ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Geographic Location Based Authentication System

Sana Dawood Khan[1], Yogeshwari S.Borse[2]

P.G. Student, Department of Computer Engineering, SSBT Engineering College, Bambhori, Jalgaon, Maharashtra, India[1]

Associate Professor, Department of Computer Engineering, SSBT Engineering College, Bambhori, Jalgaon, Maharashtra, India[2]

ABSTRACT: In today world security means everything for people specially for web application because each and every day people getting attracted to internet and it's application. Authentication is very important thing in security there is already so many technique used for authentication. Traditionally there was text password are demanding then it get replace with new techniques like Image password, Biometrics password, graphical password, map based password and further more location password from where GeoPass technique came at starting the performance of GeoPass was very good as per the memorability concern because previous techniques was efficient as per the security ,but making password more secure lead the problem of complexity of remembering password. After some time some problem came into light in GeoPass as GeoPass technique suggest to select a location which should be rememberable for user but it seen, many users select any location they found interesting on map which led to guessing attack on system. So it motivate to make system more secure as well as memorable. In the Proposed scheme at initial level the coordinate based location of selected city is provided with extension of mnemonics password. The mnemonic password is generated for selected location by using word mnemonics technique in which first letter from each location selected and make a mnemonics from selected location and substring in sequence of location selected along with annotation attributes on digital map provided for user. The result generated on basis of different threat model for existing and proposed and then compare on basis of ratio of unsuccessful attempt of login of unauthenticated user. In which proposed scheme security ratio is high for different attack models from which it conclude, a proposed solution scheme security level increase from threat by giving contribution of mnemonics password in existing scheme to make authentication more memorable and secure against online guessing attack.

KEYWORDS: Authentication, annotation, Geographic location, GPS, annoted location password, Longitude, Latitude, Geo-coding, Geo-code, Geo-coder, mnemonic password, Map Coordinates, Geopass, Geopass Note.

I. INTRODUCTION

Authentication is the only method which protects information or data of an individual or organization from a second party to access. Based upon the confidentiality of particular data or information, the level of authentication depends. Now-a-days, all this data and information what the discussion is about is getting digitized all around the world. For this digitized data or information to be secure, a proper authentication procedure must be set. This arise the need for an authentication secret which belongs to the category “Something people know” to come into picture. These secrets authenticate each secret holder as the authorized legitimate user to access their particular account. Technology is getting more advanced every day, existence and usage of online applications increase. This requires each user to remember more such authentication secrets or to reuse the same secret to access multiple accounts.

Traditional passwords may no longer be secure enough. To overcome these problems, computer scientist Bill Cheswick has devised a new method for logging into secure areas by clicking on a map. “The key idea, for which you have a data set with very deep data, and you have to drill down. You could drill down on a map of anything. Probably better if it’s a map of someplace you have never been, so you are not tempted to pick your childhood home,” said Cheswick, a scientists at AT & T research. “You could have a 10 digit latitude, and a 10 digit longitude, then you have

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

a 20 digit password [2].”By using a map with zoom, this new method renders those mouse-tracking programs useless. Sure, the virus will know where the mouse clicks, but unless it knows what map the user is looking at, and how deeply zoomed in they are, the hacking program can’t record the longitude and latitude which serve as the password.

For proposed scheme there is need of location coordinates named as latitude and longitude and to convert the location in these GPS coordinate for obtaining values of latitude and longitude for location password, in which locations are set as password on digital map for user authentication. So, to convert location address into longitude and latitude coordinates, there is a number of ways to accomplish this. You may have a GPS device which shows you these coordinates, and you could just take a reading from the GPS while at the address and note down the coordinates. There are also a number of software packages out there which provide this conversion, but you don’t particularly need to buy one of those geo-coders unless you need to geo-code a large number of addresses. (Digital Maps API also provides geo-coding of this sort, although it may not be as user-friendly to those unfamiliar with programming, and the service limits you to a certain number of requests per time period.)

