International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 1 Issue 6, October 2014

Attack Resistant User Authentication using Visual Verification Mechanism

Ms. V.Karthikeyani
II Year M.E(CSE)
Shree Venkateshwara Hi-Tech Engg College, Gobi
mahe11191@gmail.com

Dr. T. Senthil Prakash
Professor & HOD
Shree Venkateshwara Hi-Tech Engg College, Gobi
jtyesp@yahoo.co.in

Ms. S. Rabiyathul Basiriya
II Year M.E(CSE)
Shree Venkateshwara Hi-Tech Engg College, Gobi
rabiyasabu19@gmail.com

Abstract- *Captcha as graphical passwords (CaRP) is a graphical password scheme used for user authentication. Online guessing attacks, relay attacks and shoulder surfing attacks are handled in CaRP. CaRP is click-based graphical passwords where a sequence of clicks on an image is used to derive a password. Dynamic captcha challenge image is used for each login attempt in CaRP. Text Captcha and image-recognition Captcha are used in CaRP scheme. Text CaRP scheme constructs the password by clicking the right character sequence on CaRP images. CaRP schemes can be classified into two categories recognition based CaRP and recognition-recall based CaRP. Recognition-based CaRP seems to have access to an infinite number of different visual objects. Recognition-recall based CaRP requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall. Password information is transferred and verified using hash codes. Secure channels between clients and the authentication server through Transport Layer Security (TLS).*

The CaRP scheme is enhanced with strength analysis and security features. Pattern based attacks are handled with Color and Spatial patterns. Pixel colors in click points are considered in the color pattern analysis model. Pixel location patterns are considered in the spatial pattern analysis model.

Keywords: Captcha as graphical passwords, image-recognition Captcha, Text Captcha

1. INTRODUCTION

Beginning around 1999, a multitude of graphical password schemes have been proposed, motivated by the promise of improved password memorability and thus usability, while at the same time improving strength against guessing attacks. Like text passwords, graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. However, where text passwords involve alphanumeric and/or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images or sketches.

Despite the large number of options for authentication, text passwords remain the most common choice for many reasons. They are easy and inexpensive to implement; are familiar to essentially all users; allow users to authenticate themselves while avoiding privacy issues that have been raised about biometrics; and have the advantage of portability without, for example, having to carry physical tokens. However, text passwords also suffer from both security and usability disadvantages -- for example, passwords are typically difficult to remember, and are predictable if user-choice is allowed.

One proposal to reduce problems related to text passwords is to use password managers. These typically require that users remember only a master password. They store and send on behalf of the user the appropriate passwords to web sites hosting user accounts. Ideally the latter are generated by the manager itself and are stronger than user-chosen passwords. However, implementations of password managers introduce their own usability issues that can exacerbate security problems, and their centralized architecture introduces a single point of failure and attractive target: attacker access to the master password provides control over all of the user's managed accounts.

When text password users resort to unsafe coping strategies, such as reusing passwords across accounts to help with memorability, the decrease in security cannot be addressed by simply strengthening, in isolation, the underlying technical security of a system. Usability issues often significantly impact its real-world security. User interface design decisions may unintentionally sway user behaviour towards less secure behaviour. Successful authentication solutions must thus also include improved usability design based on appropriate research taking into account the abilities and limitations of the target users. In graphical passwords, human memory for visual information is

leveraged in hope of a reduced memory burden that will facilitate the selection and use of more secure or less predictable passwords, dissuading users from unsafe coping practices.

Early surveys of graphical passwords are available. More recent papers briefly summarize and categorize 12 schemes and review numerous graphical password systems while offering usability guidelines for their design. In this paper we provide a comprehensive review of the first twelve years of published research on graphical passwords, and reflect on it. It is now clear that the graphical nature of schemes does not by itself avoid the problems typical of text password systems. However, while proposals in this first period of research exhibit some familiar problems, we see signs that an emerging second generation of research will build on this knowledge and leverage graphical elements in new ways to avoid the old problems.

2. RELATED WORKS

2.1. Graphical Passwords

A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. Each type will be briefly described here. More can be found in a recent review of graphical passwords [1].

A recognition-based scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Passfaces [2] wherein a user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted. Story is similar to Passfaces but the images in the portfolio are ordered, and a user must identify her portfolio images in the correct order. Deja Vu is also similar but uses a large set of computer generated "random-art" images. Cognitive Authentication [5] requires a user to generate a path through a panel of images as follows: starting from the top-left image, moving down if the image is in her portfolio, or right otherwise. The user identifies among decoys the row or column label that the path ends. This process is repeated, each time with a different panel. A successful login requires that the cumulative probability that correct answers were not entered by chance exceeds a threshold within a given number of rounds.

