International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 7 Issue 5 May 2020

A brief study of various Highly User-Friendly, Secure, Privacy-Preserving and Revocable Authentication Mechanisms

Umesh Kumar Namdev[1], Sanjay Kumar Brahman[2]
Dept. of CSE, RKDF College of Engineering, Bhopal[1]
Dept. of CSE, Bhabha Engineering Research Institution, Bhopal[2]
umesh.namdev@gmail.com[1], sanjushukla2007@gmail.com[2]

Abstract: *We are living in a digital era, where most of the critical information whether it is confidential, academic documents or chats and even money transaction is being done in digit format. Digital technology is progressing at its large because of its ease & speed. With this digital data advancement responsibility & core need arises for its security arises. In protecting this data authentication mechanism plays a very important role. Authentication mechanism assures security of data by allowing legitimate users to access it. Using single phase authentication mechanism (UID & Password) is the easiest and convenient mechanism to implement and use in past days. With growing cruciality of data need arised to develop more secure & complicated authentication mechanism which cannot be easily breached. This gave birth to two phase authentication mechanisms that are commonly known as two-factor authentication mechanisms. Two phase authentication mechanisms provide additional security by adding one more factor for authentication in traditional single phase authentication mechanisms. There are lots of two phase authentication mechanisms that developed with technological advancement. In this paper we will review various two phase authentication mechanisms by considering security Enhancement they provide & ease of use in their implementation.*

Keywords— Authentication; Digital Data; Security; Single Phase Authentication; Two Phase Authentication**.**

1. INTRODUCTION

Authentication is a mechanism to assure whether or not somebody or one thing is, in fact, what it declares itself to be. Authentication mechanism provides access management for systems by checking to ascertain if a user's credentials match the credentials in a stored database of approved users present at data authentication server.

Users are typically known having a user ID and password. Authentication is accomplished once the user provides a credentials, as an example a password and user ID that matches therewith user ID and password stored on the database of authentication server. Most users are most aware of employing a password, which, as a chunk of data that ought to be well-known solely to the user, is termed a data authentication factor.

Authentication is vital as a result of it permits organizations to keep their networks secure by allowing solely genuine users (or processes) to access its protected resources, which can include pc systems, networks, databases, websites and different network-based applications or services.

Once genuine, a user or method is sometimes subjected to an authorization method as well, to see whether or not the genuine entity ought to be permissible access to a protected resource or system. A user may be genuine however fail to be given access to a resource if that user wasn't granted permission to access it.

Types of Authentication Mechanisms [14]:

Two-factor Authentication -- Two-factor authentication adds an additional layer of protection to the method of authentication. 2FA needs that a user offers a second authentication consider addition to the password. 2FA systems usually need the user to enter a verification code received via text message on a preregistered mobile phone, or a code generated by an authentication application.

Multifactor Authentication -- Multifactor authentication needs users to evidence with over one authentication factor, together with a biometric factor like fingerprint or face recognition, security key sort of possession factor or a sort of token created by an authenticator app.

One-Time Password -- A one-time password is an mechanically generated numeric or character set string of characters that authenticates a user. This password is merely valid for one login session or group action, and is sometimes used for brand new users, or for users who lost their passwords and are given a one-time password to log in and alter to a replacement password.

Three-factor Authentication -- Three-factor authentication (3FA) could be a sort of MFA that uses 3 authentication factors, typically a data factor (password) combined with a possession factor (security token) and immanency factor (biometric).

Biometrics -- whereas some authentication systems will rely exclusively on identification, biometrics are typically used as a second or third authentication factor. The additional common kinds of identification out there embody fingerprint scans, facial or retina scans and voice recognition.

Mobile authentication -- Mobile authentication is that the method of confirming user via their devices or confirming the devices themselves. This lets users log into secure locations and resources from anyplace. The mobile authentication method involves multifactor authentication that may embody one-time passwords, identification or QR code validation.

Continuous Authentication -- With continuous authentication, rather than a user being either logged in or out, a company's application frequently computes an "authentication score" that measures however certain it's that the account owner is that the individual who's using the device.

API authentication -- the quality ways of managing API authentication are: HTTP basic authentication; API keys and OAuth.

In HTTP basic authentication, the server requests authentication info, i.e., a username and password, from a client. The client then passes the authentication data to the server in an authorization header.

In the API key authentication methodology, a first-time user is appointed a singular generated value that indicates that the user is known. Then every time the user tries to enter the system once more, his distinctive key's accustomed verify that he's identical user who entered the system antecedently.

Open Authorization (OAuth) is an open standard for token-based authentication and authorization on the web. OAuth permits a user's account data to be utilized by third-party services, like Facebook, while not exposing the user's password. OAuth acts as an intermediator on behalf of the user, providing the service with an access token that authorizes specific account data to be shared.

