iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41611

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Authorization and Authentication in Mobile Devices

Vinay Kumar B
Final Year PG Student, School of Computer Science & Information Technology, Jain Deemed-to-be University, Bengaluru[1]

Abstract: ***With the rapid evolution of the wireless communication technology, user authorization and authentication is important in order to ensure the security of the wireless communication technology. Password play an important role in the process of authentication. In the process of authentication, the password enter by the user will be transmitted along the traffic to the authentication server in order to allow the server to grant access to the authorized user. The attackers will use the chance to attempt sniff others person password in order to perform some illegal activities by using others person password in order to perform some illegal activities by using others identitity to keep them safe from trouble. Due to the issues, there are many solutions has been proposed to improve the security of wireless communication technology. In this paper. The previously proposed solution will be used to enhance the security of the system. . For mobile apps , we need to make a clear distinction between user authentication and app authentication. User authentication is about how users prove that they are the legitimate apps users. App authentication covers how the app authenticates towards the backend . Sometimes device authentication also mentioned , is accessible to all apps running on your phone and generally easy to spoofs.***
Keywords: Authorization , Authentication , Cryptography , Hash Function , Face Authentication.

I. INTRODUCTION

Authorization is the process of gaining permissions on specific actions to given entities-in our scenario specifically to users devices or applications. There are a total of 20 rticles in the identified pool addressing this topic. Access control based on trust in ARM-Complaint model is proposed. It describes various levels of trust , a multidimensional attribute which describes various concerns in the network the authors call dimensions quality of service including network availability and thoughput , security authentication and authorization protocols. Groups of mobile devices to which an individual device belongs e.g., made by a certain manufacturer or currently in particular location. This trust is used for final authorization within the environment. Develops an authorization architecture based on IoT-OAS authenticating users using tokens similar to those used opened. Every device has a designated owner and set of action permissions with one another multiple operational cases are described. Gerdes et al. tackle the problem of authorization and authentication for devices with constrained computational power. The authors divide IOT devices into the categories "constrained" and "less-constrained" devices to perform some authorization function on behalf of the constrained devices. Entitles request authorization tokens to access services provided by or data stored on another server devices. Every node in the network has a full database of all access control policies for each resource-requester pair in the form of transactions. Traditional authentication methods enhanced with multifactor authentication based on a location, are described in. their systems considers user location, and they develop an additional factor for multifactor authentication which ascertains the physical of a user being in a particular location. Authentication server address and digital signature , scanning QR code and sending it to the authentication manager allow the manager to decide which authentication method it should enforce on the user. The digital world is much complex and so the security of it. It became difficult for an institution to match the users choice and quality security at once. User friendly security were rarely available , like remembering of passwords. Face recognition is a technique which uses the computerized image or video to match the face of the human to perform identification and authentication. This is performed by various techniques like Eigen faces, fisher faces and pattern histogram. Online applications to provide online clients and merchants with a quick and convenient way to exchange goods and services. However , the deployment of these applications is still facing many problems such as security threats and online attacks. The authentication process is composed of two layers the first layer is performed on behalf of the mobile phone-side, in which the client launches a pin-protected application on the phone , called DGCH (Decrypt, Generate, Compare , and Hash) the second layer is performed on behalf of the merchant-side in which users authenticity.

II. RELATED WORK

The accompanying statistics and feedback reveal that Triple-Des grants a better-nice encryption method than des higher encryption and decryption overall performance method. Using a community to execute numerous approaches. The second has arrived might be superior withinside the destiny for the Triple-DES method undertaking could additionally encompass a better stage of warranty for all forms of multimedia, nice and overall performance are difficult statistics.

