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.2022.41610

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, Dept of MCA, School of Computer Science & Information Technology, Jain Deemed-to-be University, Bengaluru, India

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 articles 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 though put , 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.

The 5 pillars of information assurance is a safeguard the privacy of the people? Promising and providing 100 percent security is always very difficult to accomplish. There always remains a loophole or a vulnerability to be addressed. In the 1970's "cyber security" specifically, security in computer systems was used for the first time and people became aware of it. With the creation of creepers, a program created by researcher Bob Thomas, it could move freely across the network of AROANET and leave a trial. From that time till date, many new technology and advancements took place.

1) *Confidentiality:* very organization whether small or large needs to keep some data of theirs private and confidential. The information or data is so vital for the organization that is survival depends on it. Competitors of the company are always trying to extract that information to get an upper hand in the market. There are different ways and methods to keep that confidential data safe. Some methods are; Encryption, Intrusion Detection, Firewall, Penetration testing,and awareness training and policies. Some of the attacks which can be utilized by the hackers extract confidential data are; password attacks, Port scanning, Ping sweep, Keyloggers, Phishing, and pharming.

2) *Integrity:* Integrity means that the data in storage or transit shouls not be changed, manipulated, or deleted by an unauthorized user. If the dat or the information is changed, that so called data nno longer viable and can bring more harm than good. A few techniques that are used for maintaining integrity are access control, logging, monitoring, ad auditing are few of the techniques. The attacks that can be used to disrpt the integrity of the data are session hijacking and man in the middle attacks.
3) *Availability:* Availability of the data or system resource mean the data and the system should be available for utilization to unauthorized users when needed. Most of the time, it's thought that the confidentiality and the integrity of the data are much important. Rather than ensuring the availability of the data, confidentiality and integrity should be safeguard. It is called as CIA not CI triads are important and availability is very important. Few techniques which are used to ensure the availability of the system.
4) *Authentication:* it's the method of validating the users or system identity. Authentication confirms the identity of the user when he/she logs in to that system. The fundamental goal of authentication is to enable authorized users access to the system while denying unauthorized users access. The very basic methods of authentication are knowledge based the system while denying unauthorized users access.

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 eigenfaces, 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.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

III. ANALYSIS : SECURITY SYSTEMS IN A COMPUTER

Most of the time a lot of users don't take authorization and authentication seriously while designing their systems.in terms of the mobile devices , authentication can play a significant influence in reducing and mitigating several unauthorized access and data breaches. Although, various measures like encryption and cryptographic algorithms are used at the backend of the system to keep the confidential and private data of the users and patients safe still the malicious attackers get their hands on the data using different means.

The most common and expensive attack is ransomware which costs the authorization and authentication in mobile devices , most of the researchers have emphasized keeping the data in storage and transit safe from malicious actors, which important but finding a safe and secure way to access that data is also very important.

Because most of the time regulations, and weak security policies. To understand the security in detail we will looking into each of the aspects one by one. Authentication is the act of proving the legitimacy of the identity of the user, using different security measures or credentials like username and password, OTP, Biometric , Geolocation, however, authorization is to allow the specific user to use the system once his/her identity has been verified usually the authorization is followed by authentication. There are a variety of authentication methods available, ranging between credential access and biometric, to authenticate a user's identity before granting access to the system. These techniques of authentication provide different layers of security and prevent attacks like data breaches and unauthorized access. However, a mix of several sorts of authentications is frequently used to ensure safe system reinforcement against potential threats.

A. Types of Security

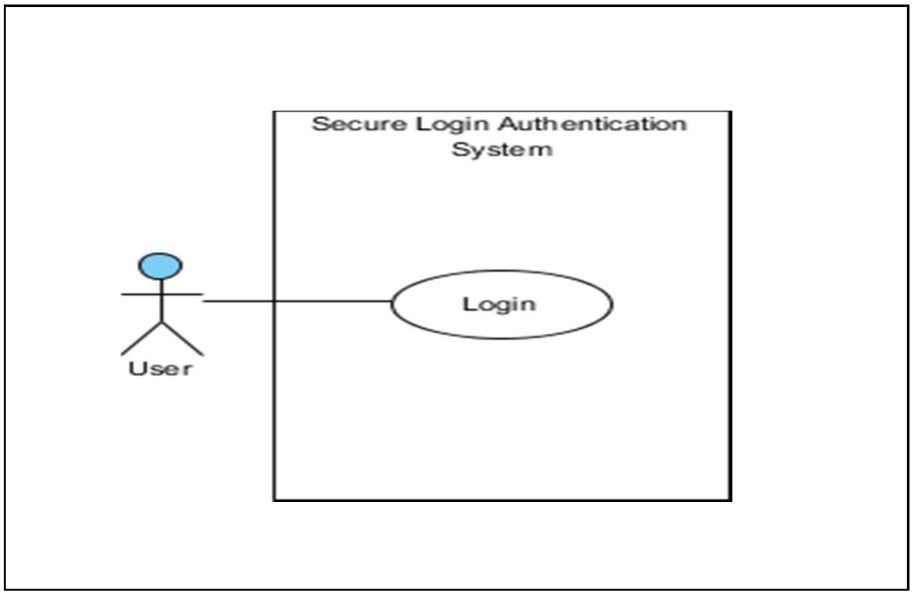
Data Security isn't just about getting data from unapproved access. Data Security is essentially the act of forestalling unapproved access, use, exposure, interruption, change, assessment, recording or obliteration of data. Data can be physical or electronic one. Data can be whatever like Your subtleties or we can say your profile via web-based media, your information in cell phone, your biometrics and so forth Along these lines Data Security ranges so many examination regions like Cryptography, Portable Processing, Digital Legal sciences, Online Web-based Media and so forth.