2. LITERATURE REVIEW

In this paper [1] authors provided a novel and efficient authentication system which uses the mobile phone and cloud data centers to find the originality of the product. The system uses Quick Response codes to identify the products details. The project when implemented in the real life will provide a more effective authentication system which the common people can use to find the originality of the product before buying it. They can also make sure that the product which these buy is originally manufactured by the respective manufacturer and not from any counterfeiter. The system also reduces the cost of the authentication process as there is no need for adding up any costly tags to each product. Printing the QR codes is more economical than other authentication systems. The most important advantage of the system is that the authentication is done by the user itself and there is middleman in the process which increases the trustworthiness and security of the system.

In this paper [2], authors used principal curves approach for fingerprint minutiae extraction then these stored them in a DB on a cloud, then authors used the Bio-Hash function to secure the biometrics templates. Also they compared there approach with the approach presented in previous researches, and calculated the error rates for their approach and proved that these increase the system performance by 25%.

In this paper [3], authors present some advances on offline signature identification. Form the analysis of the recent literature in the field some of the most valuable approaches are presented and the most interesting directions for further research are highlighted.

In this paper [4], authors propose the implementation of a voice-based Fuzzy Vault authentication mechanism, for secure access and encryption support within Cloud platforms and Cloud shared storage. The experimental outcome, emphasis on assessing the performances of the biometric matcher, have shown FRR rates varying from 0% to 32% and FAR rates varying from 2.5% and 11.3%.

In this paper [5], authors propose a new image integrity authentication scheme based on fixed point theory. In the proposed scheme, the following three criterions are considered for selecting an appropriate transform $fk\ (\cdot\ )$

whose fixed points are used for image integrity authentication. 1) Fragility: the fixed points of *fk (·)* must be sparse; 2) easy calculation: a fixed point can be easily found by few iterations; 3) transparence: a fixed point can be found in a very small neighborhood of a given image function. They construct an appropriate transform *fk (·)* satisfying these criterions, based on the Gaussian Convolution and Deconvolution, called GCD transform. After establishing a theorem for the existence of fixed points of the GCD transform *fk (·)*, these give algorithms for a quick calculation of a fixed point image which is very close to the given image, and for the whole image integrity authentication scheme using the obtained fixed point image. The semi-fragility problem is also mathematically considered via the commutativity of transforms. Experimental results show that the proposed scheme has very good performance.

In this paper [6], authors developed an iris recognition algorithm based on Fisher algorithm which can be run in a lighter computing platform. Experiments conducted with CASIA database shows exciting results where the system achieves a very high accuracy. Iris recognition is a biometrics authentication system using iris image. It is one of the most reliable biometrics systems. The systems however require substantial computing power. Hence it is not been able to penetrate the market yet.

This paper [7] discusses the different ICA based techniques which are used in last decade. This paper reviews the comparative study of different face recognition techniques which is based on ICA. The important part of this survey is the discussion of previous work of face recognition related to ICA. There are different methods available related to ICA. Also, compare the different methods in tabular form. In this survey paper give the brief overview of “How to recognition face using image processing”.

In this paper [8] the human behavior is recognized from a set of video samples and the features are extracted using HOG transform. KNN classifiers are used to classify the features extracted from the videos. The HOG feature based analysis has achieved higher recognition and accuracy of 93%compared to the existing methods. There are several factors affects this Gait Authentication which can be classified into two categories. They are (i) External factors: angles, lighting atmosphere, clothes which have same colour as background and other external objects. (ii) Internal factors: changes in gait due to natural effects such as sickness, ageing, pregnancy, gaining or losing weight.

In this paper [9] authors proposed a robust face recognition technique by using local binary pattern and histogram of oriented gradient feature extractor and descriptors. In this study author have found that LBP feature extractors have almost one percent higher accuracy result than the HOG feature extractors which does not have that much difference. They have tested it for authentication purpose to sign in to their device by taking one label as an administrator and it gave significant results.

In this paper [10], authors present a novel security framework for NFC Secure Element-based Mutual Authentication and Attestation for IoT access with a user device such as a mobile device using NFC based.

Host Card Emulation (HCE) mode for the first time. The newly framework for NFC Secure Element-based Mutual Authentication and Attestation for IoT access provides a novel on-demand communication and control of IoT devices with security, privacy, trust and proof-of-locality using the NFC-based HCE mode and secure tamper-resistant SE and TPM modules. This system cannot verify the dynamic device state such as Control-Flow Integrity.

Author proposes a noisy vibration scheme for cloaking vibration sounds during pairing against such attacks. The scheme only requires a speaker for emitting the masking sound during key transmission [11]. They also study motion sensor exploits against this scheme and compliment it with additional measures to mask vibration effects on motion sensors. There analysis shows that while vibration pairing may seem to be an attractive mechanism for ensuring the security and trust in an IoT network, it needs to be protected against acoustic side channel attacks by defensive measures such as masking signals that are low cost and easy to implement.

