

Forth Factor Authentication: Who Am I

Mohammed Ali Shaik, V. Sudharani

Abstract— The process of authentication for a user is considered to be most vital and important in the field of computing systems, most of the conventional authentication process depends on one or all the three factors such as a password or a fingerprint and sometimes even through SMS or Voice. In this paper, we try to implement and explore the fourth factor authentication system which is based on the social networks which now a day's considered to be part of living for every user.

In this paper I will be dealing with the process of Human authentication through mutual acquaintance is traditional process but most authentic for implementing computer security, by performing delegation of privileges, generation of peer-level certificates, assistance at various levels and providing quality networks for authenticating by relying on unreliable human beings tendency is to change at a rapid rate.

The methodology which I propose is useful when existing authentication process consisting of passwords and Voice of SMS or Finger print's are compromised or out of reach when compared with cloud, in other words it is an emergency authentication process, which is a practical prototyping model that questions who am i.

Index Terms— Cloud, Human Factors, Security, Authentication, Networks, Cloud Computing, Key.

1 INTRODUCTION

In the present cloud computing era enormous amount of data is yielded from computers and smart phones or any transactional data which is to be stored on the cloud computing environment needs security and reliability of data.

Cloud computing is the result of the progress and utilization of existing technologies and paradigms where the main goal of cloud computing is to allow various users to take benefit from all of these technologies without possessing deeper knowledge or expertise with each one of them as the cloud aims to cut costs and helps the users focus on their core business without concentrating on present day IT obstacles [1].

The process of authentication ensures us and confirms a user's identity by providing the login credentials where authentication process for every user is unique and the process of authentication is considered to be one among five pillars pertaining to information assurance where ever user is authenticated and authorized to access the data on cloud and figure 1 represents the cloud computing architecture.

The Public Key Infrastructure authentication process uses digital certificates for providing a user's identity before the certificate is expired and some of the other authentication tools are key cards and USB tokens. In the present day one of the greatest authentication threat is due to email because whenever a user forgets the credentials an email is sent to his or her account for generating new access credentials and sometimes these type of

unsecured emails often appear legitimate.

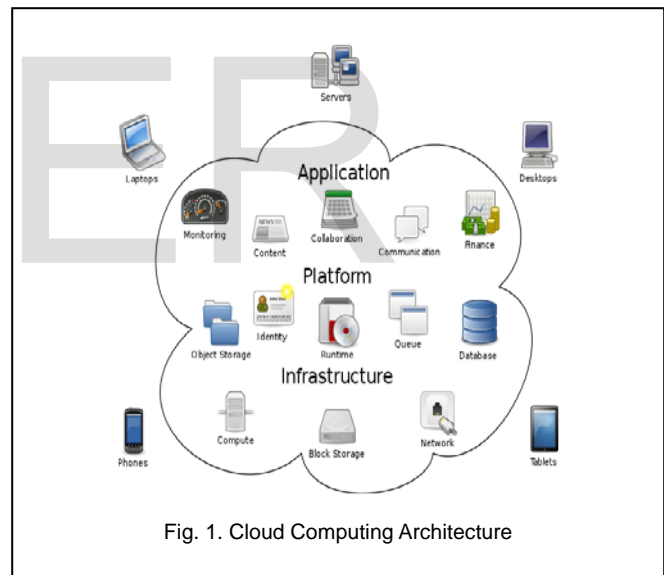


Fig. 1. Cloud Computing Architecture

Many user authentication tools and technologies are almost vulnerable to theft or loss or a part of illegal use as the technology depends on wired or wireless network systems that compensates the information disclosure where the illegal data use have been reported very frequently due to various security threats at various levels. And one of the key rule of present day is to never trust in the manager who provides third party authentication. In other words, it is not that much easy to guarantee the authentication and verification of entities in the real world scenario.

2 RELATED WORK

Most of the researchers have published their research and findings in this area and I have identified some of them pertaining to be a major concern towards my paper and researches are:

- Mohammed Ali Shaik is currently working as Assistant Professor in Computer Science & Engineering department, Aurora's Research & Technological Institute, Warangal, Telangana, India, PH-9000498496. E-mail: niharali@gmail.com
- V. Sudharani is currently working as Assistant Professor in Computer Science & Engineering department, Aurora's Research & Technological Institute, Warangal, Telangana, India, PH-8106860069. E-mail: suchisafriend@yahoo.com@gmail.com

As per Hadid and etl [2] there exist many different modalities that consist of many verification processes and some of them mainly concentrates on face recognition or fingerprint recognition or password or CAPTCHA or voice verification and recognition code sent through SMS for providing authentication in hand held or the portable devices.

