INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

# Anti-Phishing Based on Face Recognition and Bio-Metric

**Dr. D. Aruna Kumari**
Department of ECM, KL University, Vaddeswaram, India
**Dr. K. Rajasekhara Rao**
Director, Shri Prakash Engineering and Technology, Tuni, India
**Dr. M. Suman**
Department of ECM, KL University, Vaddeswaram, India

***Abstract:***
*Developing security methods for the Web is a daunting task, in part because security concerns arose after the fact. From the past few decades people all over the world are using internet.*
*Even though many people are using internet in many ways for many reasons there is no security and privacy concerns for our accounts. Many institutions, faculty/children share their printers, laptops, systems so the files get misplaced; many of our accounts are being hacked, because of the vendors. So, in order to avoid the security problems in this paper we are introducing the new proposal that works with face recognition approach and bio-metric approach.*
*Since these systems include many subsystems Operating System, Database System etc and multiple organizations may also participate. Providing complete security solutions are enormously complex. The proposed approach main aim is to make the websites more secure by creating the image (picture) along with the details during Registration process of that web site. The proposed work deals with face recognition, bio-metric and security questions.*

***Keywords****: Email, Security question, image, face recognition, bio-metric*

## 1. Introduction

Web security was First developed in 1995,It may seem obvious that more people are going online to shop, send email, manage their bank accounts, and just about everything in between, but when you stop to think about just how many people use the internet, the numbers are dramatic.

Now- a- days Internet is playing a prominent role and is being used by all the people around the world in many ways. In olden days many educated people/industries use the internet for sending mails or for searching the topics for delivering the class/lesson very well. But now a day everybody is using web and internet for both official and personal purpose. Children also search the matter related to studies and many other things they want they even play games. And many people store their documents, photos…etc in their accounts. Since many of us don't want any one of our friends to know individuals private information. Web user is worrying more about security of their accounts. For example Facebook, yahoo, Gmail…etc, Domain manager has to make sure that the emails are not getting hacked.

Security is a critical part of Web applications. Web applications by definition allow Multiple users access to a central resource — the Web server — and through it, to others such as database servers. By understanding and implementing proper security measures, you guard your own resources as well as provide a secure environment in which your users are comfortable in working with your application.

As the usage of the internet has grown, the web has also become more popular with scammers, identity thieves, and other cybercriminals. So, Threats to internet users have became more, and it is observed that more than 3.5 million people fall victim to "phishing". Phishing is a type of online identity theft.

In order to avoid these problems and to provide security over internet users, we are introducing a new method in our paper. The proposed work deals with face recognition. Previously there are many types of security methods are there like security questions [4], authentication, etc. and also they provides recovery mail option at the time of registration with mobile number for sending the password .

During Registration process, security image is going to be uploaded by the user and that image will be saved in the database. Whenever user wants to logon to their accounts user has to upload the image along with username and password. In this approach,

there are some limitations they are, every time user has to carry the image if user is logging from other systems. Some times because of the unavailability of the image right user may not logon to their accounts.

**2. Why Many People are Interested in Hacking?**

- Recognition
- Admiration
- Curiosity
- Gaining Power
- Revenge
- Gaining Money

RECOGNITION: People are interested for hacking because for their popularity to be increased and to be recognized as the famous talented person in front of their managers etc….
ADMIRATION: People are interested for hacking the accounts because if they complete the work very fast and with good result they are being praised and people also look admirable so, they are interested to hack the accounts.
CURIOSITY: People are interested in hacking because if any fascinating thing happened and if it is not known to us and we feel very curious to know about it and so in the process of knowing the facts they hack the accounts.
POWER: People are interested in hacking because in order to become superior to one another and to gain power they hack the accounts.
REVENGE: People are interested in hacking because if any problem occurred because of us they also try to harm us so in order to take revenge on us they try to hack our accounts.
MONEY: People are interested in hacking because some people In order to gain money by gathering/collecting some information which leads them to become great and gain money so they are interested for hacking the accounts.

**3. Literature Survey (Existing Work)**

We have just studied two important areas where security is needed: communications and e-mail. You can think of these as the soup and appetizer. Now it is time for the main course: Web security. The Web is where most of the Trudies hang out nowadays and do their dirty work. In the following sections we will look at some of the problems and issues relating to Web security. Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, secretly modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use [6][7][8].
In present days there are many methods for avoiding our accounts from being hacked and to provide security and privacy.
The Ways That Are in present in current world:

- CAPTCHA
- SECURITY QUESTIONS
- RECOVERY MAIL
- MOBILE NUMBER
- GUESSING THE PHOTOS IN OUR ACCOUNT
- IMAGES AT TIME OF REGISTRATION

