AN AUTHENTICATED AND SECURED CREDENTIAL PROTECTION SYSTEM FOR MOBILE ENVIRONMENT

Ms. Sivaraju Sai Krishna Deepthi #1, Ms. Sangu Maheswari #2, Ms. Panyam Guru Tejaswini #3, Mr. Chinthamaneni Saiabhilash #4, Mrs.K.V. Nagalakshmi #5

#1 Student, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam (Dt) India.
#2 Student, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam (Dt) India.
#3 Student, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam (Dt) India.
#4 Student, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam (Dt) India.
#5 Assistant Professor, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam

Abstract

Validation dependent on passwords is utilized to a great extent in applications for PC security and protection. In any case, human activities, for example, picking awful passwords and contributing passwords in an uncertain way are viewed as "the weakest connection" in the verification chain. Instead of subjective alphanumeric strings, clients will in general pick passwords either short or significant for simple retention. With web applications and portable applications heaping up, individuals can get to these applications whenever and anyplace with different gadgets. This advancement brings extraordinary accommodation yet additionally expands the likelihood of presenting passwords to bear surfing assaults. Assailants can watch straightforwardly or utilize outside chronicle gadgets to gather clients' qualifications. To defeat this issue, we proposed a novel confirmation framework PassMatrix, in light of graphical passwords to oppose bear surfing assaults. With a one-time legitimate login marker and circulative level and vertical bars covering the whole extent of pass-pictures, PassMatrix offers no indication for aggressors to make sense of or restricted down the secret word even they lead different camera-based assaults. We additionally executed a PassMatrix model on Android and did genuine client trials to assess its memorability and ease of use. From the test result, the proposed framework accomplishes better protection from shoulder surfing assaults while looking after ease of use.

Keywords: *Validation, graphical passwords, security.*

I. INTRODUCTION

Printed passwords have been the most broadly utilized verification strategy for quite a long time. Contained numbers and upper-and lower-case letters, printed passwords are viewed as sufficiently able to oppose against animal power assaults. Be that as it may, a solid literary secret phrase is difficult to remember and recall . Thusly, clients will in general pick passwords that are either short or from the word reference, instead of arbitrary alphanumeric strings. Surprisingly more terrible, it's anything but an uncommon case that clients may utilize just a single username and secret word for numerous records. As indicated by an article in Computer world, a security group at an extensive organization ran a system secret phrase saltine and shockingly split around 80% of the workers' passwords inside 30 seconds . Printed passwords are frequently unreliable because of the trouble of keeping up solid ones. Different graphical secret phrase verification plans were created to address the issues and shortcomings related with printed passwords. In view of certain investigations, for example, those in people have a superior capacity to remember pictures with long haul memory (LTM) than verbal portrayals. Picture based passwords were ended up being less demanding to recall in a few client examines . Accordingly, clients can set up an intricate verification secret word and are fit for remembering it after quite a while regardless of whether the memory isn't actuated intermittently. Notwithstanding, the vast majority of these picture based passwords are defenseless against shoulder surfing assaults (SSAs). This sort of assault either utilizes direct perception, for example, looking out for somebody's shoulder or applies video catching strategies to get passwords, PINs, or other touchy individual data . The human activities, for example, picking awful passwords for new records and contributing passwords in an unreliable path for later logins are viewed as the weakest connection in the validation chain [16]. In this way, a confirmation plan ought to be intended to conquer these vulnerabilities. In this paper, we present a safe graphical verification framework named PassMatrix that shields clients from getting to be casualties of shoulder surfing assaults while contributing passwords out in the open through the utilization of one-time login pointers. A login marker is arbitrarily produced for each pass-picture and will be pointless after the session ends. The login marker gives better security against shoulder surfing assaults, since clients utilize a dynamic pointer to call attention to the situation of their passwords instead of tapping on the secret phrase object specifically Motivation As the portable promoting.

