International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey of Multi level Authentication for improving the Privacy Preservation and Security

Mr.Sachin M.Vaidya[1], Prof. Rahul Patil[2]

[1]Final year Student of Master of Computer Engineering, Bharati Vidhyapeeth College of engineering, Navi Mumbai – 410210, Maharashtra,India sachin.m.vaidya@gmail.com

[2]Assistant Professor of Master of Computer Engineering, Bharati Vidhyapeeth College of engineering, Navi Mumbai – 410210, Maharashtra,India Rahhul.patil@gmail.com

ABSTRACT

The paper introduces a agenda for multi-Level or composite authentication in the system. The paper discusses challenges of authentication and different area of the authentication.This paper also describes the existing emerging sensors (by Level providers) that allow to authenticating a user with the system offline or by existing the cloud. The basic challenges of user as well as the service provider perspective are also verified with system Now a day, digitalization determined to all the sides of the updated society environment. Also maintain the authentication that covers many different areas of a hyper-connected world, including payments, communications, access management, etc. we also focus on the evolution of authentication systems towards Multi-Level Authentication (MLA) starting from Single-Level Authentication (SLA) and through Two-Level Authentication (2LA). MLA is expected to be used for human-to-everything communication by enabling fast, user-friendly, and reliable authentication when authenticated a service.

Keywords: survey; authentication; SLA; 2LA; MLA; evolution; vision

INTRODUCTION

The implementation of smart devices and related connectivity loads has impacted mobile services around the digitalization environment. According to work of authentication process where a "user identifies himself by sending data to the system. This definition not changed drastically over time in spite of the fact that a simple password is no longer the only level for validating the user in the information technology perspective.

Authentication is safeguard against illegal access to the device or any other sensitive application, where offline or online.

Single-level Authentication (SLA) was mostly adopted by the society due to its simplicity and user friendliness. As an example, the use of a password (or a PIN) to confirm the ownership of the user ID could be considered. This is the basic level of authentication. With sharing the password, one can compromise the account respectively. Likewise, an unauthorized can also attempt to implement access with utilizing the dictionary threads, rainbow table, or social engineering techniques. Generally, the password complexity requirement to be considered whereas utilizing this type of authentication

Further, it was realized that authentication with just a single level is not reliable to provide adequate protection due to a number of security threats. As an next step forward, Two-Level Authentication (2LA) was proposed that couples the representative data (username/password combination) with the level of personal ownership, such as a smartcard or a phone.

Basically three Classifications of level groups are available to join individual with the established credentials

Knowledge Level:

In this level something is the user knows, such as a password, simply, a "secret" for the authentication

Figure: Knowledge level Authentication

In the knowledge Level User having the Knowledge of their Authentication Parameters as likes Pin or Password

Ownership Level:
In the Ownership level that something the user has, such as cards, smartphones, or other tokens

Figure: Ownership level Authentication

Biometric Level is something that user is connected with hardware, i.e., biometric data or behavior pattern.

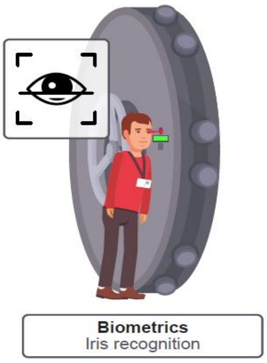

Figure: Biometrics level Authentication

Multi-Level Authentication (MLA) was proposed to provide a multi level of safety and securities to facilitate continuous protection of computing devices as well as other critical services from unauthorized access by using more than categories of credentials. In important part of MLA is based on biometrics, which is automated recognition of individuals based on their behavioral and biological characteristics.
The evolution of authentication methods is shown in Figure.