CAPTCHA: In this method we give them words either case sensitive or without case sensitive in the zigzag/scrambled way and we have to guess the words and then Retype it in place provided to us by this we can confirm whether the system/human is accessing the account. By doing this also security is not provided.
SECURITY QUESTIONS: In this method, at the time of registrations we are provided with some drop down list of questions and we choose one of the questions from that and answer that security question. So, at the time of any problem in accessing our account they ask us that question and if provide correct answer only we can access our account. This also seems that we cannot provide much secure.
RECOVERY MAIL: In this method, we provide them the other option of sending the mail to another account of ours/our belongings/our friends so that the passwords/links will be sent to their mails and to some extent the hacking may be avoided. By this also there is an drawback that if account get deleted then we may not provide secure.
MOBILE NUMBER: In this method we provide our mobile numbers so that the passwords may be sent to ours mobiles so that no one can see our passwords except us so in that way we can avoid hacking. For this method if the mobile number is missed/any problem then we may not.
GUESSING THE PHOTOS IN OUR ACCOUNT: In this method we are provided with an option of guessing the images that already exist in our accounts, so that they can verify our accounts. In this method also there is an drawback that is as our close friends will be with us they may know our images. Pictures in our account and can access the accounts so we may lose security.
IMAGES AT TIME OF REGISTRATION: In this method we should register with an certain/particular image only and the same image should be given at the time of logging into the account by this way also there is an drawback because we should carry the image with us wherever we go so this is the drawback.
Now existing all this drawbacks we are going to introduce a new theme in this project.

In this project we are going to introduce a new method that is we are going to provide a new way of securing our accounts, ie, by the face recognition.

**4. Proposed Work**

In present state all the people who are being using the many websites for searching the information or other work they are doing and people who wish to keep their information safe and secret in their web accounts , i.e., mails etc are facing many problems.
In this work we proposed two techniques.

- Bio-metric along with traditional system.
- Using Face recognition along with traditional systems

*4.1. Approach 1*

Generally user is asked to enter username and password before he/she logins, but in this approach user is asked give his/her bio-metric (thumb press). After providing required details, user is allowed to enter into the account. So, in this context it is sure that 100 % privacy is achieved to the individuals account, as bio-metric of individuals never matches with any other bio-metrics.

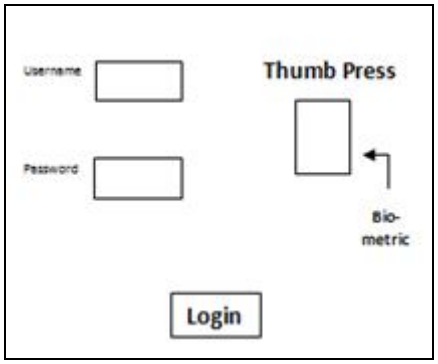


*Figure 1: Login form using Bio-metric*

Figure 1 describes the login form that takes username, password and Bio-metric also. After that, user is allowed to login. Figure 1 Describes the Registration form, before user logins, usually user has to register. During the registration process user should give their bio-metric and then upload, so bio-metric will be uploaded into data base finally user has press register button, it completes registration process.

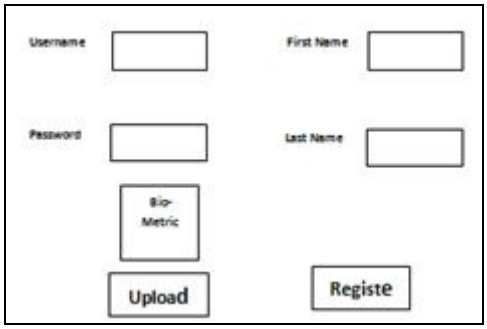


*Figure 2: Registration using Face Bio-metric*

*4.2. Approach 2*

In Second Approach, user name, password and Face recognition will takes place. Figure 3 shows registration process with face recognition. Figure 4 shows login form using face recognition

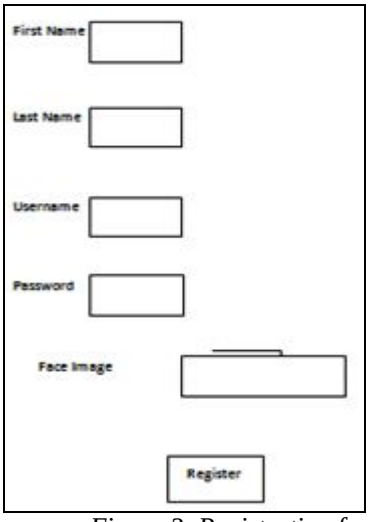


*Figure 3: Registration form using Face recognition*

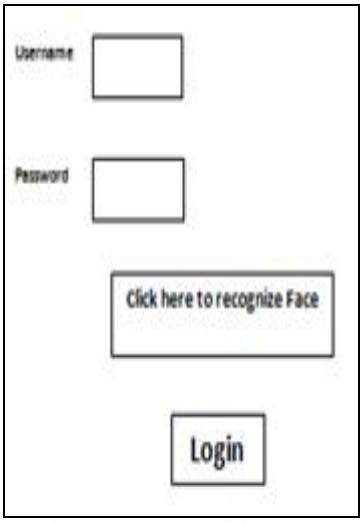


*Figure 4: Login form using face recognition*

During the registration process, user is asked to fill the details of his their account. If account holder wants face recognition option, he can upload his image. So that every time account holder can login into his account by providing face recognition along with the username and password.

