Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 12, December -2017

A Secure One-Time Password Authentication Scheme Using Image Texture Features

N. Vinaya Kumari, P. Ramya Krishna

[1] N. Vinaya Kumari, Assistant Prof, Dept. of CSE,
Malla Reddy Institute of Technology and Science , Maisammaguda, Secunderabad.

[2]P. Ramya Krishna, Assistant Prof, Dept. of CSE,
Malla Reddy Institute of Technology and Science , Maisammaguda, Secunderabad.

Abstract *Phishing, a serious security danger to Internet clients is an email misrepresentation in which the culprit conveys an email which resembles honest to goodness, in a request to assemble individual and money related data of the beneficiary. It is critical to avoid such phishing assaults. One of the approaches to keep the password robbery is to abstain from utilizing passwords and to validate a client without a content watchword. In this paper, we are proposing a verification benefit that is picture based and which kills the requirement for content passwords. Utilizing the texting administration accessible in web, client will get the One Time Password (OTP) after picture confirmation. This OTP at that point can be utilized by client to get to their own records. The picture construct verification strategy depends in light of the client's capacity to perceive pre-picked classes from a lattice of pictures This paper incorporates Image based authentication and HMAC based on onetime password to accomplish abnormal state of security in confirming the client over the web. These Algorithms are exceptionally sparing to actualize given they are time synchronized with the client.*

Keywords *IBA (Image Based Authentication), OTP (One Time Password), SHA-1(Secure Hash Algorithm)*

1. Introduction

Access controls exist to counteract unapproved get to. Organizations ought to guarantee that unapproved get to be permitted and furthermore approved clients can't make pointless adjustments. The controls exist in an assortment of structures, from Identification Badges and passwords to get to authentication conventions and safety efforts. There are primarily two sorts of watchword

- Static password
- Dynamic Password

Static passwordis the conventional watchword which is typically changed just when it is fundamental: it is changed when the client needs to reset the secret word, i.e., either the client has overlooked the watchword or the secret word has terminated. Static passwords are exceedingly powerless to breaking, since passwords utilized will get stored on the hard drives. To illuminate this we created One Time Password Token. Not at all like a static secret word, is dynamic watchword a passwordwhich changes each time the client signs in. An OTP is an arrangement of characters that can go about as a frame personality for one time as it were. Once the passwordis utilized, it is never again utilized for any further confirmation. Regardless of whether the aggressor gets the secret key, it is in all likelihood that it was effectively utilized once, as it was being transmitted, along these lines futile to the assailant. This lessens the powerlessness of the programmer sniffing system movement, recovering a secret key, and to effectively validate as an approved client. This passwordis utilized just for that session and when the client logins next time, another watchword is produced progressively. Picture based authentication is incorporated to give extra security coordinated OTP. With IBA, when the client performs first time enlistment on a site, he settles on a decision of a few mystery classes of pictures that are anything but difficult to recollect, for example, pictures of regular view, cars. Each time the client sign in, a network of arbitrarily produced pictures is exhibited to the client. The client distinguishes pictures that were beforehand chosen. One-time get to code is produced by the chosen pictures, influencing the verification to process more secure than utilizing just a static content secret word. It's fundamentally less demanding and profitable for the client since he needs to recollect just a couple of classifications to perceive the chose pictures. The proposed work comprises of the accompanying advances: - The client will be made a request to enter his client name, beforehand chose pictures (for confirmation) and his email. An OTP will be produced following the accommodation and will be sent to the email id. The client needs to enter the specific OTP imparted through mail. In the event that OTP get checked then he will be coordinated to the landing page.

1.1. Different Techniques Involved in Authentication Current authentication methods can be classified as follows:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based methods, for example, scratch cards, bank cards and savvy cards are generally utilized. Numerous token based authentication frameworks additionally utilize learning based methods to improve security. For instance, ATM cards are for the most part utilized with a PIN number. Biometric based verification methods, for example, fingerprints, iris output and facial acknowledgment are not yet generally received. The real disadvantage of this approach is that such frameworks can be costly, and the distinguishing proof process can be moderate and regularly untrustworthy. Nonetheless, this sort of system gives the most elevated amount of security. Learning based systems are the most broadly utilized authentication methods and incorporate both content based and picture-based passwords. The photo based methods can be further sub partitioned into two classifications: acknowledgment based and review based graphical strategies. Utilizing acknowledgment based methods, a client is given an arrangement of pictures and the client is confirmed by perceiving and distinguishing the pictures he or she chose amid the enlistment organize. Utilizing review based procedures, a client is made a request to imitate something that he or she made or chose before amid the enlistment organize.