The latter could entail encrypting statistics with a cross-platform of video and audio files, diverse algorithms [3] this technique is handiest whilst implemented on the organisational stage. Because of the Triple DES method employed, even though the statistics is hacked, the hacker will now no longer be capable of get entry to the account. SFTP encrypts the record at some stage in transmission and decrypts the encrypted statistics on the receiving end. The cap potential to encrypt keys is one of the maximum crucial functions of SFTP. The record is encrypted the use of a non-public key at some stage in encrypted record switch. The SFTP generates the non-public key from the customer`s registration statistics. To decode the encrypted record, The key should be communicated via way of means of the sender to the recipient. As a result, the encrypted record is despatched at the side of the non-public key. Encryption is used right here to defend the non-public key. That is, a static software program key encrypts the non-public key. As a result, with this key, the recipient can speedily decrypt the contents. [7] all of it laboured and defined the statistics is encrypted into cypher textual content the use of the Triple DES technique. They should achieve a brand-new key from a permitted character who's locked in; in the event that they use an unauthorised key, they chance dropping all the hidden statistics. The AES set of rules and the chaotic series are used to encrypt and decrypt on this research. [11] makes use of a statistics encryption device produced with none extra analytical price to help industrial companies in deciding on the maximum reliable International Journal of Advanced Science and encryption algorithms for his or her enterprises. [12] it defined the way to enhance the Key Schedule Method, a completely unique FORTIS set of rules is proposed on this research. The identity of operations from the electricity hint have become extra hard with the creation of the Comparator and bendy shifter withinside the Key Schedule Algorithm, due to which the PGE values have been decreased and the set of rules become harmed.

III. TECHNICAL BACKGROUND

PHP is a general purpose scripting language geared toward web development. Hypertext Preprocessor. PHP code is usually processed on a web server by a PHP interpreter implemented as a module, a daemon or as a Common Gateway Interface (CGI) executable. On a web server, the result of the interpreted and executed PHP code-which may be any type of data, such as generated HTML or binary Image data-would form the whole part of an HTTP response. Various web template systems, and web frameworks exist which can be employed to orchestrate or facilitate the generation of that response. Additionally, PHP can be used for many programming tasks outside the web context, such as standalone graphical applications and robotic drone control. PHP code can also be directly executed from the command line. PHP has been widely ported and can be deployed on most web servers on variety of operating systems and platforms.The computer language used to create websites is known as Hyper Text Markup Language (HTML). The language, which contains code words and grammar like any other language, is relatively simple to learn and, as time goes on, becomes more powerful in terms of what it can be used for. Under the aegis of the World Wide Web Consortium, the body that defines and maintains HTML, the language continues to expand to satisfy the expectations and requirements of the Internet. SQL is a Structured Query Language is a domain-specific language used in programming and designed for managing data held in a relational database , or for stream processing in a relational data stream management stream management systems . SQL consists of many types of statements, which may be informally classed as sublanguages, commonly: a data query language(DQL), a data control language (DCL), and a data manipulation language (DML). SQL was one of the first commercial languages to use relational model. SQL code requires at least.