A recall-based scheme requires a user to regenerate the same interaction result without cueing. Draw-A-Secret (DAS) was the first recall-based scheme proposed. A user draws her password on a 2D grid. The system encodes the sequence of grid cells along the drawing path as a user drawn password. Pass-Go [4] improves DAS's usability by encoding the grid intersection points rather than the grid cells. BDAS [6] adds background images to DAS to encourage users to create more complex passwords.

In a cued-recall scheme, an external cue is provided to help memorize and enter a password. PassPoints is a widely studied click-based cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password, and re-clicks the same sequence during authentication. Cued Click Points (CCP) [8] is similar to PassPoints but uses one image per click, with the next image selected by a deterministic function. Persuasive Cued Click Points (PCCP) [9] extends CCP by requiring a user to select a point inside a randomly positioned viewport when creating a password, resulting in more randomly distributed click-points in a password.

Among the three types, recognition is considered the easiest for human memory whereas pure recall is the hardest. Recognition is typically the weakest in resisting guessing attacks. Many proposed recognition-based schemes practically have a password space in the range of 2^{13} to 2^{16} passwords A study reported that a significant portion of passwords of DAS and Pass-Gowere successfully broken with guessing attacks using dictionaries of 2^{31} to 2^{41} entries, as compared to the full password space of 2^{58} entries. Hotspots were exploited to mount successful guessing attacks on PassPoints a significant portion of passwords were broken with dictionaries of 2^{26} to 2^{35} entries, as compared to the full space of 2^{43} passwords.

2.2. Captcha

Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. There are two types of visual Captcha: text Captcha and Image-Recognition Captcha (IRC). The former relies on character recognition while the latter relies on recognition of non-character objects. Security of text Captchas has been extensively studied. The following principle has been established: text Captcha should rely on the difficulty of character segmentation, which is computationally expensive and combinatorial hard.

Machine recognition of non-character objects is far less capable than character recognition. IRCs rely on the difficulty of object identification or classification, possibly combined with the difficulty of object segmentation. Asirra relies on binary object classification: a user is asked to identify all the cats

from a panel of 12 images of cats and dogs. Security of to machine-learning attacks. IRCs based on binary object classification or identification of one concrete type of objects are likely insecure. Multi-label classification problems are considered much harder than binary classification problems. Captcha can be circumvented through relay attacks whereby Captcha challenges are relayed to human solvers, whose answers are fed back to the targeted application.

2.3. Captcha in Authentication

It was introduced to use both Captcha and password in a user authentication protocol, which we call Captcha-based Password Authentication (CbPA) protocol, to counter online dictionary attacks. The CbPA-protocol requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access. An improved CbPA-protocol is proposed by storing cookies only on user-trusted machines and applying a Captcha challenge only when the number of failed login attempts for the account has exceeded a threshold. It is further improved by applying a small threshold for failed login attempts from unknown machines but a large threshold for failed attempts from known machines with a previous successful login within a given time frame.

Captcha was also used with recognition-based graphical passwords to address spyware, wherein a text Captcha is displayed below each image; a user locates her own pass-images from decoy images, and enters the characters at specific locations of the Captcha below each pass-image as her password during authentication. These specific locations were selected for each pass-image during password creation as a part of the password. In the above schemes, Captcha is an independent entity, used together with a text or graphical password. On the contrary, a CaRP is both a Captcha and a graphical password scheme, which are intrinsically combined into a single entity.

3. CAPTCHA AND GRAPHICAL PASSWORD SCHEMES

A fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. For example, the problem of integer factorization is fundamental to the RSA public-key cryptosystem and the Rabin encryption. The discrete logarithm problem is fundamental to the ElGamal encryption, the Diffie-Hellman key exchange, the Digital Signature Algorithm, the elliptic curve cryptography and so on.

Using hard AI (Artificial Intelligence) problems for security, initially proposed is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, beyond the capability of computers but easy for humans. Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. The new paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications. In this paper, we introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which we call CaRP. CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt.

The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple-object classification can be converted to a CaRP scheme. We present exemplary CaRPs built on both text Captcha and image-recognition Captcha. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images. CaRP offers protection against online dictionary attacks on passwords, which have been for long time a major security threat for various online services. This threat is widespread and considered as a top cyber security risk [3]. Defense against online dictionary attacks is a more subtle problem than it might appear. Intuitive countermeasures such as throttling logon attempts do not work well for two reasons: 1) It causes denial-of-service attacks and incurs expensive helpdesk costs for account reactivation. 2) It is vulnerable to global password attacks whereby adversaries intend to break into any account rather than a specific one, and thus try each password candidate on multiple accounts and ensure that the number of trials on each account is below the threshold to avoid triggering account lockout.

CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection, wherein Captcha challenges are relayed to humans to solve. Koobface [12] was a relay attack to bypass Facebook's Captcha in creating new accounts. CaRP is robust to shoulder-surfing attacks if combined with dual-view technologies. CaRP requires solving a Captcha challenge in every login. This impact on usability can be mitigated by adapting the CaRP image's difficulty level based on the login history of the account and the machine used to log in. Typical application scenarios for CaRP include:

1) CaRP can be applied on touch-screen devices whereon typing passwords is cumbersome, esp. for secure Internet applications such as e-banks. Many e-banking systems have applied Captchas in user logins. For example, ICBC (www.icbc.com.cn), the largest bank in the world, requires solving a Captcha challenge for every online login attempt.

2) CaRP increases spammer's operating cost and thus helps reduce spam emails. For an email service provider that deploys CaRP, a spam bot cannot log into an email account even if it knows the password. Instead, human involvement is compulsory to access an account. If CaRP is combined with a policy to throttle the number of emails sent to new recipients per login session, a spam bot can send only a limited number of emails before asking human assistance for login, leading to reduced outbound spam traffic.

4. PROBLEM STATEMENT

Captcha as graphical passwords (CaRP) is a graphical password scheme used for user authentication. Online guessing attacks, relay attacks and shoulder surfing attacks are handled in CaRP. CaRP is click-based graphical passwords where a sequence of clicks on an image is used to derive a password. Dynamic captcha challenge image is used for each login attempt in CaRP. Text Captcha and image-recognition Captcha are used in CaRP scheme. Text CaRP scheme constructs the password by clicking the right character sequence on CaRP images. CaRP schemes can be classified into two categories recognition based CaRP and recognition-recall based CaRP. Recognition-based CaRP seems to have access to an infinite number of different visual objects. Recognition-recall based CaRP requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall. Password information is transferred and verified using hash codes. Secure channels between clients and the authentication server through Transport Layer Security (TLS). The following problems are identified from the existing system.

- Click point relationship are not analyzed
- Directory attacks are not handled
- Device dependant shoulder surfing attack handling mechanism
- Hash code security is not considered

5. CAPTCHA AS GRAPHICAL PASSWORDS (CARP)

In CaRP, a new image is generated for every login attempt, even for the same user. CaRP uses an alphabet of visual objects to generate a CaRP image, which is also a Captcha challenge. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. CaRP schemes are clicked-based graphical passwords. According to the memory tasks in memorizing and entering a password, CaRP schemes can be classified into two categories: recognition and a new category, recognition-recall, which requires recognizing an image and using the recognized objects as cues to enter a password [7]. Recognition-recall combines the tasks of both recognition and cued-recall and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space. Exemplary CaRP schemes of each type will be presented later.

5.1. Converting Captcha to CaRP

In principle, any visual Captcha scheme relying on recognizing two or more predefined types of objects can be converted to a CaRP. All text Captcha schemes and most IRCs meet this requirement. Those IRCs that rely on recognizing a single predefined type of objects can also be converted to CaRPs in general by adding more types of objects [11]. In practice, conversion of a specific Captcha scheme to a CaRP scheme typically requires a case by case study, in order to ensure both security and usability. We will present several CaRPs built on top of text and image-recognition Captcha schemes. Some IRCs rely on identifying objects whose types are not predefined. A typical example is Cortcha which relies on context-based object recognition wherein the object to be recognized can be of any type. These IRCs cannot be converted into CaRP since a set of pre-defined object types is essential for constructing a password.

5.2. User Authentication With CaRP Schemes

Like other graphical passwords, we assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS). A typical way to apply CaRP schemes in user authentication is as follows [10]. The authentication server AS stores a salt s and a hash value H(ρ, s) for each user ID, where ρ is the password of the account and not stored. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. Upon receiving a login request, AS generates a CaRP image, records the locations of the objects in the image, and sends the image to the user to click her password. The coordinates of the clicked points are recorded and sent to the user ID. AS maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable

points of visual objects, ρ, that the user clicked on the image. Then AS retrieves salt s of the account, calculates the hash value of ρ' with the salt, and compares the result with the hash value stored for the account. Authentication succeeds only if the two hash values match. This process is called the basic CaRP authentication.