1.2. Different Techniques Involved in Generation of One Time Password One time secret word can be created in any of the two ways:

- Time-synchronized OTP: In time-synchronized OTPs the client ought to enter the watchword inside a specific timeframe else it gets lapsed and another OTP must be created.
- A counter-synchronized OTP: With counter-synchronized OTPs, a counter is synchronized between the customer gadget and the server. The gadget counter is progressed each time an OTP is asked. For instance, consider hash-based OTPs wherein we utilize hash Algorithms, for example, SHA-1 and MD5 that can be utilized to figure the OTP. A cryptographic hash work additionally called one-way work maps message of subjective length to a settled length process. Along these lines, a hash-based OTP begins with the information parameters (synchronization esteem, username, secret key), runs them through the cryptographic hash capacity, and produces the settled length watchword, i.e., OTP.

1.3. Modes of OTP Delivery

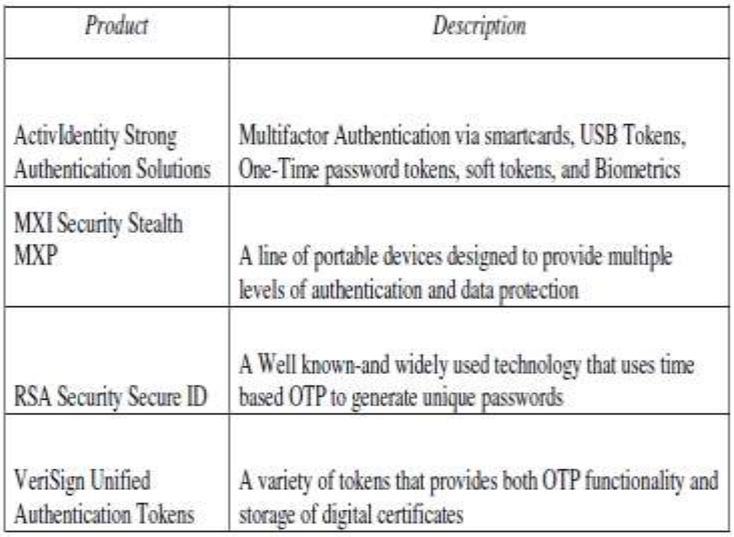
- Text informing: It is the regular technique utilized for the conveyance of OTP.
- Instant Message Services and Email: These administrations are practically normal and the cost of utilizing them is insignificant.

2. Related Work

2.1. Recognition Based Techniques Dhamija and Perrig proposed a graphical verification plot in view of the Hash Visualization technique.In this procedure, the client is solicited to choose a specific number from pictures from an arrangement of arbitrary pictures produced by a program. At that point the client will be validated by methods for distinguishing the preselected pictures. This strategy neglects to awe since the server needs to store the seeds of the portfolio pictures of every client in plain content. Akula and Devisetty's Algorithm is like the procedure proposed by Dhamija and Perrig. The distinction is that by utilizing hash Algorithm SHA-1, which creates a 20 byte yield, the verification is more secure and requires less memory. The creators proposed a conceivable future change by giving tireless stockpiling and this could be sent on the Internet, PDAs and PDAs. In the photo acknowledgment ponder; a client is prepared to perceive a vast arrangement of pictures (100 – 200 pictures) chose from a database of 20,000 pictures. This investigation uncovered that photos are the best among the three plans talked about. Pseudo codes can likewise be utilized as an option yet requires legitimate setting and preparing. Jansen et al. proposed a graphical secret word instrument for cell phones. Amid the enrolment organize, a client chooses a topic (e.g. ocean, feline, and so on.) which comprises of thumbnail photographs and after that registers a succession of pictures as a watchword. Amid the confirmation, the client must enter the enrolled pictures in the right arrangement. One disadvantage of this system is that since the quantity of thumbnail pictures is constrained to 30, the passwordspace is less. Every thumbnail picture is allocated a numerical esteem, and the succession of choice will create a numerical secret key. The outcome portrayed that the picture arrangement length is for the most part shorter than the literary watchword length. To address this issue, two pictures can be consolidated to form another letter set component, in this way extending the picture letters in order measure. Takada and Koike talked about a comparable graphical watchword system for cell phones. This system enables clients to utilize their most loved picture for confirmation. The client's initially enlisttheir most loved pictures (pass-pictures) with the server. Amid authentication, a client needs to go through a few rounds of check. At each round, the client either chooses a pass-picture among a few distraction pictures or picks nothing if no pass-picture is available. The program approves a client just if all confirmations are effective. Enabling clients to enrol their own particular pictures makes it less demanding for client to recall their watchword pictures.