As per Vaidehi and etl [3] the skin color based technique is effectively used for detecting and verifying the human face which is compared with the input image as the visual features such as Profile Fourier Coefficients PFC is extracted using template matching approach as PFC is effectively used to combat terrorism in public areas such as airports and territorial border crossing points or by countries border security force to safe guard the nation.

As per A K Jain and etl [5] the basic component analysis is used to attain the required features by verifying fingerprints using improved Minutiae Extraction Algorithm MEA is used to attain the essential effective features. But in this approach the only disadvantage is it is computationally expensive when compared to other existing biometric comparison devices.

As per D Currie [7] voice recognition is also used as a means of authentication for voice modality authentication where the task is identified at different levels with their levels of features and will extract the pronunciation of vowels and consonants. And based on the overall accuracy of authentication process many independent measurements are combined together but the voice recognition lacks the robustness in a noisy environment or a place where huge public gathering is available.

Most of the end users mobile phones consist of information pertaining emergency authentication where most of the institutions consisting of higher risk in online transactions which can be operated in many ways. Most of the time a financial institution initiates by making a phone call to a customer and tends to request confirmation of completion of the transaction using automated voice recognition or keypad based data entry system. Or the other approach consists of transmission of a SMS messaging via a phone (one time password) and then request the user to provide with the received code or SMS data into the web page. And is considered to be one of the effective method by present day implementers.

Due to immense use of portable devices such as mobile phones or tabs the usage of portable computing is increasing day by day, though it requires streams of authentication we can also consider the analysis of keystrokes as proposed by F Bargadano [9] which may also include the dynamic keystrokes attained by either virtual keyboard or the physical keyboard that is based on the device being used.

Most of the current day industries which have confirmed their existence in the market are implementing two factor authentication mechanisms that uses multi factor authentication for their existing cloud applications and apps by generating one time passwords by sending a SMS or text message or by making a automated phone call to the user.

The above said approach is considered to be a static one as it does not include various concepts of authentication such as various user roles and their login credentials or the available environmental factors or constraints and various devices and media that are used for imparting and delivering various modalities. By considering all the above said factors and devices into consideration the implemented process is appeared to be best suited for processing sensitive cyber systems in a cloud computing environment.

The techniques that are implemented in entities authentication process that is intern based on the concept of IC card or the process of implementing RFID which is used for various wired or wireless communication devices and their implemented services. These services are most often seen in laptops or in case of smart phones.

As per B Ross limitations of passwords that are generated by third party or themselves is most often known in the security community due to poor selection by users such as their sir names or their children names or their spouse name or their date of birth to be the password which are easily attained by most of the strangers. Some hackers can attain passwords by implementing phishing or by fraudulent use of email spoofing which can capture user passwords based on various domain names [9].

As per the reference of R Griffith life questions which are something you can recollect very easily as a authenticator and but are most often used in emergency authentication process or in case of recovery process. There are many features and facts related to life questions where these are used as a shield for implementing the authentication process for recovering an account in cloud computing environment and thus receive infrequent use. As it renders a hacker to provide with answer consistently as the answers are related to popular life questions most often and are much vulnerable to attacks in any environment [10].

3 METHODOLOGY

The frame work which I proposed is based on the concept of Active Authentication Mechanism (AAM) and is considered to be an iterative protection attainment against all kinds of illegal access and threats of use in present day cloud computing systems [11].

The framework of AAM requires continuous and rigorous monitoring of various user activities for providing random re-authentication process for tackling the ongoing threats that tends to breach the whole authentication system where the cloud environment is prone to such security threats, for attaining an open ended solution where every users authenticity can be compromised in many ways and can be re initiated in many ways and some of them are through known password authentication or pin numbers verification and authentication as the users will posses smart card or digital certificate.

In other cases a user can be tested using his or her fingerprint or iris scan or through voice recognition or a critical one is by





using the GPS or IP address of the targeted machine. In the present scenario two or more process of authentication are combined and a framework is constructed for obtaining secured authentication process which is hardend to become non vulnerable or hacker prone.

In the present era of authentication system there are several authentication modalities exists in the present era and one or more of such can be used and they may be face authentication system or finger print authentication system or retina authentication system or password authentication system or CAPTCHA authentication system or SMS authentication system or Voice authentication system and keystroke authentication system can be used.

In our proposed frame work AAM we use password authentication system as Factor-1, then Finger print authentication system as Factor-2, then SMS/Voice authentication system as Factor-3, and Who Am I as forth Factor where we use the social networks for authentication a user.