Advanced authentication with CaRP challenge-response will be presented. We assume in the following that CaRP is used with the basic CaRP authentication unless explicitly stated otherwise. To recover a password successfully, each user-clicked point must belong to a single object or a clickable-point of an object. Objects in a CaRP image may overlap slightly with neighboring objects to resist segmentation. Users should not click inside an overlapping region to avoid ambiguity in identifying the clicked object. This is not a usability concern in practice since overlapping areas generally take a tiny portion of an object.

6. User Authentication using Visual Verification Mechanism

The CaRP scheme is enhanced with strength analysis and security features. Pattern based attacks are handled with Color and Spatial patterns. Pixel colors in click points are considered in the color pattern analysis model. Pixel location patterns are considered in the spatial pattern analysis model. Dictionary attacks and transmission attacks handling process is also improved with high security. Password security level assessment mechanism is used in the graphical password construction process. Cryptography (RSA) and data integrity (SHA) schemes are also integrated with the system to improve the security level in online applications. CAPTCHA and graphical password schemes are used for the user authentication process. Pixel physical and spatial properties are used in the strength analysis process. Transmission security is improved with integrity verification mechanisms. The system is divided into six major modules. They are CaRP with Text CAPTCHA, authentication server, CaRP with image Recognition CAPTCHA, pattern analysis, attack handler and enhanced CaRP scheme.

Character sequence selection is used in CaRP with Text CAPTCHA scheme. The authentication server is designed to manage and verify the user accounts. CaRP with Image Recognition CAPTCHA scheme uses the recognition and recall mechanism with image objects. The color and spatial patterns are analyzed under the pattern analysis module. The directory and shoulder surfing attacks are handled under attack handler module. Enhanced CaRP Scheme integrates the security and attack control mechanism for user authentication process.

6.1. CaRP with Text CAPTCHA

Textual characters based CAPTCHA is used in Text CaRP scheme. Password is constructed by selecting character sequences in the text CAPTCHA collection. The textual CAPCHA characters are dynamically rearranged at the time of recognition process. Password details are converted into hash codes and applied in verification process.

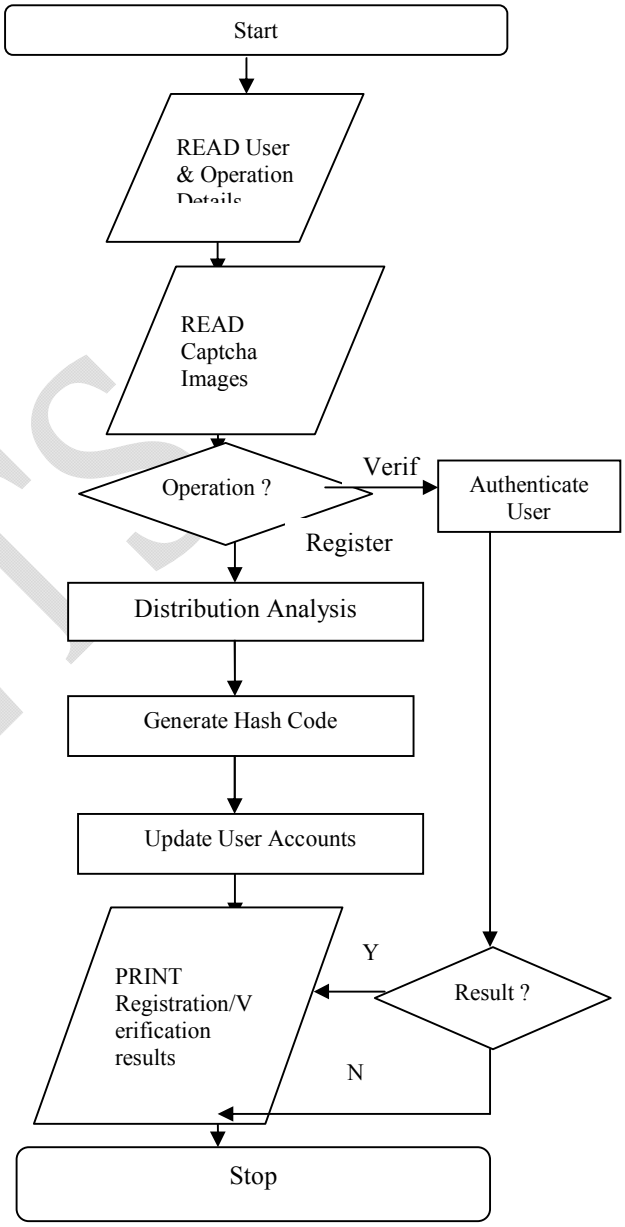

Fig. No: 6.1. Visual Verification based User Authentication Scheme

6.2. Authentication Server

The authentication server application is used to authenticate the users. User registration and password management operations are carried out

under the server. Password verification is carried out under the server. Key and signature values are maintained under the server.