About Mnemonics: Mnemonic devices are useful memory aids which can be applied to many different aspects of daily life. There are always certain tidbits of information, people just can’t seem to remember in the form they are presented. People rely on mnemonics when they create some association between the information they wish to remember and other concepts they already know, or find easier to remember. The use of mnemonics has also been shown to be of significant value in the field of education. Manalo has shown instruction using a specific type of mnemonics known as “process mnemonics” produced improvements of mathematical ability in students classified as learning disabled [3].Process mnemonics are used specifically for remembering rules and procedures. The mnemonics used in this system are used to allow the user to easily remember numerical and lexical information. Sentences can be created which exploit the properties of items to be remembered.

Expression or Word Mnemonic: This is by far the most popularly used mnemonic. To make an expression or Word mnemonic, the first letter of each item in a list is arranged to form a phrase or word.

Examples:

- In English, the 7 coordinating conjunctions are For, And, Nor, But, Or, Yet, So = FANBOYS.
- The order of operations for math is Parentheses, Exponents, Multiply, Divide, Add, and Subtract = Please Excuse My Dear Aunt Sadaf.
- The categories in the classification of life are Kingdom, Phylum, Class, Order, Family, Genus, Species,
- Variety = Kings Play Cards On Fairly Good Soft Velvet.
- Aamir wants to remember the sentence “Naziya Like Tea” So, he can remember as word mnemonic form as: NLT, first latter of each word.

A good password is often defined as one which is memorable and hard to guess. In this paper, focused is on the latter condition: the difficulty of guessing a password depends on the quality of the password selected. Memorability is no doubt important, but it may not be a necessary condition [3]. Experts sometimes frown upon users who write down their passwords. However, for online accounts, writing down many unique passwords may be preferable to reusing one password across different sites. Furthermore, password management systems, such as Password Safe, can be used to securely store passwords in encrypted form. This can be achieves by using mnemonics, here proposed scheme is use one of the mnemonics type named as “Word Mnemonic” to create a password for authentication.

II. RELATED WORK

Al-Ameen et al., in [2],GeoPass, the most promising of a class of user authentication schemes based on geographic locations in Digital maps. Study showed very high memorability and satisfactory results against online guessing attack, which means the GeoPass has compelling features for real-world use. No comprehensive study, however, has been conducted for GeoPass or any other location-based password scheme. It presents a systematic approach for the detailed evaluation of a password system, which implement to study GeoPass to evaluate the suitability of GeoPass for widespread use. It suggest it’s suitable application but still need to improved before widespread deployment could be considered.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Hung-Min Sun et al., in [10],In study of security evaluation of Geopass the 'GeoPass' application allows the user to zoom in to the maximum level and allows the user to choose a point at any zoom level at or after zoom level 16 each and every user has the same chance for selecting the authentication secret and after selection, GeoPass just places an X marker at the respective point but the proposed approach plots a marker and shows the user the latitude and longitude values on a balloon on top of the marker for a better experience. The Geopass User Authentication Scheme still have drawback like interference issues and vulnerability to shoulder surfing.

Brent MacRae et al., in [1], Geopass-Note scheme is an extension to Geopass where user select location as password similarly but with extension of annotation. Annotation is nothing but annoted location password. In this users can authenticate by using Geographic location on map by placing 'X' marker on digital map and latitude and longitude of location get selected for user as password which is highly memorable and secure way to authenticate users. It found the annotated location passwords have the ability to be stronger than text passwords against guessing attacks when proper policies are applied, thus they may be more desirable for higher-security environments. Initial thoughts were event-specific memories are what would make annotated location passwords memorable. However, it noticed some participants randomly chose places which looked interesting on the map. It raises the question of whether it is not the memories about locations, but simply locations themselves, which people remember well. Which leads to consider, as a possibility for future work, whether annotating a randomly generated location might yield the same positive results.

Mahdi Nasrullah et al., in [13],In Multiple-Password Interference in the GeoPass User Authentication scheme users can select more than one location in an online map as their password. These techniques have a potential in terms of usability and security. This scheme can further focus on different types and keywords, and figure out the correlation, if any, between the predictability of a location-password and the category of corresponding story. Which might enables to make useful suggestion for users to build a mental story.

J. Thorp et al., in [12], a video-password from any other knowledge-based authentication method is video-passwords present a video to the user, from which audio and visual cues are used upon setting a video-password. Upon subsequent logins, these cues are involved in helping the user recall his or her video password. In a video-password scheme, the video itself is an integral part of the login process.