Many calculations are evaluated and stored in various virtual machines (VMs) where the implementations of query execution and data retrieval modalities are implemented from user console or system to the authentication server located locally or at a remote location. Major benefits of imparting VMs in the proposed system will modulate significant code that can be logically separated and run independently on the cloud computing environment. Suppose in case of a VM is being compromised, implementation of decision support algorithm will tend to select data from rest of non compromised modalities from the system.

TABLE 1
FOUR FACTOR COMPUTATIONS FEATURES& PARTICULARS

Factor	Features	Particulars
 Password	1) Master password 2) Key pattern 3) Security question 4) Profile information	First two are used for authentication and last two are for recovery
 Thumb	1) Singular points 2) Ridge orientation map 3) Ridge frequency map	Pores are considered to be highly distinctive in terms of their number or position and shape. Identification of a feature.
 SMS or Voice	1) Any number of characters 2) Special characters 3) Pitch 4) Format Features	First two are used for SMS and last two are for Voice for providing authentication.
 Social Networks	1) Friends List 2) Acceptance Rate 3) Login Credentials	Authentication is based on online social networks

3.1 AAM Implementation

The implementation design of proposed AAM lies in the design process on various constraints and objective functions that may sometimes tend to yield penalty functions. As per Table 1 the authentication process takes steps one by one that is collecting the password first then the process of acquiring the thumb impression. This process may fail when the user has punctured his or her thumb or henna is applied on the thumb then the biometric device will fail to authenticate the authenticated user.

The next step is to authenticate upon receiving of SMS or voice, this process suffers when the service provider server is down or when the mobile phone is switched off, though there may be an option of acquiring or using the backup codes which are predefined or pre-allocated for every user. Factor suffers from failure.

In order to achieve this, firstly the criteria for selecting authentication modality are to be determined. Fig. 2 shows some of these criteria including the variability of devices, media, and environments and shows the appropriate frequency and count of authentication modalities in each setting.

The proposed fourth factor is considered to be most effective based on my study as the process involved is authentication is performed by the friends list in a social network as the present day era is more reluctant to social networks than any others hence we consider the forth factor to be more authentic as it is used in online social networks and is authenticated by its users or from friends list.

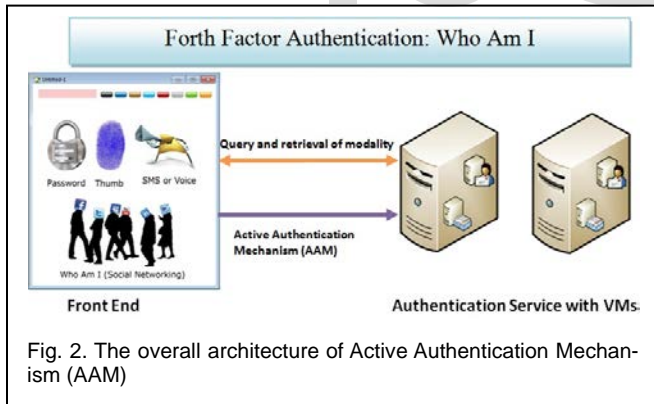


Fig. 2. The overall architecture of Active Authentication Mechanism (AAM)

Selecting the modalities from both biometric and non-biometric modalities are considered in the proposed system as specified in Fig 2 though biometric modality has uniqueness but it suffers from some drawbacks for which it is not suggested to design an active authentication system which is only based on biometric devices. Another disadvantage of biometric devices is false reading which sometimes creates vulnerability that is false acceptance rate and false rejection rate is considered to be a major drawback [12].

The above table represents detailed information of various factors of authentication are used in the proposed system.

The process authenticates based on the below figure:

F_1, F_2, F_3, F_4	$(Fms_{11} \dots 1n) \dots (Fms_{k1} \dots kn) \dots (Fms_{m1} \dots mn)$
----------------------	---

Example

F_1	0001	(0010101)..... (0010100).....(0010010)
F_2	0010	(0010110)..... (0010010).....(0010110)
F_3	0100	(0010011)..... (0010101).....(0011100)
F_4	1000	(0011100)..... (0011110).....(0010000)

In the implementation of AAM different variants of device and media are considered to create and stipulate constraints by using objective and penalty functions, where the objective function concentrates on modality that is for attaining trust-worthiness factor which is represented in the form of numeric values for a particular type of device or media where a specific value that is yielded shows the impact factor on a particular selected modality value attained. Higher the value means modality is more trustworthy in current environment and if the factor value is less then there is chance of getting the environment compromised. So decision making will be very easy.

3.2 Trust worthiness for AAM Implementation

In this paper we have proposed four modalities and some consists of biometrics (fingerprint) and the rest are the common methods of authentication (password, Voice or SMS) and the proposed one is the Who am i that is AAM prototype that is based on online social networks. Most often the trust worthiness is calculated in terms of active and passive modalities.

The function that calculates trustworthy consists of various combinations that exploit pair wise relative study and then implement the comparisons and the following three cases:

- Case 1: A Fixed Device is more trustworthy than a Portable Device.
- Case 2: A Portable Device is more trustworthy than a Fixed Device.
- Case 3: Both Devices are almost equally trustworthy or non-trustworthy.

The representation of deterministic trustworthy value is: T_{ijm} for the mth modality (4th option) with ith device with N options and jth media of P options for every pair that consists of comparison involving ith and kth devices for a fixed jth media and fixed mth modality with T_{ijm} values:

$$\sum_{i,j}^{1,2,3} T_{ij}^m - \sum_{i,j}^{1,2,3} T_{kj}^m \geq C_1 \text{ where } i \neq k \quad (1)$$

$$\sum_{i,j}^{1,2,3} T_{ij}^m - \sum_{i,j}^{1,2,3} T_{kj}^m \leq C_1 \text{ where } i \neq k \quad (2)$$

$$|\sum_{i,j}^{1,2,3} T_{ij}^m - \sum_{i,j}^{1,2,3} T_{kj}^m| \leq C_1 \text{ where } i \neq k \quad (3)$$

$$\text{Max} \sum_{i,j}^{1,2,3} T_{ij}^m = 1, \text{ and } \sum_{i,j}^{1,2,3} T_{ij}^m \geq 0 = 1, 2, 3 \quad (4)$$

After implementing the trust worthiness the values that attained are:

- Trust (Fixed Device): $TFD = 1 + 0.63 + 0.45 = 2.08,$
- Trust (Portable Device): $TPD = 1 + 0 + 0 = 1,$
- Trust (Hand Held Device): $THD = 0 + 0.28 + 0.12 = 0.30,$
- Trust (Wired Media): $TWI = 1 + 1 + 0 = 2,$
- Trust (Wireless Media): $TWL = 0.63 + 0 + 0.26 = 0.89,$
- Trust (Cellular): $TCL = 0.36 + 0 + 0.13 = 0.49,$

Based on the values attained the conditions are subject to be verified and regarded to be satisfied and I used different devices using pair wise comparison technique the table represents the designated values.

AAM framework is designed to attain the primary objective function that implements forth factor authentication system where both device and media are equally considered and by which weights are intern assigned for each of them as shown

TABLE 2
FOUR FACTOR TRUST WORTHINESS COMPUTATIONS

Trust	Value Attained
Fixed Device	2.08
Portable Device	1
Hand Held Device	0.30
Wired Media	2
Wireless Media	0.89
Cellular	0.49

in below figure:

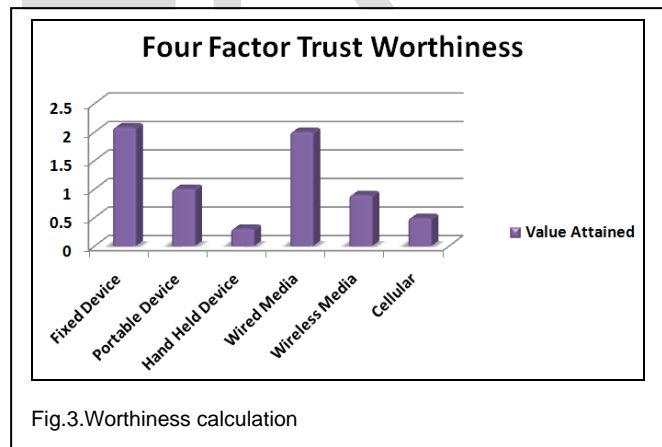
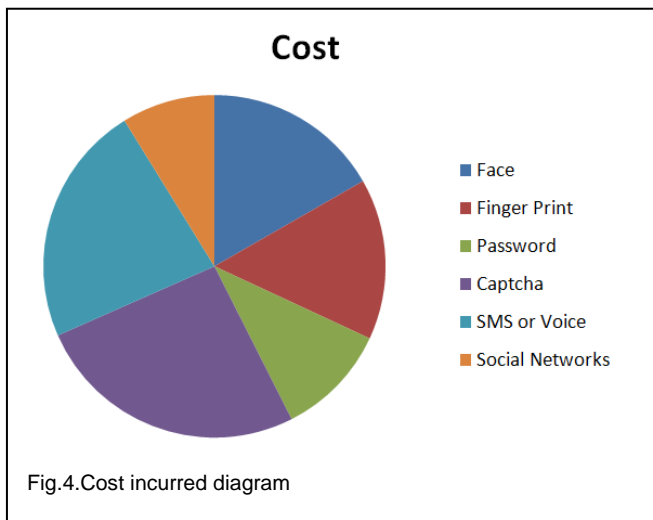


Fig.3. Worthiness calculation

And the incurred cost in implementing all the available factors as specified in the literature review by various researchers are depicted in figure as:



If we compare the figure 4 cost of the proposed fourth factor being implemented is very less than that of all others that are existing, though we combine existing three other factors such as password, figure print and SMS or Voice then the total cost incurred is moderate.

3.3 Steps Involved in AAM Framework

The below are the steps involved in AAM framework

1. User contacts the Helper System: The AAM process begins with the asker U contacting the helper H via a transmission line and claiming to be U.
2. Helper (H) authenticates user (U): The H verifies the identity of the U as the process has to assure H with probability at least $1-\mu$ that the claimed identifier U is considered to be the user's true identifier. If H gets any doubt about the authenticity then H may request U for executing fourth factor authentication.
3. Helper Authenticates at server: by using the client machine helper accesses a web page that strongly authenticates U to the server using two factor authentication that uses a authenticated password and finger print verification then the helper identifies U to be authentic. Upon failure of this step Fourth factor will be implemented.
4. Helper generates OTP: H generates OTP code using a random method which is of 8 bits.
5. Helper hands over OTP to user: the 8 bit generated OTP code will be handed over to U using SMS or through Voice call. Upon failure of this step Fourth factor will be implemented.
6. User Enters the OTP pass code: A special purpose pass code verifier will be held responsible to verifying and authenticating the pass code generated and later expires the pass code as it must be used only once. Upon failure of this step Fourth factor will be implemented.
7. Server Authenticates User (U): the server searches and identifies its own database and activates session for user upon through all the three factors or through implementing only fourth factor. In either of the cases access is provided to U.

4 CONCLUSION

In this paper I proposed various factors available for authenticating a cloud user and when any of the factors fail due to any reason then fourth factor will be used to authenticate the user. In other words fourth factor is considered to be emergency authentication technique.

I proposed and implemented Active Authentication Mechanism (AAM) framework that includes trustworthiness and yielded positive results and I also specified the steps involved in AAM framework implementation. The table represents the data used to implement based on candidate sets C1, C2 and C3 formulas.

REFERENCES

- [1] HAMDAQA, Mohammad (2012). Cloud Computing Uncovered: A Research Landscape. Elsevier Press. pp. 41-85. ISBN 0-12-396535-7.
- [2] A. Hadid, J. Heikkila, O. Silve'n, and M. Pietikainen, "Face and eye detection for person authentication in mobile phones," in Distributed Smart Cameras, 2007. ICDSC'07. First ACM/IEEE International Conference on. IEEE, 2007, pp. 101-108.
- [3] V. Vaidehi, S. Vasuhi, R. Kayalvizhi, K. Mariammal, M. Raghuraman, V. Sundara, L. Meenakshi, V. Anupriyadharshini, and T. Thangamani, "Person authentication using face detection," in Proceedings of the World Congress on Engineering and Computer Science, 2008, pp. 22-24.
- [4] RSA Security Inc. RSA SecurID authenticators, 2006. Product Specification. Referenced 2006 at www.rsasecurity.com.
- [5] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity authentication system using fingerprints," Proceedings of the IEEE, vol. 85, no. 9, pp. 1365-1388, 1997.
- [6] v-GOSSPR 5.0 product description. Referenced 2006 at www.passlogix.com.
- [7] D. Currie, "Shedding some light on voice authentication," 2009.
- [8] F. Bergadano, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," ACM Transactions on Information and System Security (TISSEC), vol. 5, no. 4, pp. 367-397, 2002.
- [9] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell. Stronger password authentication using browser extensions. In P. McDaniel, editor, USENIX Security, pages 17-32, 2005.
- [10] V. Griffith and M. Jakobsson. Messin' with Texas: Deriving mothers maiden names using public records. In J. Ioannidis, A. D. Keromytis, and M. Yung, editors, Applied Cryptography and Network Security (ACNS), pages 91-103. Springer-Verlag, 2005. LNCS no. 3531
- [11] R. P. Guidorizzi, "Security: Active authentication," IT Professional, vol. 15, no. 4, pp. 4-7, 2013.
- [12] K. Ricanek, "The next biometric challenge: Medical alterations," Computer, vol. 46, no. 9, pp. 94-96, 2013.