In this paper [12], author studied the ensemble performance of biometric authentication systems, which are based on secret key generation. Referring to an ensemble of codes based on Slepian–Wolf binning, we have provided detailed, sharp analyses of the false–reject and false–accept probabilities, in terms of error exponents, for a wide class of stochastic decoders that covers the optimal MAP decoder, as well as several additional decoders, as special cases. Converse bounds have been derived as well.

Author propose a physical-layer challenge-response authentication approach in this paper [13] based on combined shared secret key and channel state information (CSI) between two legitimate nodes in an orthogonal frequency division multiplexing (OFDM) system. The proposed approach used even if the correlation of channel coefficients exists, which can be exploited to extract the shared secret key in conventional approaches. Furthermore, channel coding is employed to mitigate the difference between the two estimated channels as well as channel fading and background noise. Thus, they observed that in the proposed approach as a physical-layer authentication approach, the decoder's output can be used for authentication and provided a reliable decision under active attack.

3. CONCLUSION

A review for various available authentication techniques is described in this paper. In most of the authentication techniques User ID & password is used as the primary means for authentication.

The server verifies the PW corresponding to the User ID from verification table. If the submitted password matches the one stored within the verification table then server authenticates the user. However, there's a threat in such a process; An trespasser will impersonate a legal user by intercepting the messages from the network and login to the server later exploitation the intercepted data. Although the PW is encrypted throughout communication, such an impersonation attack continues to be attainable.

Here arises a necessity for a mechanism that is most dynamic that if an trespasser intercepts the message then additionally he shouldn't be ready to build successful authentication try.

REFERENCES

[1] Umanandhini .D, Latha Tamil Selvan, Udhaya kumar .S & Vijayasingam .T presented paper entitled "Dynamic Authentication for Consumer Supplies in Mobile Cloud Environment" in IEEE conference at ICCCNT'12, Coimbatore, India.

[2] Heba M. Sabri, Kareem Kamal A.Ghany, Hesham A. Hefny & Nashaat Elkhameesy presented paper entitled "Biometrics Template Security on Cloud Computing" at 978-1-4799-3080-7/14/$31.00 @ 2014 IEEE.

[3] D. Impedovo, G. Pirlo & M. Russo presented paper entitled "Recent Advances in Offline Signature Identification" at IEEE 2014 14th International Conference on Frontiers in Handwriting Recognition.

[4] Marius-Alexandru Velciu1, Alecsandru P˘atra¸scu & Victor-Valeriu Patriciu presented paper entitled "Bio-cryptographic authentication in cloud storage sharing" at 9th IEEE International Symposium on Applied Computational Intelligence and Informatics • May 15-17, 2014 • Timişoara, Romania.

[5] Xu Li, Xingming Sun & Quansheng Liu Patriciu presented paper entitled "Image Integrity Authentication Scheme Based on Fixed Point Theory" at IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 24, NO. 2, FEBRUARY 2015.

[6] Hermawan Nugroho, Hamada Rasheed Hassan Al-Absi and Lee Pei Shan, "Iris Recognition for Authentication: Development on a Lighter Computing Platform", in IEEE 978-1-5386-8369-9/18/$31.00 ©2018.

[7] Rajat Naik, Dr. Dhirendra Pratap Singh and Dr. Jaytrilok Choudhary, "A Survey on Comparative Analysis of Different ICA based Face Recognition Technologies", Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018), IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1.

[8] S. Joul Monisha and G. Merlin Sheeba, "Gait Based Authentication with Hog Feature Extraction", in IEEE 978-1-5386-1974-2/18/$31.00 ©2018.

[9] Melkye Wereta Tsigie, Rasika Thakare and Rahul Joshi, "Face Recognition Techniques Based on 2D Local Binary Pattern, Histogram of Oriented Gradient and Multiclass Support Vector Machines for Secure Document Authentication", Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2.

[10] Divyashikha Sethia, Daya Gupta and Huzur Saran, "NFC Secure Element-based Mutual Authentication and Attestation for IoT access", JOURNAL OF TRANSACTIONS ON CONSUMER ELECTRONICS, VOL. 14, NO. 8, SEPTEMBER 2018, DOI 10.1109/TCE.2018.2873181, IEEE, Transactions on Consumer Electronics.

[11] S Abhishek Anand and Nitesh Saxena, "Noisy Vibrational Pairing of IoT Devices", DOI 10.1109/TDSC.2018.2873372, IEEE.

[12] Neri Merhav, "Ensemble Performance of Biometric Authentication Systems Based on Secret Key Generation", DOI 10.1109/TIT.2018.2873132, IEEE.

[13] Jinho Choi, "A Coding Approach with Key-Channel Randomization for Physical-Layer Authentication", DOI 10.1109/TIFS.2018.2847659, IEEE.

[14] https://searchsecurity.techtarget.com/definition/authentication.