S. Wiedenbeck et al., in [7], A Pass-Points password is a sequence of points, chosen by a user in an image which is displayed on the screen. It predicts probabilities of likely click points; which enables user to predict the entropy of a click point in a graphical password for a given image. It allows user to evaluate automatically whether a given image is well suited for the Pass-Points system, and to analyse possible dictionary attacks against the system and compare the predictions provided by model to form a results of experiments involving human users. In which stage, model and the experiments are small and limited; but they show user choice can be modelled and expansions of the model and the experiments are a promising direction of research.

It proposed a simple graphical password authentication system. System combines graphical and text-based passwords trying to achieve the best of both worlds [14].It also provides multi-factor authentication in a friendly intuitive system it also described the system operation with some examples, and highlighted important aspects of the system. So many work is done see the below.

Muath Al-Badawi et al., in [15],It demonstrated a 'Presentation Effect on Graphical Passwords' in which the presentation effect is a simple, unobtrusive, and acceptable way to modify the distribution of user choice in graphical passwords. It found image presentations significantly modified the distribution of user's first click-points, which adds an unknown element for an adversary attempting to discover the distribution of popular points for a target users background image. The results of user study indicate using the presentation effect from horizontally drawing the curtain does not have negative usability consequences. It also found the system is acceptable to users, which is sensible given, it does not limit allowable click-points on the background image. Which lead to some critical point whether the presentation effect might be useful for influencing users to create secure choices in other password schemes such as the distribution of text passwords might be benet.

Rajarajan et al., in [8], it proposed GRAMAP scheme which got three stages of authentication. Depending upon the level of security desired, users could opt for one or two or three stages. After the initial password creation, users could increase or decrease the number of stages at any time and they could also change the selected password in any particular stage. User studies were conducted on the proposed system to test its usability and memorability.

Recently images based graphical password schemes have received the attention of researchers. Human beings ability to remember images is well established [9].So, a new graphical password scheme based on geographical maps is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

proposed. The proposed scheme has got three stages of authentication. Depending upon the level of security desired, users could opt for one or two or three stages. After the initial password creation, users could increase or decrease the number of stages at any time and they could also change the selected password in any particular stage. User studies were conducted on the proposed system to test its usability and memorability.

Jermyn et al., in [6],In design and analysis of graphical passwords the graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and it show decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of one of the schemes, it devises a novel way to capture a subset of the "memorable" passwords so, people believe, is itself a contribution. First work are primarily motivated by devices such as personal digital assistants PDAs Personal Digital Assistants which offer graphical input capabilities via a stylus, and describe prototype implementation of one of the password schemes on such a PDA, namely the Palm Pilot [6].

Biddle et al., in [5], It highlighting novel features of selected schemes and identifying key usability or security advantages then review usability requirements for knowledge-based authentication as they apply to graphical passwords, identify security threats such systems must address and review known attacks and discuss methodological problems which relate to empirical evaluation, and identify areas for further research and improved methods.

There are so many threat increasing every day and so many schemes producing for them especially for web application security, because today world is internet world and mostly every one using it. A research work is done in map based authentication let see the below for more.

Zhou et al., in [16], Chaotic Map-Based Authentication scheme shows a real identity of the user is encrypted form with a shared key between the user and the trusted server and only trusted server can be able to determine the real identity of a user and any other entities including other users of the system get nothing about the users real identity also the shared key of encryption can be easily computed by the user and trusted server using the Chebyshev map without additional burdensome key management first the partnered two users are authenticated by the trusted server, they can easily apply with a agreement of the session key. Formal security analysis determines the proposed technique is safe under the random oracle model.

Graphical authentication proposed authentication scheme based on 'Colour Image Gallery' as a possible alternative solution to text-based authentication, motivated particularly by the fact 'humans can remember images better than text' in many networks, computer system and Internet-based environments try using graphical authentication techniques as their user authentication. It present a scheme as Graphical password authentication scheme based on 'Colour Image Gallery' which is very beneficial for computer related application such as web authentication, desktop, laptop logins and critical types servers.