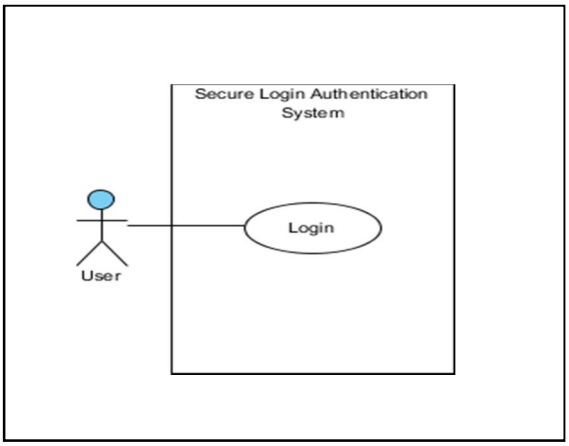


Fig 1: Usecase Diagram

A. Security Factors

1) *Knowledge Factor:* The username and password are very important in any system, proposed system also has a knowledge factor while is the very first step in verifying the identity of the user. The password is stored using md5 128-bit encryption in the database. The verification of the password is done twice. First while registering it should have all the necessary combinations of letters, numbers, special characters, and capital small letters, is known as password validation, and the second time when the user location is being verified, which will be explained further in the document.
2) *Possession Factor:* The possession factor is a very important factor of the MFA System, where it verifies the users identity twice using an OTP generator, an app, a cellphone, or the user's email. OTP stands for one-time password and it is a basic combination of numbers, alphabets, or just numbers. The OTP generator of the proposed system can generate 6 random digits but I can program it to generate more than 6. The OTP generator with the proposed system can work with my email service, for the implementation of the OTP generator library from PHP.
3) *Cloud Security:* Cloud security protects cloud or cloud-connected data and information in the same way as application and infrastructure security does. Cloud security focuses on the risks that arise from Internet-facing services and shared settings, such as public clouds, by providing additional protections and solutions. Interaction with cloud providers or third-party services is another component of cloud security. Because the infrastructure is often controlled, are often unable to fully control environments while using cloud-hosted resources and apps. As a result, cloud security procedures must account for limited control and include safeguards to prevent access and vulnerabilities caused by contractors or vendors.
4) *Authenticity:* implies checking that clients are who they say they are and that each info showing up at objective is from a confided in source. This rule assuming adhered to ensures the substantial and real message got from a confided in source through a legitimate transmission. For instance, on the off chance that take above model shipper sends the message alongside

IV. RESULTS AND DISCUSSION

Flowchart

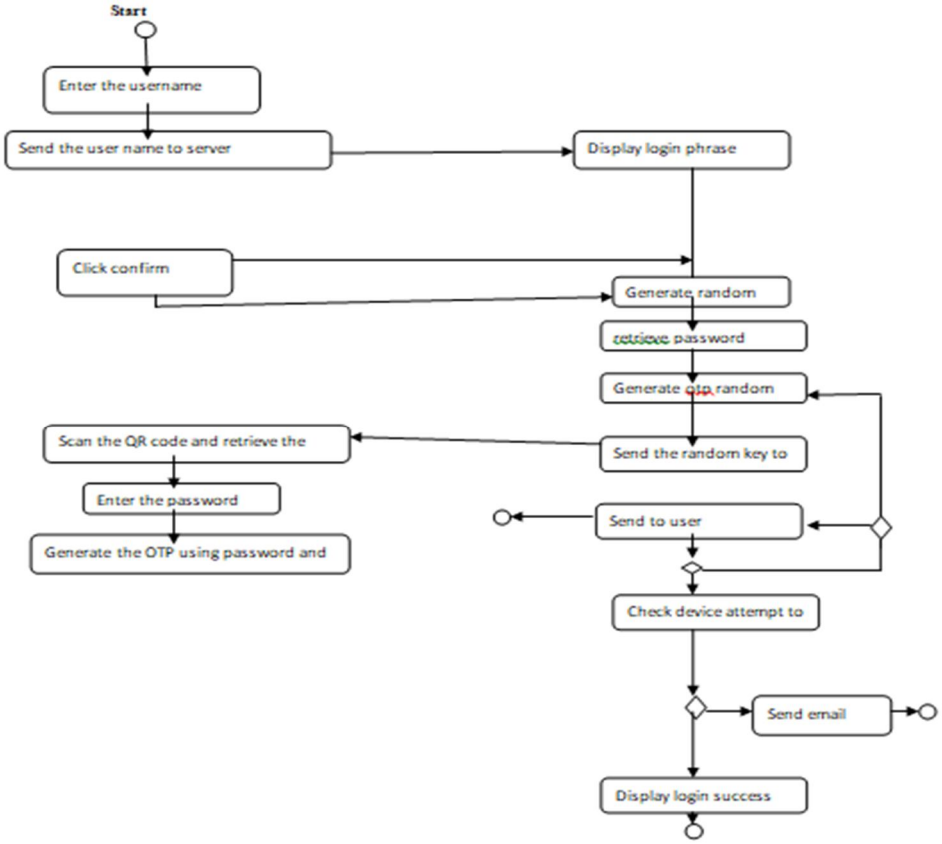


Fig 2 :Flow Chart of the System

The system validates and checks each of identity from OTP to the saved Email and verfies it with the already saved data ensure the maximum amount of security and mitigate unauthorized access and data breaches. OTP is sent to the registered email for verification. The system gives you the option of signing in using the username and password or using registered with the system. The possession factor of the system sends an OTP to the registered Email ID. The geo-location factor verifies the IP adddress of the user upon inserting username and password . The factor is the overall time from the start of the system till the user gets access to the homepage.