II RELATED WORK

In the past several decades, a lot of research on password authentication has been done in the literature. Among all of these proposed schemes, this paper focuses mainly on the graphical-based authentication systems. To keep this paper concise, we will give a brief review of the most related schemes that were mentioned in the previous section. Many other schemes such as those in [27], [28], [29], [30], [31] may have good usability, they are not graphical-based and need additional support from extra hardware such as audio, multi-touch monitor, vibration sensor, or gyroscope, etc. In the early days, the graphical capability of handheld devices was weak; the color and pixel it could show was limited. Under this limitation, the Draw-a-Secret (DAS) [6] technique was proposed by Jermyn et al. in 1999, where the user is required to re-draw a pre-defined picture on a 2D grid. We directly extract the figure from [6]. If the drawing touches the same grids in the same sequence, then the user is authenticated. Since then, the graphical capability of handheld devices has steadily and ceaselessly improved with the advances in science and technology. In 2005, Susan Wiedenbeck et al. introduced a graphical authentication scheme PassPoints [7], and at that time, handheld devices could already show high resolution color pictures. Using the PassPoint scheme, the user has to click on a set of pre-defined pixels on the predestined photo, as shown in Figure 1(a) (this figure is extracted from [7]), with a correct sequence and within their tolerant squares during the login stage. Moreover, Marcos et al. also extended the DAS based on finger-drawn doodles and pseudosignatures in recent mobile device [32], [33].

This authentication system is based on features which are extracted from the dynamics of the gesture drawing process (e.g., speed or acceleration). These features contain behavioral biometric characteristic. In other words, the attacker would have to imitate not only what the user draws, but also how the user draws it. However, these three authentication schemes are still all vulnerable to shoulder surfing attacks as they may reveal the graphical passwords directly to some unknown observers in public. In addition to graphical authentication schemes, there was some research on the extension of conventional personal identification number (PIN) entry authentication systems. In 2004, Roth et al. [34] presented an approach for PIN entry against shoulder surfing attacks by increasing the noise to observers. In their approach, the PIN digits are displayed in either black or white randomly in each round. The user must respond to the system by identifying the color for each password digit. After the user has made a series of binary choices (black or white), the system can figure out the PIN number the user intended to enter by intersecting the user's choices. This approach could confuse the observers if they just watch the screen without any help of video capturing devices. However, if observers are able to capture the whole authentication process, the passwords can be cracked easily.

In order to defend the shoulder surfing attacks with video capturing, FakePointer [35] was introduced in 2008 by T. Takada. We use Figure 2 (from [35]) below to show the usage of FakePointer. In addition to the PIN number, the user will get a new ”answer indicator” each time for the authentication process at a bank ATM. In other words, the user has two secrets for authentication: a PIN as a fixed secret and an answer indicator as a disposable secret. The answer indicator is a sequence of n shapes if the PIN has n digits. At each login session, the FakePointer interface will present the user an image of a numeric keypad with 10 numbers (similar to the numeric keypad for phones), with each key (number) on top of a randomly picked shape. The numeric keys, but not the shapes, can be moved circularly using the left or right arrow keys. During authentication, the user must repeatedly move numeric keys circularly as shown in the leftmost figure in Figure 2, until the first digit of the PIN overlaps the first shape of the answer indicator on the keypad and then confirm a selection by pressing the space key. This operation is repeated until all the PIN digits are entered and confirmed. This approach is quite robust even when the attacker captures the whole authentication process.

EXISTING SYSTEM:

In order to be more secure than the existing Android pattern password with entropy 18:57 bits against brute force attacks, users have to set two pass-images and use the graphical method to obtain the one-time login indicators. Like most of other graphical password authentication systems, PassMatrix is vulnerable to random guess attacks based on hot-spot analyzing. TEXTUAL passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds [3]. Textual passwords are often insecure due to the difficulty of maintaining strong ones.

Drawback:

Textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication.

III PROPOSED SYSTEM

This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. a lot of research on password authentication has been done in the literature. Among all of these proposed schemes, this paper focuses mainly on the graphical-based authentication systems. To keep this paper concise, we will give a brief review of the most related schemes that were mentioned in the previous section. The accuracy perspective focuses on the successful login rates in both sessions, including the practice logins. The usability perspective is measured by the amount of time users spent in each PassMatrix phase.

Advantage:

Two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder surfing. The habitual movements and the preference of users that the attacker may take advantage of to figure out the potential passwords.

1) Any communication between the client device and the server is protected by SSL so that packets or information will not be eavesdropped or intercepted by attackers during transmission.

2) The server and the client devices in our authentication system are trustworthy.

3) The keyboard and the entire screen of mobile devices are difficult to protect, but a small area (around 1:5 cm2) is easy to be protected from malicious people who might shoulder surf passwords.

4) Users are able to register an account in a place that is safe from observers with bad intention or surveillance cameras that are not under proper management.