III. GEOGRAPHIC LOCATION BASED AUTHENTICATION

It proposed a new approach for resolving problems presented in existing scheme. In proposed approach user get provided more secure and rememberable password for authentication as compare to existing scheme by extension of mnemonics password in Geopass-Note technique for better and improved system for user authentication with addition of image captcha in registration phase. It also extended approach with use of multiple locations for password selection rather than using one or two location. It select multiple location for generating mnemonics password from selected location in background of system and check the validity of system on the basis of mnemonics password generated at the time of registration phase for authenticate user only.

It is a browser-based authentication system developed using JavaScript, PHP, and Google maps API. Discussing about the digital maps, it has zoom levels from 0 to 21 where zoom level 0 is the minimum level showing the complete world map multiple times on a very small scale and zoom level 21 is the highest possible zoom which shows even every street view for a particular area it uses a minimum zoom level 3 where most of the world map is shown just once. Starting from zoom level 3, user can zoom in using the default options provided by the maps API till he/she reaches zoom level 15. At this level, the user is restricted to zoom-in further and is allowed to select the location for being the authentication secret. The point behind choosing zoom level 15 particularly is because at this point, the user will be able to select the city for which mnemonic password will generate for particular location of city. At zoom level 15, the map shows cities names and places by which the user can easily recall location password. The site first

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

show the all options home page, register and login to go further user have to decide what he/she wants to do whether he/she want to register or login.

Registration procedure: In registration process user register to get authentication for system first of all user ask to input user details to get authenticate access by filling required details this detail get stored in database for identification of authenticate users further more user have to go through captcha which comes as image chunk for validation of human. In captcha of image chunk user has given a image which is split image and there is another block of image is given user have to select the same block of image from complete image chunk. If user select the right block of image then he/she validate as human and not a robot. After successful validation digital map upload then user can select it's location for password generation by clicking on area and set flag as marker for location and by right clicking on flag one time a window open ,where user have to input the annotation to get associate with locations. After input the annotation user has to submit detail and register as authenticate user. After submitting all location the mnemonics generate for all location selected by extracting first letter from each location.

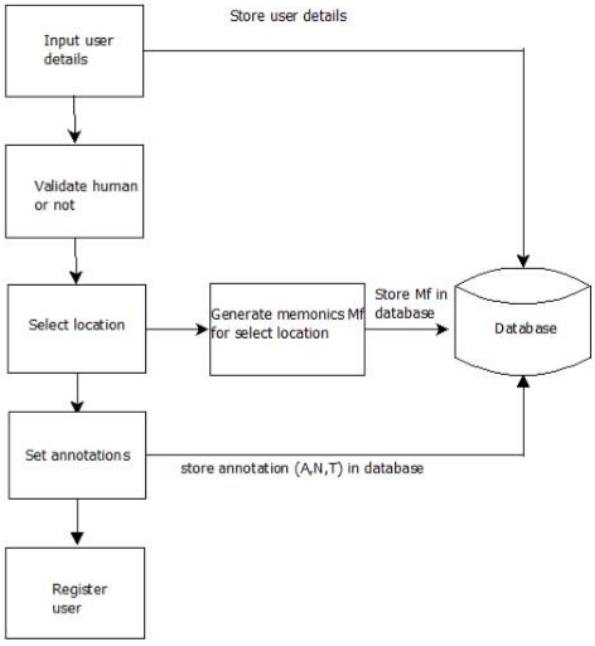

Figure 3.4: Block Diagram for Registration

Login procedure: Once the registration is complete, the particular user can get a chance to login into the system to access the contents. For which, the user needs to input details for authenticating by entering his/her respective username and password correctly if the values match with the registered one it will validate and go to map where second level of authentication done by location selection along with annotation password. Here digital map upload which is provided by Google by using it's API. Now user have to select it's location from digital map as per the same sequence he/she selected the location at the time of registration phase by click on map and set a marker position which display as flag on map after setting flag user have to click on flag to submit annotation as Name, Address and Type attributes and then submit details done the same process for all number of location user have selected at the time of registration(here authenticate user)from this locations a mnemonics password get generate for selected location and it check with the original mnemonics password which is stored in data base at the time of registration. It checks both mnemonics if they match then user is validated and get access successfully.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