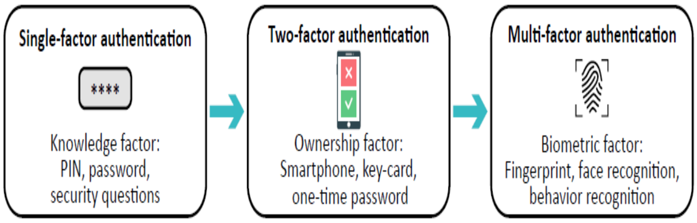

Figure: level of Authentication

Generally, MLA applications are divided into three market-related groups:
Professional applications, as like, account login, e-commerce, ATM, physical access control, etc.;
Governmental applications, as Like, identity documents, government ID, passport, driver's license, social security, border control, etc.; and
Forensic applications, as like, criminal investigation, missing children, corpse identification, etc. Generally, the number of scenarios related to authentication is indeed large.
Multi level Authentication becomes an extremely critical Level for:
Validating the identity of the user and the electronic device (or its system)
Validating the infrastructure connection with validating the interconnected internet devices, as a smartphones, wearable device, any other digital token (dongle).
Currently, the main MLA challenges are the absence of correlation between the user identity and the identities of smart sensors devices within the electronic device/system. About security, this connection must be developed so that only the legitimate operator, e.g., the one whose identity is authenticated in advance, can gain the access rights. With the same time, the MLA process also as user-friendly as possible

MULTI LEVEL AUTHENTICATION AREA

Presently, the authentication systems utilize in various area and number of sensors that enable identification of a user. In this section, we clarify on the MLA-details level, with market-available sensors, and related challenges. We explain additional details on the ones that are to be potentially deployed in the near future

1. Password Protection

In the protection password written by user itself and he/she should be remember in the memory only drawback is the recall every time when authentication

2. Token Presence

Token may be software and hardware the perspective, a user may present a smartcard, phone, wearable device, etc., which are more complicated to delegate. System equipped with a radio interface allowing for two-way communication with the token. The main drawback of the above is the problem of uncontrollable duplication.

3. Voice Biometrics

With the smart electronic devices are placed with a microphone that allows utilizing voice recognition as one level in the MLA ,because of voice changer which is a serious drawback of utilizing voice as a primary authentication method

4. Facial Recognition

Facial recognition technology was based on the landmark picture analysis, which was relatively to replicate by supplying the system with a image. The advancement of this system reached the point of recognizing the actual expressions of the user. For facial recognition required to equip the system and at least one output device with camera.

5. Ocular-Based Methodology

The iris recognition techniques approach doesn't require the user to be select to the capture device while analyzing the color pattern of the user eye. Retina verified is another attractive technique. The most challenges in those methods are required high quality capture device with robust mathematical technique to identified the image

6. Vein Recognition

The advances of fingerprint offer an opportunity to accumulate the vein picture of the finger also. More complicated devices utilize palm print recognition to acquire and store the Shape/movement of the entire hand. Vein biometrics is still weak to spoofing attacks.

7. Fingerprint Scanner

Fingerprint is biometrics authentication in the level. Most of the Smartphone user installs an additional camera for fingerprint instead of normal authentication

8. Thermal Image Recognition

Compare with vein recognition, thermal sensor is used to reconstruct the unique thermal image of one's body blood flow in proximity. Multiple challenges with this authentication method

9. Geographical Location

Use of geographical location to validate environment access to the device/service could be granted is a special case of location-based authentication.

Mainly, GPS signal could be easily jammed or considered faulty due to the transmission properties; thus, it is recommended to utilize at least two location sources, GPS and wireless network cell ID is example of location. A smartphone used to support MLA from the location acquisition.

FUTURE OF MLA INTEGRATION

For increased availability of biometric services in a wide range of readily-available user products is pushing the concept of sharp MLA integration. Currently, we and early technology adopters attempt to integrate new ideal sensors to be used in MLA systems.

1. Behavior Detection

A modern example of the identification is the process of tapping the Smartphone of the screen. This implement could be easily combined with any text-input authentication methods as a typing pattern is unique for each user. MLA system is specifically developed for predefined gesture analysis, the user is required to replicate a previously learned movement while holding or wearing the sensing device.

2. Beam-Forming Techniques

In the techniques concept from the telecommunication environments, Radio-frequency Identification (RFID) and Near-Field Communication (NFC) techniques have already observed widespread acceptance within the community. Current trends in physical-layer security claim that utilizing wireless Multiple-Input and Multiple-Output (MIMO) solutions to locate the source of the signal may become a significant breakthrough in validating the token on the user body

3. Occupant Classification Systems (OCS)

Some vehicular systems already have the OCS solutions integrated in user cars. A system of sensors can detect who is currently in the passenger/driver seat by used, for example, weight or posture and automatically adjusting the vehicle to personal needs

4. Electrocardiographic (ECG) Recognition

ECG data could be collected from the user’s smart watch or activity tracker and compared with an individually stored pattern. The main benefit of using this factor for authentication is that ECG signals emerge as a potential biometric modality with the advantage of being difficult (or close to impossible) to mimic. The only way is by utilizing the existing personal recording.