IV METHODOLOGY

Multi Layer Image Authentication

To overcome (1) the security weakness of the traditional PIN method, (2) the easiness of obtaining passwords by observers in public, and (3) the compatibility issues to devices, we introduced a graphical authentication system called Pass Matrix. In Pass Matrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. Figure 5 demonstrates the proposed scheme, in which the first pass-square is located at (4, 8) in the first image, the second pass-square is on the top of the smoke in the second image at (7, 2), and the last pass-square is at (7, 10) in the third image. In Pass Matrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the Pass Points [7] scheme. Based on the user study of Cued Click Points . CCP method does a good job in helping users recollect and remember their passwords. If the user clicks on an incorrect region within the image the login will be failed.

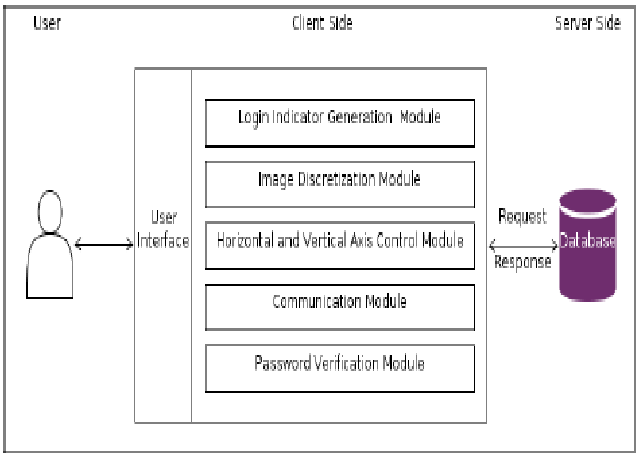

User
Client Side
Server Side
User Interface
Login Indicator Generation Module
Image Discretization Module
Horizontal and Vertical Axis Control Module
Communication Module
Password Verification Module
Request
Response
Database

Fig: Proposed System overview

Grid Image Authentication

In this type of authentication multiple images can be provided to the user, the user has the select the image that he can to log in, this will the provide more security.

Color Image Authentication

In this type the authentication is user by the color coordinates of that position. In normal Authentication the password is setting according to the regions. But in this type of authentication we choose the color coordinates for password setting.

Random Guess Attack

To perform a random guess attack, the attacker randomly tries each square as a possible pass-square for each pass image until a successful login occurs. The key security determinants of the system are the number of pass-images and the degree of discretization of each image. To quantify the security of Pass Matrix against random guess attacks, we define the entropy of a password space as in equation 3. Table 7 defines the notations used in the equation. If the entropy of a password space is k bits, there will be 2kpossible passwords in that space.

Login / Register

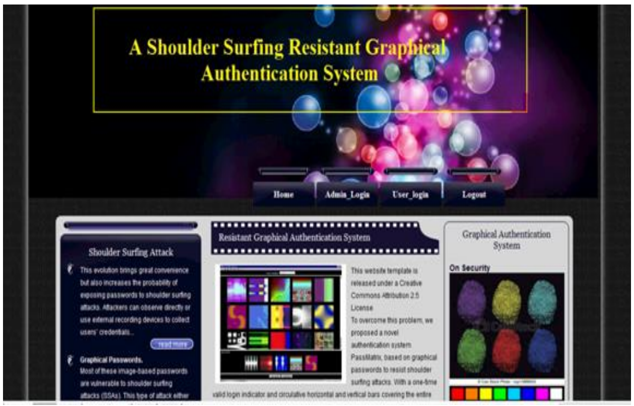
MeX will provide a secure user-id/password based secured login mechanism to access its services.

Upload Image

This is the main module in this application . The Main Process in the Mex application will be worked here. The bill picture is already stored in the mobile gallery . the user will select the picture from the gallery and upload in to the server. And also upload the details like employee name , employee id and Bill details. All the details uploaded here is stored in to the wamp server.

View Status

After uploading the details the user can check the status of the request using the same application. The status will be shown as pending until the higher authority accept or cancel the Request.


A Shoulder Surfing Resistant Graphical Authentication System
Home
Admin_Login
User_login
Logout
Shoulder Surfing Attack
read more
Resistant Graphical Authentication System
Graphical Authentication System
On Security

This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials...

Graphical Passwords.
Most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either

This website template is released under a Creative Commons Attribution 2.5 License
To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire

Fig: Home screen

View Request

The User Requested data can be view by the Higher authority. Admin is the authority to accept or reject the request. This module is done by using PHP. The Admin will use System to view the request.

Approve / Cancel

After viewing the Request the admin can have the permission to accept or reject the request. The user can check the status.