1) *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.
2) *Application Security:* Applications and application programming interfaces are protected by application security solutions (APIs). These techniques can be used to prevent, discover, and fix bugs and other vulnerabilities in software. Application and API vulnerabilities can provide a route to broader systems if they aren't secured, putting the data at risk.A significant portion of application security is based on specialised tools for application shielding, scanning, and testing. These tools can assist in identifying vulnerabilities in applications and their associated components. When vulnerabilities are discovered, they can be fixed before applications are released or vulnerabilities are exploited. Application security applies to both the applications used and those may develop, as both must be secure.
3) *Infrastructure Security:* Networks, servers, client devices, mobile devices, and data centres are among the infrastructure components that are protected by infrastructure security techniques. Without sufficient protections, the increased interconnectedness between these and other infrastructure components puts information at risk.This risk arises from the fact that connectivity spreads vulnerabilities throughout the systems. If one component of infrastructure fails or is compromised, it affects all dependent components. As a result, minimising dependencies and isolating components while still allowing intercommunications is an important goal of infrastructure security.
4) *Disaster Recovery:* Unexpected circumstances might cause the company to lose money or suffer damage, thus disaster recovery plans are essential. Ransomware, natural disasters, and single points of failure are some examples. The recovery of information, the restoration of systems, and the resuming of operations are all part of most disaster recovery plans. These measures are frequently included in a business continuity management (BCM) plan, which is aimed to help firms sustain operations with the least amount of downtime possible.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

5) *Incident Response:* A combination of protocols and measures for identifying, investigating, and responding to threats or destructive occurrences is known as incident response. It prevents or minimises system damage caused by attacks, natural disasters, system failures, or human mistake. Any harm to information, such as any damage or theft, is included in this damage. An incident response plan is a regularly used tool for incident response (IRP). The duties and responsibilities for responding to occurrences are outlined in IRPs. These plans also help to define security strategy, give recommendations or procedures for action, and guarantee that incident information is used to improve security.

B. Use case Diagram of Authentication and Authorization



C. Analysis: Security in Authorization and Authentication in Mobile Device

In today digitalized environment, cybersecurity and data protection are critical for mobile devices, countless devices that make the IoT in a safeguard of all the systems outlined above. In this implemented system will give the more security to the mobile devices , only authorized users use the mobile phones otherwise no one can be open the lock tock to others mobiles.

1) *Email:* Apart from the dedicated system for internal communication email also plays a primary role in communication within mobile devices , different kind of information is being sent, received, and disappeared using email systems. With time, the size of the mailbox of the email systems grew due to the different types of information regarding the users . due to al the reasons keeping an eye on the email security of the devices. Unintentionally someone mayopen a malicious email or malicious attachement that can infect their system. Though the network The malicious program infect the rest of the mobile devices.
2) *Physical Security:* Legacy systems are such systems that the manufacturers have stopped supporting. They can be software, OS, or mobile devices running on old OS. There are a lot of legacy systems in different devices, which pose a big cybersecurity challenge.

D. Use Case Description Of System

Use Case ID	**UC001**	**Version**	**10**
Feature	F001 Login		
Purpose	To allow the user to log in their account		
Actor	User		
Trigger	User surf website the website		
Precondition	Surf website		

Scenario Name	step	Action
Main Flow	1	User enter username
	2	system check validity of the user name
	3	system retrieves login phrase
	4	system display login phrase
	5	user confirm with login phrase
	6	system obtain random key
	7	system display random key
	8	user scan QR code
	9	user enter password
	10	system generated and display OTP
	11	user enter OTP in website
	12	System check device validity of the account in the database
	13	system display login successful
Alternate Flow		user enters invalid OTP
Invalid username		system display error message
		System generate random key
Alternate Flow Invalid key		user enters invalid OTP
		System displays error message this username doesn't exist
		Back to main flow step
Alternate Flow Trial more than 5		user enters invalid OTP more than 5 times
		System send email to user to inform account is locked
Alternate 1st attempt login of new device		user use new device to attempt login
		System send email to user verify device
		Username must exist in the database
		OTP must be matched