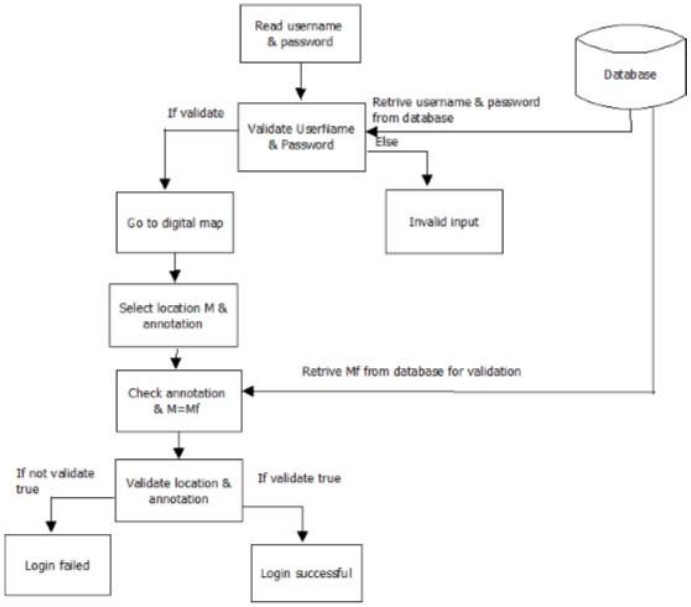

Figure 3.5: Block Diagram for Login

IV. EXPERIMENTAL RESULTS

A study conduct for 30 user who are un-authenticate users trying to attempt to get access to authorize user account as basis of existing system results of attack model ratio and proposed system result it clearly show the ratio of unsuccessful attacks is grater for proposed scheme as compare to existing scheme. Which shows the efficiency of proposed scheme which is more than existing scheme makes proposed system more secure for authentication.

It gives the comparison model of existing and proposed scheme based on attack models as

- Unknown Adversary
- Known Adversary
- Local knowledge

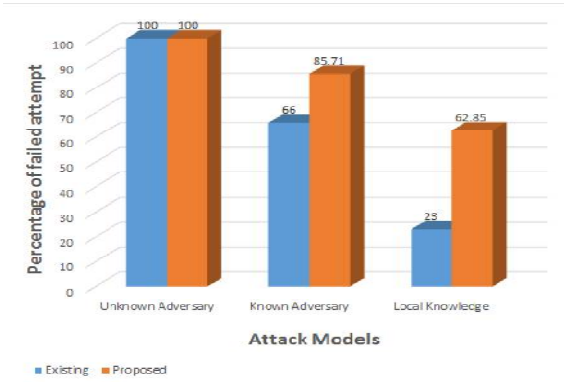

Figure 2: Comparison Based on Attack Models Chart

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Attack Models	Existing system		system safety
	Attack attempt taken	Failed Login	
Unknown adversary	35	35	100%
known adversary	35	23	66%
Local knowledge	35	8	23%

Table 1: Guessing Attacks Under Different Threat Models for Existing System

Attack Models	Proposed system		system safety
	Attack attempt taken	Failed Login	
Unknown adversary	35	35	100%
known adversary	35	30	85.71%
Local knowledge	35	22	62.85%

Table 2: Guessing Attacks Under Different Threat Models for Proposed System

Experimental Analysis: To get result a test is conducted on a basis of survey for analyzing performance of proposed system by showing it's efficiency as per the result generated from comparison of existing and proposed system security ratio according to guessing Attacks Under Different Threat Models for existing and proposed.

Experimental Results: For proposed system result is generated on the basis of security ratio of guessing attacks under Different Threat Models for existing and proposed schema by comparing the result of security of systems result is given for proposed scheme.

System security ratio:

1. Unknown Adversary:

For Existing system ,from 35 user the 35 user failed to login ,similarly for proposed system 35 user out of 35 user failed to login ,means system is highly secure ,so the ratio of system security will be as follow,

For Existing,

Failed login =35/35

=100%

For proposed,

Failed login = 35/35

=100%

Where,

100% = 100%

2. Known Adversary:

For Existing system ,32 user from 35 user failed to login, but for proposed system 30 users out of 35 failed to login ,So the ratio of system security will be as follow,

For Existing,

Failed login = 23/35

=66%

For Proposed,

Failed login = 30/35

=85.71%

Where,

87.71% > 66%

Which means at the level of known adversary the system security ratio of proposed system is greater than existing system; indicate the proposed system is more secure than existing system for known adversary attack.