V CONCLUSION

With the expanding pattern of web administrations and applications, clients can get to these applications whenever and anyplace with different gadgets. So as to secure clients' advanced property, verification is required each time they endeavor to get to their own record and information. In any case, directing the validation process in open may result in potential shoulder surfing assaults. Indeed, even a muddled secret key can be broken effectively through shoulder surfing. Utilizing customary literary passwords or PIN technique, clients need to type their passwords to validate themselves and in this manner these passwords can be uncovered effectively on the off chance that somebody looks over shoulder or uses video recording gadgets, for example, mobile phones. To conquer this issue, we proposed a shoulder surfing safe validation framework dependent on graphical passwords, named Pass Matrix. Utilizing a one-time login pointer per picture, clients can bring up the area of their pass-square without specifically clicking or contacting it, which is an activity defenseless against shoulder surfing assaults. As a result of the structure of the level and vertical bars that spread the whole pass-picture, it offers no piece of information for assailants to limit the secret key space regardless of whether they have more than one login records of that account. Moreover, we executed a Pass Matrix model on Android and completed client analyses to assess the memorability and ease of use. The test result demonstrated that clients can sign into the framework with a normal of 1:64 attempts (Median=1), and the Total Accuracy of all login preliminaries is 93:33% even two weeks after enlistment. The complete time devoured to sign into Pass Matrix with a normal of 3:2 pass-pictures is somewhere in the range of 31:31 and 37:11 seconds and is viewed as adequate by 83:33% of members in our client ponder. In view of the trial results and overview information, Pass Matrix is a novel and simple to-utilize graphical secret phrase validation framework, which can successfully reduce bear surfing assaults. Furthermore, Pass Matrix can be connected To any validation situation and gadget with basic information and yield abilities. The review information in the client think about likewise demonstrated that Pass Matrix is down to earth in reality. Mex Application is one of the helpful application in the present circumstance. This is the easy method to speak with the administrator. Representative cost guarantee work process turned into an early contender for enablement as it could take out treatment of supporting cost bills and rather utilize the camera of Smartphone to catch the bill.

VI REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005.

[4] R. Dhamija and A. Perrig, “Deja vu: A user study using images for authentication,” in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[5] “Realuser,” http://www.realuser.com/.

[6] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, “The design and analysis of graphical passwords,” in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a graphical password system,” International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[8] A. Paivio, T. Rogers, and P. Smythe, “Why are pictures easier to recall than words?” Psychonomic Science, 1968.

[9] D. Nelson, U. Reed, and J. Walling, “Picture superiority effect,” Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.

[10] S. Brostoff and M. Sasse, “Are passfaces more usable than passwords? a field trial investigation,” PEOPLE AND COMPUTERS, pp. 405–424, 2000.

[11] A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron, and M. Fischer, “Vip: a visual approach to user authentication,” in Proceedings of the Working Conference on Advanced Visual Interfaces. ACM, 2002, pp. 316–323.

[12] B. Ives, K. Walsh, and H. Schneider, “The domino effect of password reuse,” Communications of the ACM, vol. 47, no. 4, pp. 75–78, 2004.

[13] J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Elsevier Science, 2011.

[14] T. Kwon, S. Shin, and S. Na, “Covert attentional shoulder surfing: Human adversaries are more powerful than expected,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6, pp. 716–727, June 2014.

[15] “Google glass snoopers can steal your passcode with a glance,” http://www.wired.com/2014/06/google-glass-snoopers-cansteal- your-passcode-with-a-glance/.

[16] M. Sasse, S. Brostoff, and D. Weirich, “Transforming the weakest linka human/computer interaction approach to usable and effective security,” BT technology journal, vol. 19, no. 3, pp. 122–131, 2001.

[17] “Mobile marketing statistics compilation,” http://www.smartinsights.com/mobile-marketing/mobilemarketing- analytics/mobile-marketing-statistics/.

[18] D. Hong, S. Man, B. Hawes, and M. Mathews, “A password scheme strongly resistant to spyware,” in Proceedings of International conference on security and management, 2004.

[19] D. Tan, P. Keyani, and M. Czerwinski, “Spy-resistant keyboard: Towards more secure password entry on publicly observable touch screens,” in Proceedings of OZCHI-Computer-Human Interaction Special Interest Group (CHISIG) of Australia. Canberra, Australia: ACM Press. Citeseer, 2005.

[20] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, “Reducing shoulder-surfing by using gaze-based password entry,” in Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 13–19.