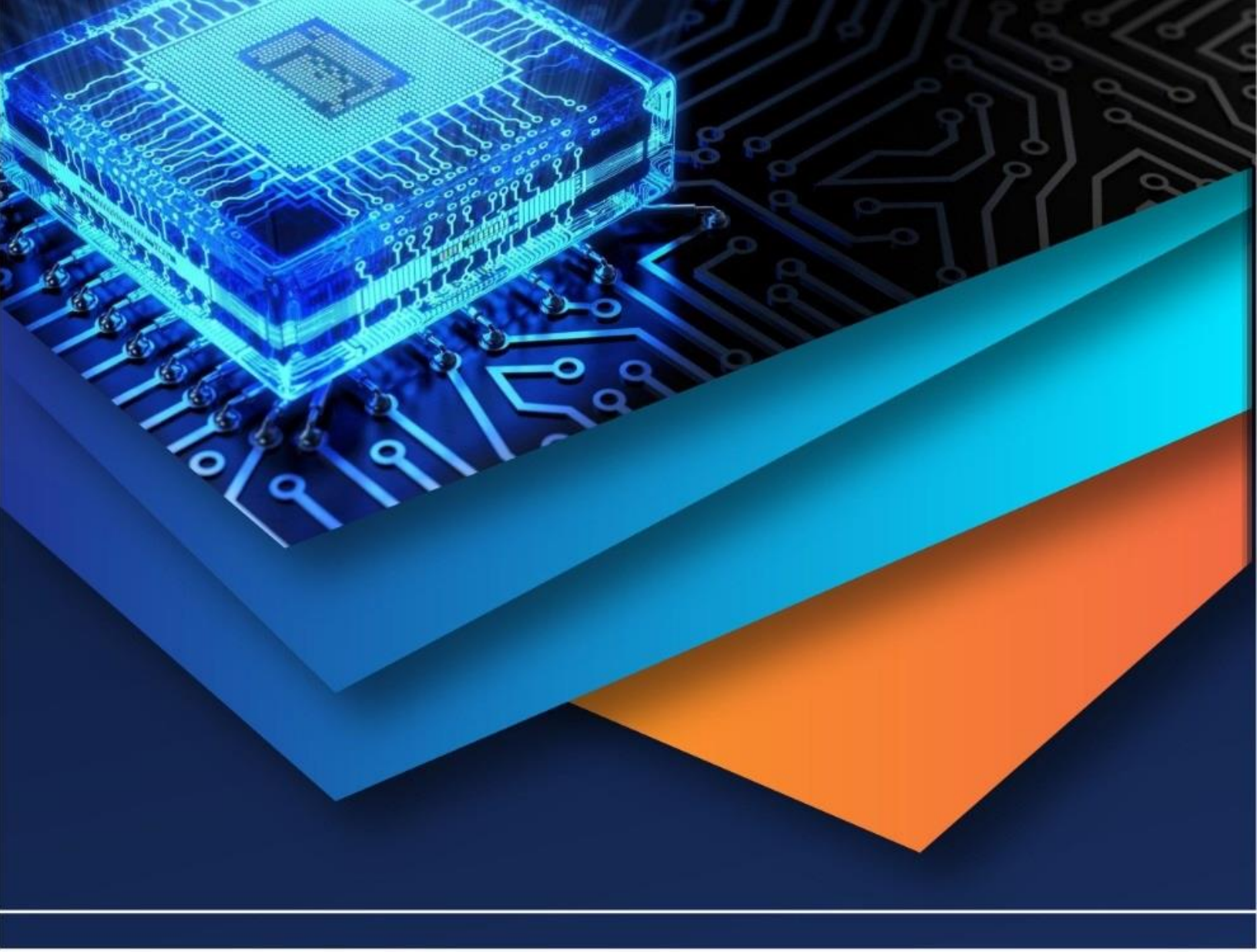
IV. CONCLUSION

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.

REFERENCES

[1] B. Hessle, 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] X. Yin, J. Zou, C. Fan and P.Zhou, "An Improved Dynamic Identity Authentication Scheme Based on PKI_SIM Card," in Wireless Communications, Networking and Mobile Computing , 2009. WiCom'09.5th International Conference on , 2009, pp.1-4.

[10] M. Xiaoming, "Study on the Model Of E-Commerce Identity Authentication Based on Multi-biometric Features Identification," in Computing, Communication, Control, and Management, 2008. CCCM'08. ISECS International Colloquium on 2008, pp. 196-200.
[11] S.Bandra, T.Yashiro, N. Koshizuka, and K. Sakamura, Access control framework for API-enabled devices in smart Buildings of the 22nd Asia-Pacific Conference on Communications, APCC 2016, pp.210-217, August 2016.
[12] A. Biason, C. Pielli, A. Zanella, and M.Zorzi, "Access control for IoT nodes with energy and fidelity constraints," IEEE Transactions on Wireless Communications, vol.17, no. 5, pp.32423257,2018.
[13] Milton k. (n.d.), Can a Hacker Bypass Encryption? , Available from: http://itstillworks.com/can-hacker-bypass-encryption-2996.html.
[14] 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.
[15] 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
[16] 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/.
[17] En.wikipeedia.org. (2017). Smartphone. [online Available at: https://enwikipedia.org/wiki/smartphone.
[18] En.wikipeedia.org. (2017). Laptop. [online Available at: https://enwikipedia.org/wiki/Laptop
[19] 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 .
[20] Margeret Rouse (2014) Authentication, Available at : http://searchsecurity.techtarget.com/definition/authentication/.
[21] 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.
[22] 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