5. Electroencephalographic (EEG) Recognition

The brain waves verifying and could be considered from the fundamental philosophical proposition “Cogito ergo sum” by R. Descartes, or “I think, therefore I am”.
It allows for obtaining a unique sample of the person’s brain activity pattern. Formerly, EEG data capture could have been performed only in clinical settings by using invasive probes under the skull or wet-gel electrodes arrayed over the scalp.

6. DNA Recognition

Human cell lines are an essential resource for research, which is most frequently used in reverse genetic approaches or as in vitro models of human diseases. It is also a source of unique DNA fingerprinting information. Even though the process is time-consuming and expensive, it may be potentially utilized to pre-authorize the user to the highly secure facility along with other factors.
Subsequently, a comparison of the main indicators for the already deployed and emerging factors is given in

Level of Authentication	Universality	Uniqueness	Collectability	Performance	Acceptability
Password	Not Applicable	Low	High	High	High
Token	Not Applicable	Medium	High	High	High
Voice	Medium	Low	Medium	Low	High
Fingerprint	Medium	High	Medium	High	Medium
Face	High	Low	Medium	Low	High
Vein	Medium	Medium	Medium	Medium	Medium
DNA	High	High	Low	High	Low

Figure: Multi level Challenges with Operation table

MLA OPERATION CHALLENGES

An integration of novel solutions has always been a major challenge for both developers and managers. In the first place, user acceptance is a critical aspect for the adoption of strong identity and multi-factor authentication. While adopting and deploying MLA solutions, it is required to follow a careful and thorough approach where most challenges arise from opportunities and potential benefits

Following challenges in multi level Authentication

Usability: usability is main challenges emerging in the authentication process that would be characterized from three perspectives
Uniqueness indicates that how well the level differentiates one person from another;
Collectability measures how easy it is to acquire data for processing;
Performance indicates the achievable accuracy, speed, and robustness;
Acceptability stands for the degree of acceptance of the technology by people in their daily life;

Some other challenges and formalizes the recommendations for improved ease of integration.

1. Task efficiency time to register and time to authenticate with the system;
2. Task effectiveness the number login attempts to authenticate with the system;
3. User preference whether the user prefers a particular authentication scheme over another.

Security and privacy of multilevel authentication

With digital system composed of critical components, such as sensors, data storage, processing devices, and communication channels. These are vulnerable to a variety of attacks at entirely different levels, ranging from replay attempts to adversary attacks Security is thus a necessary tool to enable and increase privacy. The recommendation to select appropriate processing hardware for the server/capture side. The MLA security should support a penetration of testing to assess its potential Drawbacks.
Now a Days, the multiple development are often conducting audit to evaluate the risks and act based on such verification for more careful planning. The MLA system should be assessed for deliver a more secure environment.

ROBUSTNESS TO OPERATING ENVIRONMENT

In the analysing of listed challenges, we discussed in the above sections. It is possible to verified and assess the entire MLA system. In the follows, we propose an approach to enable Multi level Authentication for vehicular integration based on the availability of a different number of sensors in modern vehicles and society

DISCUSSION AND FUTURE PROSPECTS

Currently, authentication matters more than ever before. In the digital era, most users will believe on biometrics in concerning systems security and authorization to complement the conventional passwords. Even though privacy, security, usability, and accuracy concerns are still in the place, Multi level becomes a system that promises the security and ease of use needed for modern users while acquiring access to sensitive data. Without a doubt, biometrics is one of the layers to enable the future of Multi level Authentication.

In the future Perspective of multi level authentication we also consider the next area that will be Composites and Multilevel for increasing the Securities and Privacy .with conventional single-Level systems of today are based on only one parameter (unimodality property), if its acquisition is artificial in any way (be it noise or disruption), the overall accuracy will humiliate. Many successful applications have been aware to the community for more than a decade. Examples will be found in where conventional factors, as like iris, retina, fingerprints, etc., are considered. Utilizing neural networks for the next-generation biometrics is the most likely way to proceed due to presently high levels of the analysis complexity. With summary, Authentication technology is a prominent direction driven for increasing the Securities in the cloud and mobile device market.