[21] H. Zhao and X. Li, “S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme,” in Advanced Information Networking and Applications Workshops, 2007, AINAW’07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 467–472.

[22] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, “Pas: predicate-based authentication services against powerful passive adversaries,” in 2008 Annual Computer Security Applications Conference. IEEE, 2008, pp. 433–442.

[23] Z. Zheng, X. Liu, L. Yin, and Z. Liu, “A stroke-based textual password authentication scheme,” in Education Technology and Computer Science, 2009. ETCS’09. First International Workshop on, vol. 3. IEEE, 2009, pp. 90–95.

[24] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, “Against spyware using captcha in graphical password scheme,” in 2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE, 2010, pp. 760–767.

[25] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, “Multi-touch authentication on tabletops,” in Proceedings of the 28th international conference on Human factors in computing systems. ACM, 2010, pp. 1093–1102.

[26] “Black hat: Google glass can steal your passcodes,” https://www.technologyreview.com/s/529896/black-hatgoogle- glass-can-steal-your-passcodes/.

[27] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, “Now you see me, now you don’t: Protecting smartphone authentication from shoulder surfers,” in Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, ser. CHI ’14. New York, NY, USA: ACM, 2014, pp. 2937–2946.

[28] E. von Zezschwitz, A. De Luca, and H. Hussmann, “Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance,” in

Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI ’14. New York, NY, USA: ACM, 2014, pp. 461–470.

[29] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, “The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices,” in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI ’11. New York, NY, USA: ACM, 2011, pp. 197–200.

[30] A. Bianchi, I. Oakley, and D. S. Kwon, “The secure haptic keypad: A tactile password system,” in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI ’10. New York, NY, USA: ACM, 2010, pp. 1089–1092.

[31] I. Oakley and A. Bianchi, “Multi-touch passwords for mobile device access,” in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp ’12. New York, NY, USA: ACM, 2012, pp. 611–612.

[32] M. Martinez-Diaz, J. Fierrez, and J. Galbally, “The doodb graphical password database: Data analysis and benchmark results,” Access, IEEE, vol. 1, pp. 596–605, 2013.

[33] M. Martinez-Diaz, J. Fierrez, and J. Galbally, “Graphical passwordbased user authentication with free-form doodles,” IEEE Transactions on Human-Machine Systems, vol. PP, no. 99, pp. 1–8, 2015.

[34] V. Roth, K. Richter, and R. Freidinger, “A pin-entry method resilient against shoulder surfing,” in Proceedings of the 11th ACM conference on Computer and communications security, ser. CCS ’04. New York, NY, USA: ACM, 2004, pp. 236–245.

[35] T. Takada, “fakepointer: An authentication scheme for improving security against peeping attacks using video cameras,” in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM’ 08. The Second International Conference on. IEEE, 2008, pp. 395–400.

Authors Profile

Ms. **Sivaraju Sai Krishna Deepthi** pursuing B Tech in computer science engineering from Qis college of Engineering and Technology (Autonomous & NAAC ‘A’ Grade), Pondure Road, vengamukkalapalem, Ongole, Prakasam Dist, Affliation to Jawaharlal Nehru Technological university, kakinada in 2015-19 respectively.

Ms. **Sangu Maheswari** pursuing B Tech in computer science engineering from Qis college of Engineering and Technology (Autonomous & NAAC ‘A’ Grade), Pondure Road, vengamukkalapalem, Ongole, Prakasam Dist, Affliation to Jawaharlal Nehru Technological university, kakinada in 2015-19 respectively.

Ms. **Panyam Guru Tejaswini** pursuing B Tech in computer science engineering from Qis college of Engineering and Technology (Autonomous & NAAC ‘A’ Grade), Pondure Road, vengamukkalapalem, Ongole, Prakasam Dist, Affliation to Jawaharlal Nehru Technological university, kakinada in 2015-19 respectively.

Mr. **Chinthamaneni Saiabhilash** pursuing B Tech in computer science engineering from Qis college of Engineering and Technology (Autonomous & NAAC ‘A’ Grade), Pondure Road, vengamukkalapalem, Ongole, Prakasam Dist, Affliation to Jawaharlal Nehru Technological university, kakinada in 2015-19 respectively.

MRS. **K.V. Nagalakshmi** has received her M.Tech degree from Jntu, Hyderabad in 2012. She has guided 4PG and 16 UG students. She is working as an Assistant Professor in CSE Department, QIS college of engineering and Technology, Ongole, Prakasam District.A.P. She has a total of 7 years experience in teaching.