Suppose, account holder is logging in the hardware facility his may omit this option but there are some chances for getting hacked.

In this work, we are going to provide a new type of security to accounts in the easiest way. The solution we are proposing for preventing hacking is that "we enter our username and password while opening our accounts", now in our method we are also providing another option which is for everyone to open their accounts.

That rule is that not only the username and password user has to provide ether face image or bio-metric. At the time of registration we register along with our own face recognition, if user is going with approach 2. At the time registration we register along with bio-metric, if we are going with apporach1.

As the technology is increased and all the laptops and systems are having camera in the systems so we can make use of this option and provide security for our accounts which is also the best and easy way to provide secure and privacy way. For bio-metric, system should have the facility to read the bio-metric of the user.

When a customer or user visits the web site for registration, user is allowed to fill the registration form by filling all the details. One of the compulsory fields is "FACE RECOGNITION". Like password and security question, user has to upload the image at the time of registration.

When a customer or user visits the web site for registration, user is allowed to fill the registration form by filling all the details. One of the compulsory fields is "BIO-METRIC". Like password and security question, user has to give Thumb press at the time of registration.

In this work, it is make sure that the accounts will never be hacked, if the user goes for either of the options. It is up to the vendors that, if the vendors provides this option as compulsory, then individuals privacy will be more, because each time user give either bio-metric or face image to login into the accounts.

**5. Advantages**

Hardware equipments are required and this system is more security than tradition system including OTP *(One Time Password)* through mobile.

**6. Sample Outputs**

BASIC APPLICATION FORM BASIC LOGIN PAGE THE BASIC LOGIN PAGE

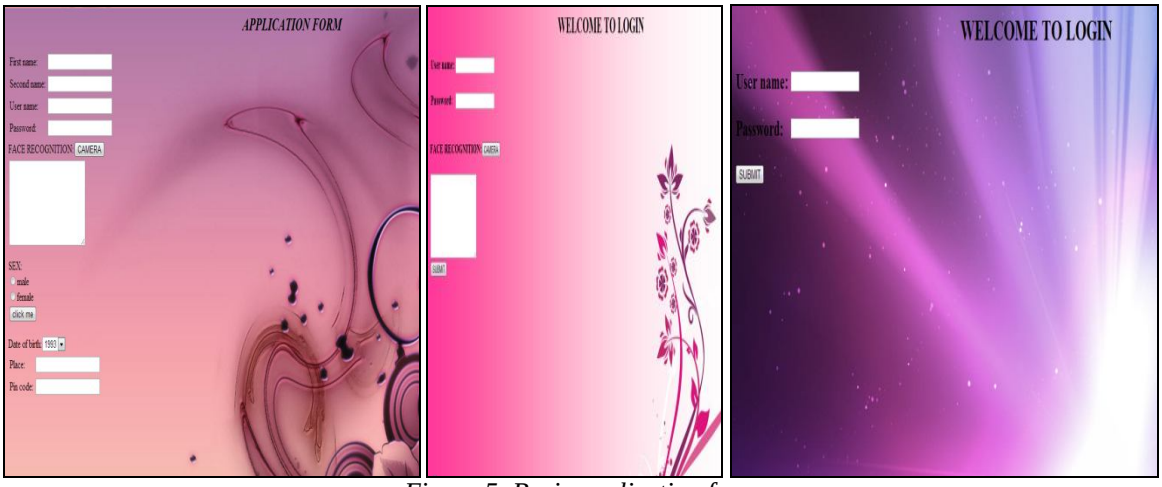


*Figure 5: Basic application form*
*Figure 6: application form for face recognition*
*Figure 7: Basic login page*

**7. Performance Evaluation**

When any new techniques are introduced, we should evaluate the performance of the proposed technique. Whether the proposed techniques satisfies the required constraints or not. In this paper we have taken privacy as main parameter to calculate the efficiency.

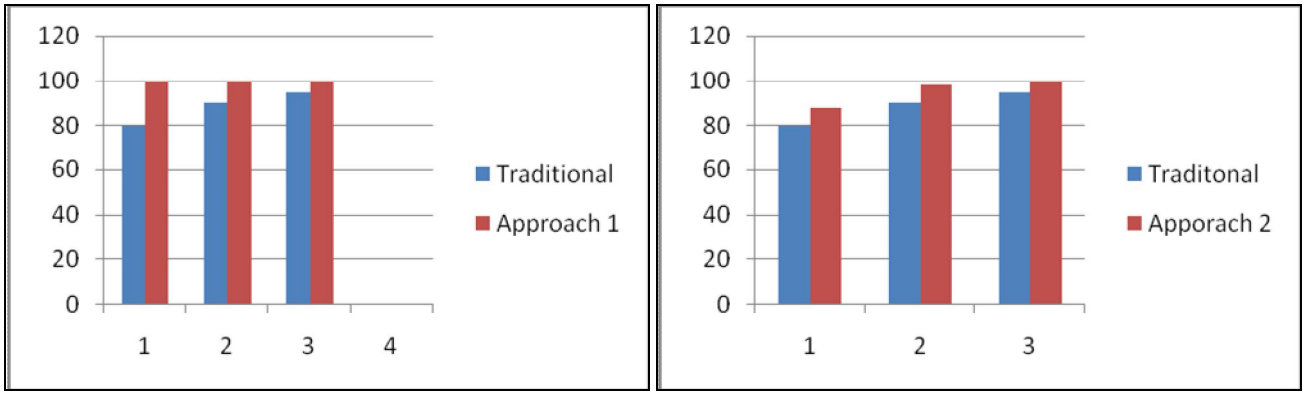


*Figure 8: Comparison of traditional system with Approach 1*
*Figure 9: Comparison of Traditional system with Approach 2*

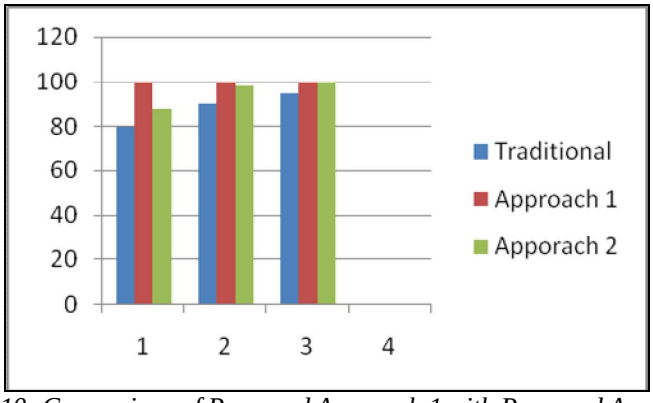


*Figure 10: Comparison of Proposed Approach 1 with Proposed Approach 2*

It is observed that proposed approach 1 gives more efficiency than proposed approach 2. Because, bio-metric of individuals will not be matched with any others.

**8. Conclusion**

From our Approach, we conclude that we can provide more security for our accounts by using image as it cannot be hacked by hackers and difficult to hack and its very new to all the users so it plays a very important role in our day-to-day lives. And people can be free from tension and can easily store the data and store it safely in their accounts. So it also gives the people some relief and free from tensions and can keep their accounts safe.

**9. References**


1. Jyothi chikkara, Ritu Dahiya, Nehgarg, Monika rani "Phishing and anti phishing techniques: a case study" in IJARSSE, may 2013.
2. http://en.wikipedia.org/wiki/Phishing.
3. Gaurav, Mukesh misra , anurag jain"Anti-Phishing technique: review published in IJERA, mar-April 2012.
4. D.Aruna Kumari, Prasamsa, Indra Praveen "Antiphishing solution based on security question and image "ICMP Trivendram , 2010.
5. A Frost & Sullivan White Paper on " Key Challenges in fighting Phishing and Pharming"
6. JungMin Kang, DoHoon Lee, "Advanced White List Approach for Preventing Access to Phishing Sites", 2007 International Conference on Convergence Information Technology, ICCIT 2007, p 491-496,2007
7. Nirmal, K.; Ewards, S.E.V.; Geetha, K.; "Maximizing online security by providing a 3 factor authentication system to counter attack 'Phishing'", in Proceedings of IEEE International Conference on Emerging Trends in Robotics and Communication Technologies, 2010.
8. Tianyang Li.; Fuye Han.; Shuai Ding and Zhen Chen "LARX: Large scale Anti-phishing by Retrospective Data Exploring Based on a Cloud Computing Platform", in Proceedings of IEEE
9. 20th International Conference on Computer Communications and Networks, 2011.
10. Qingxiang Feng.; Kuo Kun Tseng.; Jeng Shyang Pan.; Peng Cheng and Charles Chen "New Antiphishing Method with Two Types of Passwords in Open ID System", in Proceedings of IEEE Fifth International Conference on Genetic and Evolutionary Computing, 2011