Conclusion: with this concluded this session we are observing that the multilevel Authentication will improve the Security and privacy also consider the composites authentication for the future Enhancement of the topic or research object.

References

Konoth, R.K.; van der Veen, V.; Bos, H. How anywhere computing just killed your phone-based two-factor authentication. In Proceedings of the International Conference on Financial Cryptography and Data Security,Christ Church, Barbados, 22–26 February 2016; Springer: Berlin, Germany, 2016; pp. 405–421.

Kim, J.J.; Hong, S.P. A method of risk assessment for multi-factor authentication. J. Inf. Process. Syst. 2011,7, 187–198.

Dasgupta, D.; Roy, A.; Nag, A. Toward the design of adaptive selection strategies for multi-factor authentication. Comput. Secur. 2016

Bonneau, J.; Herley, C.; Van Oorschot, P.C.; Stajano, F. Passwords and the evolution of imperfect authentication. Commun. ACM 2015, 58, 78–87.

Wang, D.; Wang, P. Offline dictionary attack on password authentication schemes using smart cards.In Information Security; Springer: Berlin, Germany, 2015; pp. 221–237.

Ah Kioon, M.C.; Wang, Z.S.; Deb Das, S. Security analysis of MD5 algorithm in password storage.Appl. Mech. Mater. 2013, 347, 2706–2711.

Heartfield, R.; Loukas, G. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Comput. Surv. (CSUR) 2016

Grassi, P.A.; Fenton, J.L.; Newton, E.M.; Perlner, R.A.; Regenscheid, A.R.; Burr, W.E.; Richer, J.P.

Lefkovitz, N.B.; Danker, J.M.; Choong, Y.Y.; et al. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management; Technical Report; National Institute of Standards and Technology:

Gaithersburg, MD, USA, 2017. Frank, M.; Biedert, R.; Ma, E.; Martinovic, I.; Song, D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Inf. Forensics Secur. 2013, 8, 136–148.

Jorgensen, Z.; Yu, T. On mouse dynamics as a behavioral biometric for authentication. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; ACM: New York, NY, USA, 2011; pp. 476–482.

National Research Council;Whither Biometrics Committee. Biometric Recognition: Challenges and Opportunities; National Academies Press: Washington, DC, USA, 2010.

Huang, X.; Xiang, Y.; Bertino, E.; Zhou, J.; Xu, L. Robust multi-factor authentication for fragile communications. IEEE Trans. Dependable Secur. Comput. 2014, 11, 568–581.

Tahir, H.; Tahir, R. BioFIM: Multifactor Authentication for Defeating Vehicle Theft. In Proceedings of the World Congress on Engineering, London, UK, 2–4 July 2008; Volume 1, pp. 1–3.

Coventry, L.; De Angeli, A.; Johnson, G. Usability and biometric verification at the ATM interface. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Ft. Lauderdale, FL, USA, 5–10 April 2003; ACM: New York, NY, USA, 2003; pp. 153–160.

SC Media UK. 68% of Europeans Want to Use Biometric Authentication for Payments. 2016. Available online: https://www.scmagazineuk.com/68-of-europeans-want-to-use-biometric-authentication-forpayments/ article/530818/ (accessed on 4 January 2018).

Khan, R.; Hasan, R.; Xu, J. SEPIA: Secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices. In Proceedings of the 3rd IEEE International Conference on Mobile Cloud Computing,Services, and Engineering (MobileCloud), San Francisco, CA, USA, 30 March–3 April 2015; pp. 41–50.

Adeoye, O.S. Evaluating the performance of two-factor authentication solution in the banking sector. Int. J. Comput. Sci. 2012, 9, 457–462.

Aloul, F.; Zahidi, S.; El-Hajj, W. Two factor authentication using mobile phones. In Proceedings of the International Conference on Computer Systems and Applications, Rabat, Morocco, 10–13 May 2009;pp. 641–644.

VNI Cisco Global Mobile Data Traffic Forecast 2016–2021. White Paper, 2017.