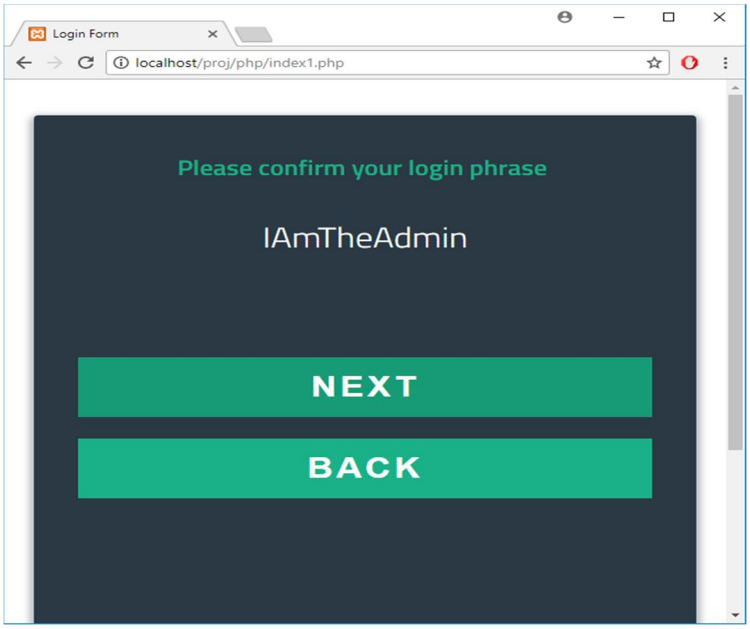


Fig 1 : Login Phrase Display

The login phrase will then retrieve from the database of the user details and display on the website. The user will need to confirm the login phrase is correct.

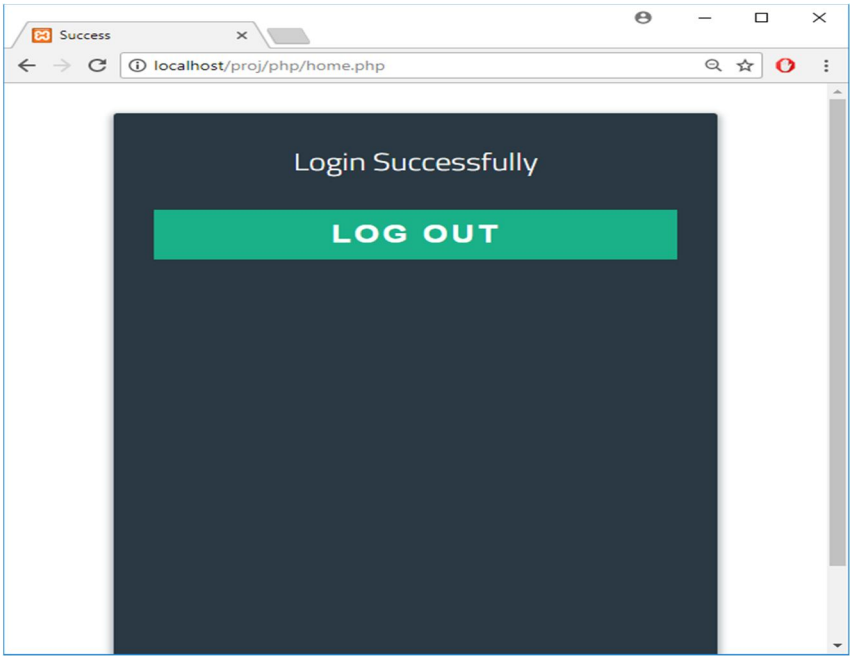


Fig 2: Final Outcome of the system (Page of the website)