2.2. Products Using One-Time Password Technology

Table 1. Name of Products



Product	Description
ActivIdentity Strong Authentication Solutions	Multifactor Authentication via smartcards, USB Tokens, One-Time password tokens, soft tokens, and Biometrics
MXI Security Stealth MXP	A line of portable devices designed to provide multiple levels of authentication and data protection
RSA Security Secure ID	A Well known-and widely used technology that uses time based OTP to generate unique passwords
VeriSign Unified Authentication Tokens	A variety of tokens that provides both OTP functionality and storage of digital certificates

3. Proposed Solution

The proposed arrangement includes two techniques: picture based verification and an OTP age strategy.

- Image Based Password Authentication
- HMAC-Based One-Time Password

3.1. Picture Based Authentication The Image-construct verification is situated in light of Recognition Techniques. At the point when the client registers for first time in a site they select arrangement of pictures that are anything but difficult to recall, for example, characteristic landscape, vehicles and so forth. Each time the client sign into the site, they are furnished with a framework of pictures that is haphazardly produced. The client can recognize the pictures that were beforehand chosen by him. It is essentially simpler for the client since they have to recollect a couple of straightforward pictures as it were. IBA depends on a client's effective distinguishing proof of his arrangement of pictures. At the point when the client logins out of the blue, the site shows a lattice of pictures, which comprises of pictures from the client's passwordset blended with different pictures. The client is verified by effectively recognizing the passwordpictures. Performing beast drive assaults or different assaults on such frameworks is exceptionally troublesome. An arrangement of various pictures is chosen to verify the client. The Image Identification Set (IIS), for every client is then put away at the Authentication System. At the point when a client logins, the IIS for that client is recovered and used to confirm that specific client. The framework does not store the pictures but rather the classification of the pictures is put away in IIS as pictures are extensive documents. This procedure is likewise more secure and requires less memory. In the event that this progression is fruitful, next OTP is created and send to the client email-id.

3.2. HMAC-Based One-Time Password Algorithm This paper depicts anAlgorithm which is utilized to create Time-synchronized OTP esteems, in view of SHA-1 based Hash Message Authentication Code (HMAC). This is called as the HMAC-Based One-Time Password in light of the fact that here OTP is created in light of HMAC. One-Time Password is clearly one of the least demanding and most prevalent types of two-factor verification that can be utilized for securing access to accounts. One-Time Passwords are regularly alluded to as safe and more grounded types of authentication, and enabling them to introduce over various machines including home PCs, cell phones and so forth. At the point when the client chooses the pre-chosen pictures to login an OTP is produced and sent to the client's email id. The client is then coordinated to next page where the client is made a request to enter the OTP. The client gets the OTP utilizing the email record and enters it. On the off chance that the OTP is confirmed the client prevails with regards to signing in the framework.

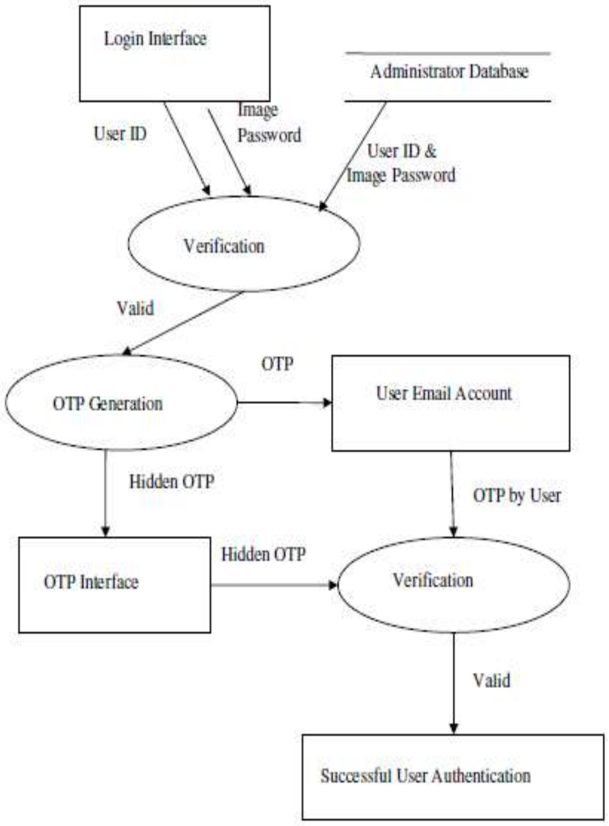


Figure 1. Data Flow Diagram

3.3 Algorithm Requirements
A - The Algorithm MUST be time synchronized.
B - The Algorithm SHOULD be prudent to execute by decreasing the measure of equipment required.
C - The Algorithm MUST work with any kind of code creating tokens.
D - The esteem showed on the token or any mail message ought to be anything but difficult to peruse and entered by the client. For this the OTP esteem ought to be of sensible length, for example, 8-digit esteem. It is attractive for the OTP incentive to be a numeric digit with the goal that it can be effectively entered. E - User-accommodating instruments ought to be accessible to resynchronize the time.

3.3.1. Algorithm The documentations utilized as a part of OTP Algorithm Symbol Represents T It is the Time esteem, the evolving Factor. Key Shared mystery amongst customer and server, i.e. Username and Image Based Password. Digit Number of digits in a HOTP esteem.

3.3.1.1Description The OTP Algorithms depend on an expanding time esteem work and a static symmetric key known just to customer and server. To make the OTP esteem, a HMAC-SHA-1 Algorithm is utilized. Since the yield of the HMAC-SHA-1 computation is 160 bits, we need to truncate this incentive to a littler digit with the goal that it can be effectively entered.
OTP (Key,T) = Truncate(ToHex(HMAC-SHA-1(Key,T)))
Where – Truncate proselytes the esteem produced through HMAC-SHA-1to OTP esteem.

3.4. Generation of OTP Value The Algorithm can be portrayed in 3 stages:
Stage 1: Generate the HMAC-SHA-1 esteem Let HMK = HMAC-SHA-1(Key, T)/HMK is a 20-byte string
Stage 2: Generate a hex code of the HMK. HexHMK=ToHex (HMK)
Stage 3: Extract the 8-digit OTP esteem from the string
OTP = Truncate (HexHMK)
The Truncate capacity in Step 3 does the dynamic truncation and lessens the OTP to 8-digit.

3.5 Operation

```
MessageDigest md = MessageDigest("SHA1")
md.update(Key,T)
output = md.digest()
buf = hexDigit((output >> 4) & 0x0f)
```

```
otp=buf.toString()
otp=otp.substring(0,7)
```

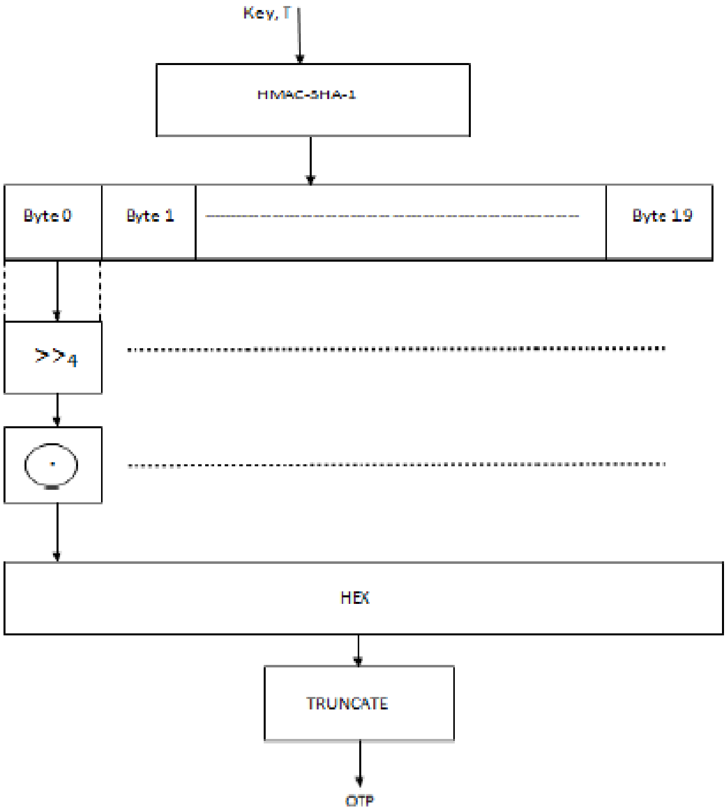
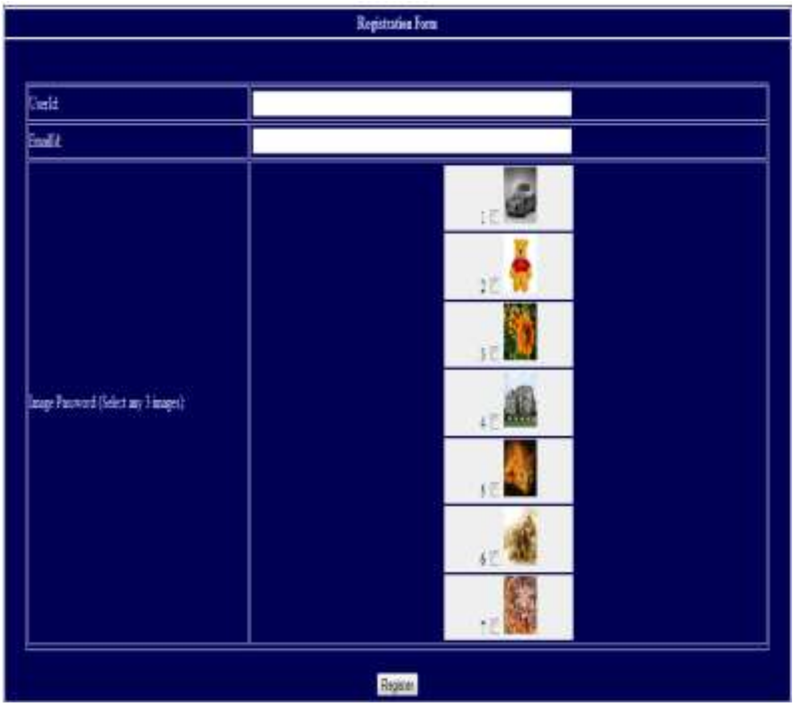


Figure 2. Operation of HMAC-SHA-1

3.6 Applications Google is as of now utilizing one time secret key. Hotmail is additionally utilizing one time password to give high security to clients. RBI made OTP mandatory for exchange made with charge card. All saving money frameworks are utilizing OTP. E.g.:- ICICI Bank, HDFC, Citi Bank, Axis, SBI and so forth.

4. Screenshots



Registration Form

UserId	
EmailId	
Image Password (Select any 3 images)	