6.3. CaRP with Image Recognition CAPTCHA

Image objects are used in recognition-recall based CaRP Recognition CAPTCHA. Object recognition and click cue identification mechanism are used in the system. Rectangular regions are used in the cued recall process. CAPTCHA-Zoo image object collection is used for the password construction process.

64. Pattern Analysis

Color and spatial patterns are analyzed in the system. Pixel color for click points are used in the color pattern analysis. Spatial patterns are extracted from location information. Password complexity is assessed with pattern information.

6.5. Attack Handler

Directory and shoulder surfing attacks are managed by the system. RSA algorithm is used to perform password encryption/decryption tasks. Image dimming mechanism is used to control shoulder surfing attacks. Mouse cursor size and location are automatically adjusted for attack handling process.

6.6. Enhanced CaRP Scheme

CaRP scheme and attack handling mechanism are integrated in the Enhanced CaRP scheme. Distribution, strength and pattern analysis schemes are integrated with CaRP scheme. The Secure hashing algorithm (SHA) is used to generate password signatures. Reusability level is analyzed.

7. Conclusion

The graphical passwords are used to ensure the high level security for the remote logins. CAPTCHA techniques are used to verify the source type of request. Captcha as Graphical Passwords scheme integrates the text and image captchas to construct graphical password scheme. CaRP scheme is enhanced with strength based password construction and attack resistant user authentication model. Password complexity prediction system is integrated to improve password construction process. The system increases the success and recall rates. User interface is upgraded to avoid capture attacks in password recall process. Efficient shoulder surfing attack controlling models are used to protect the system from attackers.

References

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, 2012.
[2] The Science Behind Passfaces [Online]. http://www.realuser.com/published/ScienceBehindPassfaces.pdf
[3] HP TippingPoint DVLabs, Vienna, Austria. Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online]. Available: http://dvlabs.tippingpoint.com/toprisks 2010.
[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.
[5] D. Weinshall, "Cognitive authentication schemes safe against spyware," in Proc. IEEE Symp, 2006.
[6] P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret' graphical passwords," in Proc. ACM CCS, 2007.
[7] Napa Sae-Bae and Kowsar Ahmed, "Multitouch Gesture-Based Authentication", IEEE Transactions On Information Forensics And Security, April 2014.
[8] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007, pp. 359–374.
[9] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in Proc. Brit. HCI Group Annu. Conf. vol. 1. 2008.
[10] Sooyeon Shin and Sarang Na, "Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected", IEEE Transactions On Systems, Man, And Cybernetics: Systems, June 2014.
[11] Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014
[12] N. Joshi. Koobface Worm Asks for CAPTCHA Online]. Available: http://blogs.mcafee.com/mcafee-labs/koobface-worm-asksfor- CAPTCHA, 2009

AUTHORS BIOGRAPHY

MS.V.Karthikeyani pursuing M.E(CSE) degree from Shree Venkateshwara Hi-Tech engineering college, Erode, India in 2014 and B.E(CSE) degree from Nandha College of Technology, Erode, India in 2013. She has attend a National conference on Cloud Security and 2 workshops. Her research interests include Network Security, Data mining.

Dr.T.Senthil Prakash received the Ph.D. degree from the PRIST University, Thanjavur, India in 2013 and M.E(CSE) degree from Vinayaka Mission's University, Salem , India in 2007 and M.Phil.,MCA.,B.Sc(CS) degrees from Bharathiyar University, Coimbatore India, in 2000,2003 and 2006 respectively, all in Computer Science and Engineering. He is a Member in ISTE New Delhi, India, IAENG, Hong Kong..IACSIT, Singapore SDIWC, USA. He has the experience in Teaching of 10+Years and in Industry 2 Years. Now He is currently working as a Professor and Head of the Department of Computer Science and Engineering in Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamil Nadu, and India. His research interests include Data Mining, Data Bases, Artificial Intelligence, Software Engineering etc.,He has published several papers in 17

International Journals, 43 International and National Conferences.

Ms.S.Rabiyathul Basiriya pursuing M.E(CSE) degree in Shree Venkateshwara Hi-Tech Engineering College, Erode, India in 2014 and B.E(CSE) degree from Sri Ramakrishna Institute of Technology, Coimbatore, India in 2013. She has published 1 National conferences, 4 workshops. She is a Member of Computer Society of India(CSI).Her research interests include Data Mining, Networks.