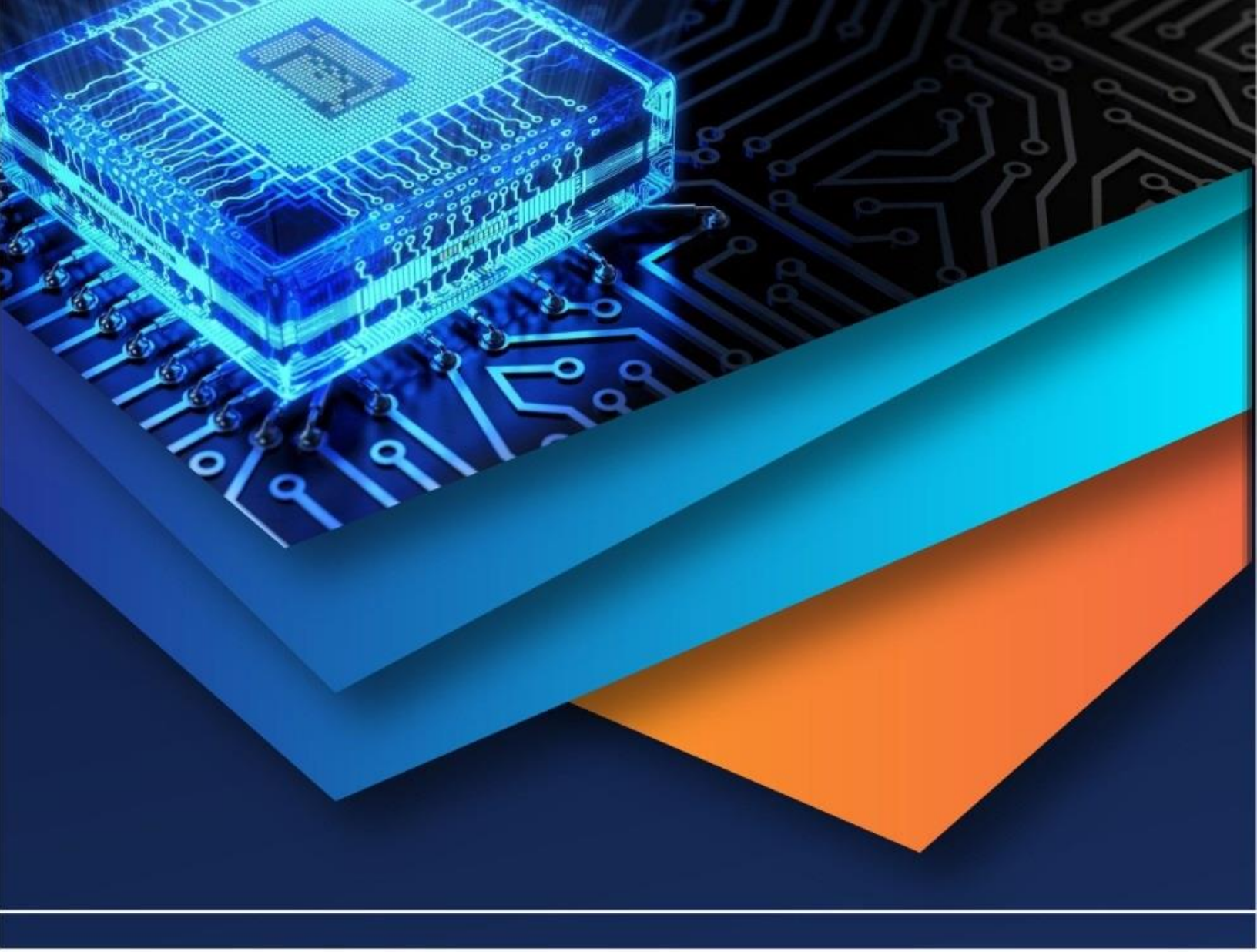
Once the OTP is matched within the trial of 5 times, the website will display login successful.

V. CONCLUSION FUTURE ENHANCEMENT

The project has achieved a huge success to mitigate with the rainbow table attack where the attackers will need to generate a huge rainbow table to exploit the system. A huge rainbow table will require a lot of time to be generated. Apart from that, the system also uses the 2 factor authentication where it requires the actual password and OTP to grant success to the system. Next, one of the huge success where will be the OTP can be generated without connection to internet which help to prevent the attackers to able to retrieve the actual password from the network flow. The main future is to implement a secure login authentication system with utilizing with two factor authentications. By using the concept two factor authentication could help need to pass through the next barrier of defence to success to login. this system will help enhance the login authentication system. Next future is to ensure login password will not be transmitted over the network. As compared to the previous solution, the password is just encrypted, but the attackers might succeed to decode the data and retrieve the password. So in order to prevent this happens, the password with the random key will need to be hash before the sender sends the password to the server. It is important to secure the password of the user.