3. Local Knowledge:

For Existing system ,8 user from 35 user failed to login, but for proposed system 22 users out of 35 failed to login ,So the ratio of system security will be as follow,

For Existing,

Failed login = 8/35

=23%

For Proposed,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Failed login = 22/35
=62.85%

Where,

62.85% > 23%

Which means at the level of local knowledge attack model the system security ratio of proposed system is greater than existing system; indicate the proposed system is more efficient than existing system for known adversary attack.

V. CONCLUSION

There are so many techniques available now a day but still there is need of more authenticate and attractive ways to authenticate users for security purpose. The most important issue of today's authentication method is difficulty of remembering of password because of complex passwords which made to make system more secure and reliable for user. To avoid this proposed solution is given, in this user select locations as password along with annotation by creating mnemonic password of location selected for better authentication, so user not only authenticate at higher level but also remember password because of attractive approach of location selection for password generation.

REFERENCES

[1] B. MacRae, A. Salehi-Abari, and J. Thorpe, "An exploration of geographic authentication schemes,"IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1997–2012, 2016.
[2] M. N. Al-Ameen and M. Wright, "A comprehensive study of the geopass user authentication scheme,"arXiv preprint arXiv:1408.2852, 2014.
[3] S. Chowdhury, R. Poet, and L. Mackenzie, "A study of mnemonic image passwords," in Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on. IEEE, 2014, pp. 207–214.
[4] C. Kuo, S. Romanosky, and L. F. Cranor, "Human selection of mnemonic phrase-based passwords," in Proceedings of the second symposium on Usable privacy and security. ACM, 2006, pp. 67–78.
[5] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys (CSUR), vol. 44, no. 4, p. 19, 2012.
[6] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords." USENIX Association, 1999.
[7] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 20–28.
[8] S. Rajarajan, M. Prabhu, S. Palanivel, and M. Karthikeyan, "Gramap: Three stage graphical password authentication scheme." Journal Of Theoretical & Applied Information Technology, vol. 61, no. 2, 2014.
[9] M. N. Al-Ameen, M. Wright, and S. Scielzo, "Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues," in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, 2015, pp. 2315–2324.
[10] J. Thorpe, B. MacRae, and A. Salehi-Abari, "Usability and security evaluation of geopass: a geographic location-password scheme," in Proceedings of the Ninth symposium on usable privacy and security.ACM, 2013, p. 14.
[11] S. D. Ghogare, S. P. Jadhav, A. R. Chadha, and H. C. Patil, "Location based authentication: A new approach towards providing security," International Journal of Scientific and Research Publications,vol. 2, no. 4, pp. 2250–3153, 2012.
[12] J. Thorpe, A. Salehi-Abari, and R. Burden, "Video-passwords: advertising while authenticating," in Proceedings of the 2012 workshop on New security paradigms. ACM, 2012, pp. 127–140.
[13] M. N. Al-Ameen and M. Wright, "Multiple-password interference in the geopass user authentication scheme," in Proc. Workshop Usable Secur.(USEC), 2015, pp. 1–6.
[14] A. Almulhem, "A graphical password authentication system," in Internet Security (WorldCIS), 2011 World Congress on. IEEE, 2011, pp. 223–225.
[15] J. Thorpe, M. Al-Badawi, B. MacRae, and A. Salehi-Abari, "The presentation effect on graphical passwords," in proceedings of the SIGCHI conference on human factors in computing systems. ACM,2014, pp. 2947–2950.
[16] Y. Zhou, J. Zhou, F. Wang, and F. Guo, "An efficient chaotic map-based authentication scheme with mutual anonymity," Applied Computational Intelligence and Soft Computing, vol. 2016, 2016.

BIOGRAPHY

It is a great pleasure and moment of immense satisfaction for me to express my profound gratitude to Head of Department of Computer engineering, **Dr. Prof. G. K. Patnaik** for his valuable advice and guidance. I acknowledge all the staff members of the department of Computer Engineering, SSBT's College of Engineering & Technology for their help and suggestions during various phases of project work. Great thanks to my mother **Ms. Durreshehwar Dawood Khan** , family and friends and to those who helped me directly or indirectly for completion of thesis work.