Figure 3: Registration Form

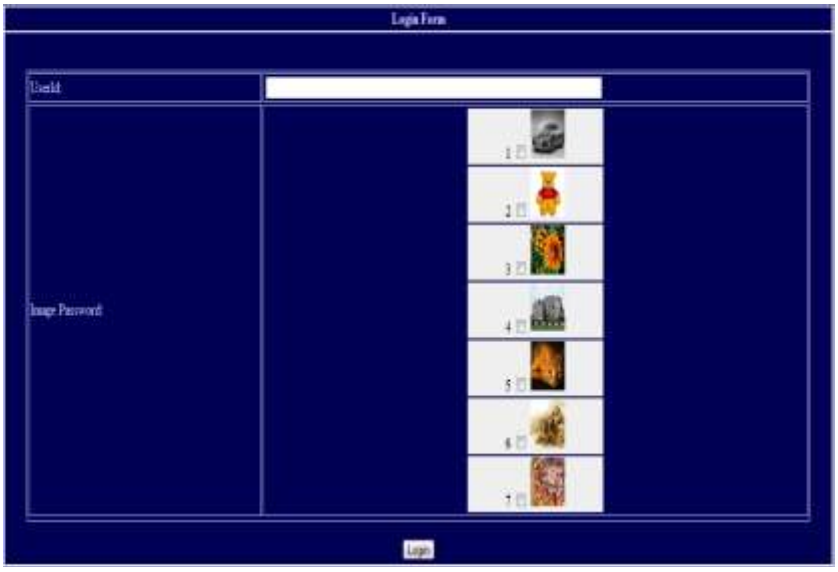


Figure 4. Login Form

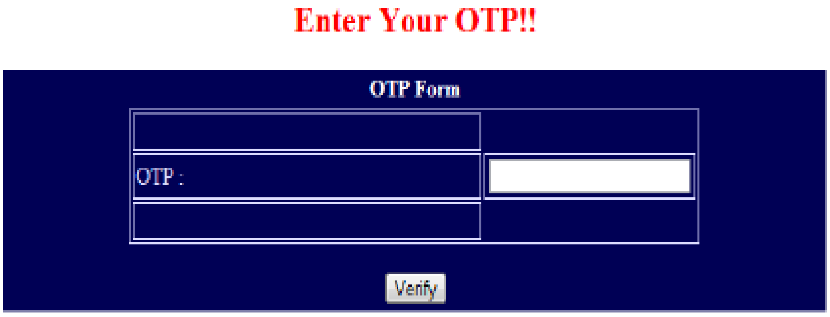


Figure 5. OTP Form

Figure 6. Home Page

5. Conclusion

The proposed framework coordinates the security methods Image Based Password Authentication and Hash-MAC based onetime secret key. At first, the Image Based Password Authentication is done where client is confirmed utilizing picture secret word that was already chosen by the client himself, trailed by the Hash - MAC based One Time Password which utilizes SHA-1 Algorithm for the age of a safe one time watchword. This authentication method is straightforward and very secure. The cryptographic quality of the HMAC relies on the cryptographic quality of the hidden hash work and in this paper SHA-1 is utilized for the count of HMAC. SHA-1 being a most broadly acknowledged cryptographic hash work because of its high security when contrasted with other cryptographic hash capacities, for example, MD5 adds to the security of HMAC. Recuperation of lost watchword in view of mystery question and answers can be a future upgrade.

References

[01] Active Identity Strong Authentication Solutions, http://www.actividentity.com/

[02] Mastering Java Security (Cryptography, Algorithms & Architecture) by Rich Helton & JohennieHelton (Wiley/ Dream Tech)

[03] MXI Security Stealth MXP, http://www.Processor.com/MXI

[04] RSA Security SecurID**,** http://www.rsasecurity.com

[05] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedingsof 9th USENIX Security Symposium*, 2000.

[06] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in*Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*,1999.

[07] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings ofMidwest Instruction and Computing Symposium*, 2004.

[08] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in *Proceedingsof Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 2004, pp.1399-1402.

[09] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in *Data Security*, 2004.

[10] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual LoginTechnique for Mobile Devices," National Institute of Standards and Technology Interagency ReportNISTIR 7030, 2003.

[11] D. M'Raihi, M. Bellare, F. Hoornaert, and D. Naccache, "HOTP: An HMAC based one-timepassword algorithm, RFC 4226", Dec. 2005.

[12] Nitin ,Durg Singh Chuhan, Vivek Kumar Sehgal, Ankit Mahanot," Security Analysis andImplementation of *JUIT–Image Based Authentication System using Kerberos Protocol", SeventhIEEE/ACIS International Conference on Computer and Information Science, pp. 575-580

[13] Balkis Hamdane, Ahmed Serhrouchni, Adrien Montfaucon, Sihem Guemara." Using the HMACBasedOne-Time Password Algorithm for TLS Authentication" 978-1-4577-0737-7/11/ ©2011 IEEE

[14] Srinath Akula, Veerabhadram Devisetty ,"Image Based Registration and Authentication System",Department of Computer Science,aksr0201@stcloudstate.edu, deve0301@stcloudstate.edu

[15] Chun-Ying Huang, Shang-PinMaa, Kuan-TaChen," Using one-time passwords to prevent passwordphishing attacks" Journal of Network and Computer Applications 34 (2011) 1292–1301, pp.1292-1300.

ABOUT AUTHORS:

N. Vinaya Kumari is currently working as an Assistant Professor in Computer Science & Engineering Department, Malla Reddy Institute of Technology and Science, Maisammaguda, Secunderabad.

P.Ramya Krishna is currently working as an Assistant Professor in Computer Science & Engineering Department, Malla Reddy Institute of Technology and Science, Maisammaguda, Secunderabad.