REFERENCES

[1] Heisele, P. Ho, and T.Poggio, “Face Recognition with Support Vector Machines”: Global versus component based approach, 2001.
[2] S. Dobrisek, V. Struc, J. Krizaj, and F.Mihelic, “Face recognition in the wild with the Probabilistic Gabor-Fisher Classifier,” 2015 11th IEEE International conference and workshops on Automatic Face and Gesture Recognition , 2015.
[3] S. Dalali and L. Suresh, “Daubechives wavelet based face Recognition Using Modified LBP,” Procedia Computer Science , Vol.93, pp.344-350,2016.
[4] K.Maurya, M. Singh and N.Jain, “Real Time Vehicle Tracking System Using GSM and GPS Technolgy-An Anti-theft Tracking System,” International Journal of Electronics and Computer Scince engineering, 2012.
[5] P. Hillmann, L. Stimert, G. Dreo, and O. Rose, “On the Path to High Precise IP Geolocation : A Self-Optimizing Model,” International Journal of Inteligent Computing Research, vol.7,no,1,2016
[6] A.K. Singh, V.Bansal, “SVM Based Approach for Multiface Detection And Recognition in Static Images” Journal of Image Processing and Artifical Inteligence, vol.5, Issue 2, pp.1-11,2018
[7] O. O. Alharaki, F. S. Alaieri, A.M. Zeki, “ The integraton of GPS Navigator Device with Vehicles Tracking System for Rental Car Firms”, International journal of computer science and Information Security , vol.8, No. 6, September 2010.
[8] S. Hallsteinsen, I. Jorstad, and T. Do Van, “Using the mobile phone as a security token for unified authentication,” in Systems and Networks Communications, 2007. ICSNC 2007. Second International Conference on, 2007, pp. 68-68.
[9] Milton k. (n.d.), Can a Hacker Bypass Encryption? , Available from: http://itstillworks.com/can-hacker-bypass-encryption-2996.html.
[10] Vaithyasubramanian, S, Christy, A. and Sarvanan, D.(2015) ‘Two Factor Authentications for Secured Login in Suppot of Effective Information Preservation’, 10(5), pp 2053-2056. Available from: http://www.arpnjournals.com/jeas/research papers/rp 2015/jeas 0315 17113.pdf.
[11] Long A. (2011), How Hackers Take Your Encrypted Password and Crack Them, Available from: https://null-byte.wonderhowto.com/how-to/hackers-take-your-encrypted-passwords-crack-them-0130638
[12] Cheng, X. R. et al. (2005) ‘Research and realization of authentication technique based on OTP and Kerberos’, proceedings – Eighth International Conference on High-Performance Computing in Asia-Pacific Region, Hpc Asia 2005, 2005,, pp. 409-413. Doi: 10.1109/HPCASIA.2005.86.Available from : http://ieeexplore.ieee.org/document/1592297/.
[13] En.wikipeedia.org. (2017). Smartphone. [online Available at: https://enwikipedia.org/wiki/smartphone.
[14] En.wikipeedia.org. (2017). Laptop. [online Available at: https://enwikipedia.org/wiki/Laptop
[15] Mathur, A. (2012) ‘A Research paper : An ASCII value based data encryption algorithm and its comparision with others symmetric data encryption algorithms’, I’nternational Journal on Computer Science and Engineering (IJCSE), 4(9), pp. 1650-1657 Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.433.7344&rep=rep1 &type=pd f .
[16] Margeret Rouse (2014) Authentication, Available at : http://searchsecurity.techtarget.com/definition/authentication/.
[17] Cristofaro, E. et al. (2014) ‘A Comparative Usability Study of Two Factor Authentication’, cs.CR, (February). Doi:10.14722/usec.2014.23025. Available at : https://pdfs.semanticsscholar.org/028aa/70fc1836e113fd18f12b99e08fb024f6bb04.pdf.
[18] Symmetric and Asymmetric Encryption – What are the difference? N.d., Available from: https://www..ssI2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differnces.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY