of control mechanisms and secure channels. The success of security mechanisms, however, is contingent upon the innovativeness of the intruders in devising threat modules.

Security provision in distributed systems can be achieved by means of access control mechanisms and secure channels. The 'public-key' and 'secret-key' cryptography provide the basis for authentication and for secure communication. Other popular methods which are able to provide secure and authenticated communications include 'Kerberos' and SSL [3]. Hoa & Phuong [3] list three security techniques: cryptographic algorithms, digital signatures and cryptography pragmatics.

Authorisation preceded by authentication plays a crucial role in providing security amongst distributed systems. Chou [2] describes various other 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.

The FingerID authentication mechanism is based on all of the above mentioned techniques; therefore, it can be stated that FingerID authentication is multi-factored. Following is an explanation of the authentication mechanism in terms of three above stated factors:

- 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.

3. Proposed Solution

Extensive studies are underway in the field of computer technology with the objective to overcome the problems that have been discussed in the preceding section. Some ideas have already been implemented so as to enhance security over the Internet; some of them are IPsec Protocol [10], [11], Pretty Good Privacy (PGP) [13], Multipurpose Internet Mail Extension (MIME) [12], Secure/Multipurpose Internet Mail Extensions (S/MIME) [14], Circuit-Level Gateways [15] and Application-Level Gateways [15].

However, not much work has so far been carried out to replace the conventional form of authentication of username and password on the World Wide Web. 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]. There is now the need for Internet users to break the relation between long passwords and their obligation to remember them [8]; therefore we began with the concept of a service that would maintain web accounts for the user rather than the user going through the ordeal. Similar services already exist, but each has its limitations and drawbacks.

Computer technology has improved so much that natural features are now being used for authentication. These natural characteristic are termed as 'biometric', 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 biometric of fingerprints has been chosen for the authentication purpose of FingerID.

Both existing, 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.

3.1. 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) concurrent studies in progress; (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 humans interact 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.

3.1.1. 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. Figure 1 shows the architecture that provides the framework of the system which serves as the base for the centralised access of web accounts and fingerprint authentication system.

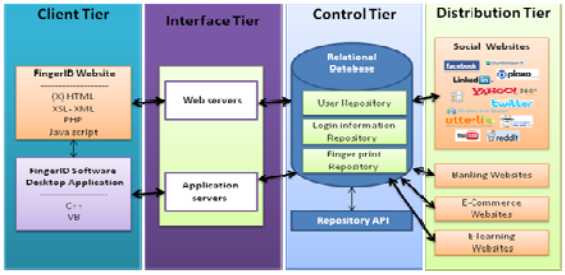

Figure 1. 4-Tier architecture of FingerID

The client tier of the application can be defined as the GUI (HTTP to Web Server) at the client side of the communication. As can be seen in the above figure, this tier comprises two components:

- **FingerID Website**—a standard web browser-based application for browsing the web.
- **FingerID Software Desktop Application**—this application is downloaded and installed at the

client. It is used to scan the fingerprint of the user and to register it for later use.

It can be seen from figure 1 that the interface tier is constituted of web and application servers. It has been programmed to facilitate the instantiation of multiple web servers so that parallelism can be increased in the system. There exists an option to achieve load balancing of the traffic from the web. For this job, a load balancer[3] can be installed in front of the web server which manages the load and then subsequently forwards it to the system in a constant flow.

The control tier is composed of one of the main components of the system: the database and repository. It performs management, control and distribution activities for the rest of the tiers.

The distribution tier comprises servers and collection servers. Multiple provisioning servers can be instantiated so as to facilitate faster computational activities which can exist in parallel. These servers offer simultaneous processing of multiple jobs so that tasks can be completed in a shorter period of time. Multiple instances of collection servers can also be created with the objective to retrieve the data at a faster rate from the network. It deals with a set of domain servers where the users are registered, such as Yahoo, Hotmail, etc.

3.1.2. Important Algorithms. There are many algorithms within the system, but the most important is the register algorithm performs the following functions;

- Checks if the user has entered all the required information correctly.
- Checks if the entered username or email address exists in the database or not.
- If the information is entered correctly then a secure code is generated and provided to the user.

The following figure shows a flowchart for 'Register' page algorithm at FingerID website:

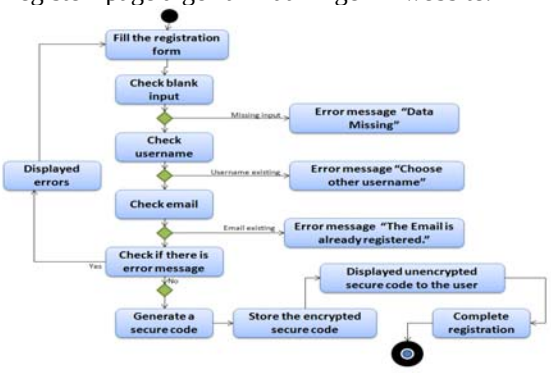

Figure 2. Algorithm on Register Web page

The process regarding the biometric identification in the FingerID software involves several classes, functions and libraries. The following figure shows the flowchart regarding the biometric identification process of the user:

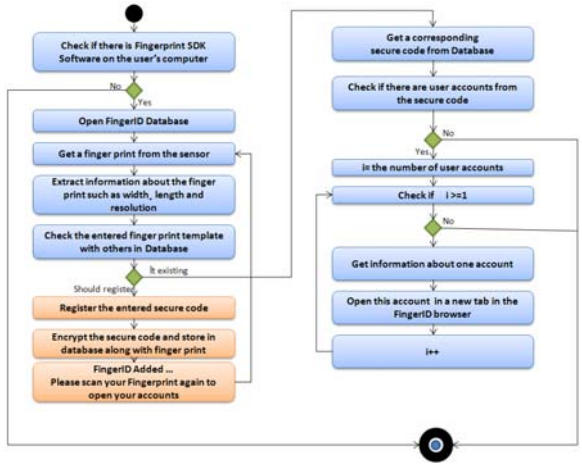

Figure 3. Algorithm of FingerID software

It can be seen from figure 3 that the orange boxes describe the registration activities, whereas the blue boxes show the utilisation of the FingerID once the user has been provided with access to his accounts.

The algorithm of connecting FingerID system is important when connection is to be established between the software and the website. This connection is established with the help of the secure code generated and provided to the user at the time of registration. If the users have forgotten the secure code, they can get it any time by logging in to the FingerID website. When the users enter their secure code on the FingerID software, they first register their fingerprint along with their secure code. The algorithm takes the secure code from the software and returns a comma separated array of user's account information using a secure HTTP/POST communication protocol. In this way, the software is able to gather the user's account information which is saved on the website with the help of this algorithm. Figure 4 shows the flowchart for this algorithm:

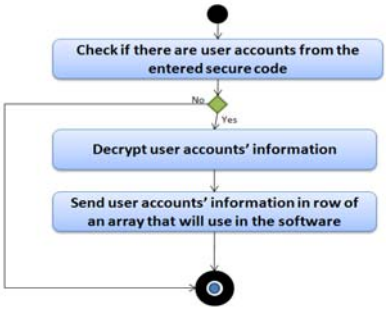

Figure 4. Algorithm of connecting FingerID software with FingerID website

3.1.3. FingerID Design. 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

[3] The load balancing service is provided by web hosting company.

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. The following figure shows the FingerID flowcharts:

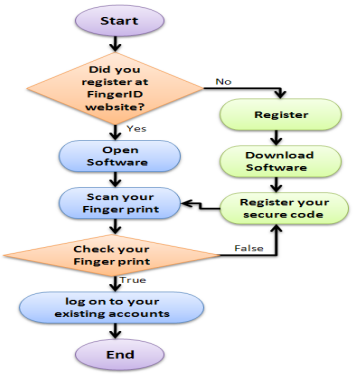

Figure 5. FingerID Flowchart

3.1.4. FingerID 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 original design specification 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.

The FingerID system is composed of two main parts: website and software (browser). 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. Nevertheless, the software developed and tested on a computer installed with Windows XP, VB.Net 2008 and Microsoft Access.

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. The following figure shows a screen shot of the FingerID system:

Figure 6. FingerID Browser and FingerID Website

The system is live, and a user community has been established[4].

4. 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:

4.1. 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 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 a highly 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 is OASIS' Security Assertion Markup Language (SAML). This provides further privacy to access on the web by giving the power to the

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

browser user and the home web page so as to control the flow of information sent out to each application [16]. Moreover, there are some secure services that 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 as 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 and therefore the security level is good [40].

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; that it 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]. Another 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 are 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.

4.2. Accessibility

Several problems have been identified through research over the years regarding accessibility and some tools and methods 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, most users will have no problem in utilising the services offered by FingerID.

4.3. 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 that do 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.

5. Summary and Results

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. The research question that had been framed to accumulate the purpose and direction of the research study is as follows:

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

This is the question which directed the project towards achieving a certain aim and objective. An effective research question ensures the researcher remains focused on the path rather than exploring new dimensions for research on diverse topics. Three research questions were formulated and three hypotheses were developed based on the criteria of accessibility, usability and security. 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.

Table 1 shows a critical review of an extensive evaluation of similar software applications in the market denote that FingerID is coupled with security, usability and accessibility. No software or application has so far been established which matches the features and innovation that can be witnessed by the usage of FingerID.

Table 1. 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	✓ [40]	✗ [27]	✓ [26]
Liberty Alliance	✗ [29]	✗	✓ [30], [31]
Microsoft Passport	✗ [34], [33]	✓ [18], [19]	✓ [20]
FingerID	✓	✓	✓

FingerID is an efficient and reliable alternate to the conventional authentication mechanism of username and password. 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.

6. Conclusion and Future Work

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. FingerID will enhance the security of the application since it will be based on the unique individual characteristic of the internet user. This trait is more difficult to access and therefore be stolen compared with the character type of username and password.

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. Besides, 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.

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 for all of these required areas. 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.

This solution will make the experience of access to distributed web accounts a more secure, accessible and usable one. 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. 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.

7. References

[1] M. Soshi, M. Maekawa, "The Saga Security System: A Security Architecture for Open Distributed Systems", *IEEE*, 1997.

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

[3] L. K. Hoa, T. X. Phuong, "Distributed Systems Security", *Technical Report*, 2009.

[4] G. J. Popek, C. S. Kline, "Encryption and secure computer networks", *ACM Computing Summit*, 11(4):331-356, Dec. 1979.

[5] D. Scott, R. Sharp, "Developing Secure Web Applications", *IEEE Internet Computing*, pp. 38-45, November 2002.

[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] InterPeak AB, "IPsec- Internet Protocol Security", *InterPeak AB, Version 1.22-r*, 2005.

[11] TimeStep Corporation, "Understanding the IPSec protocol suite", *IPSec2.0*, 1998.

[12] N. Borenstein, N. Freed, "MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies", *Network Working Group*, 1993.

[13] The Corporation for Research and Educational Networking (CREN), "PGP: Pretty Good Privacy", *Cren.net*, 2001.

[14] Javvin Technologies Inc., "MIME and SMIME: Multipurpose Internet Mail Extensions and Secure MIME", *Jaavin.com*, 2010.

[15] AT&T and Lumeta Corporation, "Firewall Gateways", *AT&T and Lumeta Corporation*, 1994.

[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.

[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.

[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.

[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.

[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. A. Wulf, C. Wang, D. Kienzle, "A New Model of Security for Distributed Systems", *Virginia State University*, 1996.

[37] J. Dollimore, T. Kindberg, "Distributed systems: concepts and design", ISBN 0321263545, *Addison-Wesley*, 2005.

[38] H. Yan, "Introduction of Distributed Systems", *School of EECS, Peking University*, 2009.

[39] M. Steen, "Distributed Systems: Principles and Paradigms", *Virtual University Amsterdam*, 2009.

[40] M. Simhachalam, "Securing REST Web Services With OAuth", *Oracle Corporation*, 2009.

[41] R. Jinghai, "Distributed Systems: Concepts and Design", *Norwegian University of Science and Technology*, 2000.

[42] I. Lee, "Introduction to Distributed Systems", *Department of Computer and Information Science, University of Pennsylvania, CIS 505*, 2007.

[43] R. Dobry, M. D. Schanken, S. Prabhakar, "Security Concerns for Distributed Systems". *IEEE*, 1994.

[44] D. Peleg, "Distributed Computing: A Locality-Sensitive Approach", *SIAM*, ISBN 0-89871-464-8, 2000.

[45] Y. Demchenko, L. Gommans, C. Laat, "Job-Centric Security Model for Open Collaborative Environment", *IEEE*, 2005.

[46] I. Keidar, "Distributed computing column 32 – The year in review", *ACM SIGACT News.* pg: 53–54, 2008.

[47] B. Godfrey, "Exploring the Effect of Heterogeneity in Distributed Systems", *OASIS Retreat*, January 11, 2005.

[48] R. Buyya, "High Performance Cluster Computing", *Prentice Hall*, USA, 1999.

[49] I. Foster, C. Kesselman, S. Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", *International Journal of High Performance Computing Applications*, vol.15 (3) pp 200-222, 2001.

[50] R. Subramanian, B. Goodman, "Peer-to-Peer Computing: Evolution of a Disruptive Technology", *Idea Group Inc.*, Hershey, PA, USA, 2005.

[51] K. Nadiminti, M. D. Assunção, R. Buyya, "Distributed Systems and Recent Innovations: Challenges and Benefits". *Grid Computing and Distributed Systems Laboratory*, 2006.

[52] A. Levi, M. U. Caglayan, "The Problem of Trusted Third Party in Authentication and Digital Signature Protocols", *The Twelfth International Symposium on Computer and Information Sciences*, 27 - 29 October, Antalya, 1997.

[53] T. Y. C. Woo, S. S. Lam, "Designing a Distributed Authorization Service", *IEEE*, 1998.

[54] L. Bauer, M. A. Schneider, W. Felten, "A Proof-Carrying Authorization System", *Electrical and Computer Engineering at Carnegie Mellon University*, 2001.

[55] M. Gasser, E. McDermott, "An Architecture for Practical Delegation in a Distributed System", *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pp. 20-30, 1990.

