ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 4, April 2019

Comparative Study of Multi-Factor Authentication Systems

Oladimeji Biodun S, Prof. Gloria Chukwudebe ,Dr. A.O Agbakwuru,Osodeke Charles Efe

PhD. Student Department of Computer Science, Imo State University Owerri Imo State Nigeria
Dean school of Computing and Information Technology, Federal University of Technology Owerri
Senior Lecturer Department of Computer Science, Imo State University Owerri
PhD. Student Department of Computer Science, Imo State University Owerri Imo State Nigeria

ABSTRACT: Multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction. The goal of MFA is to create a layered defence and make it more difficult for an unauthorized person to access a database or a computer system. Due to advancements and improvements in internet and communication systems, more people are relying on database to store their confidential information. The idea of Static passwords has been compromised just because most of the users try to use easily guessable, weak passwords or keywords from their personal information, which makes it easy for the attackers to guess their passwords in few combinations using Brute Force attack. Thus, the idea of using Multi-Factor Authentication has been introduced in the world of internet and database to harden the security of network and make it difficult for the attackers to crack systems. In this paper, we reviewed and analyzed various Multi-factor Authentication mechanisms.

KEYWORDS: Multifactor Authentication, Biometric, Verification, Token, MFA etc.

I. INTRODUCTION

As information technologies increase over time, more people are relying on database to store their confidential information. Earlier, the idea of Static passwords was being used but most of the users try to use easily guessable, weak passwords or keywords for their personal information, which makes it easy for the attackers to guess their passwords in few combinations using Brute Force attack [17]. Thus idea of using Multi-Factor Authentication has been introduced in the world of internet to harden the security of network and make it difficult for the attackers to crack systems. In this system, users are required to provide some extra information along with their username, login Id and password. One popular mechanism is using One-Time Passwords that are generated randomly and valid only for single login and even for short duration of time (usually 30 to 60 seconds).Today, people rely more on internet to store the confidential and important data. However, there is a risk that private data may be wiretapped. Therefore, it is necessary to authenticate users in order to keep this web data safe on cloud. Almost every client and server implement cryptographic techniques to encrypt this sensitive data, as well as verify entities at the other end of the connection [1].Thus if more confidential data is to be stored online, it is necessary that the network security should stay up to date with modern attacks. However, online users continue to use weak and easily guessable passwords like birth dates, partner names, children names etc. and they are typically only letters. Also, if the user sends the same password every session, an attacker can easily masquerade as a user, because the attacker may succeed in getting the user's password through internet. So, it is becoming clear that only passwordsare not sufficient means to protect the database accounts [2].Various authentication techniques are used today to harden the security of online data or information. Authentication also plays an important role when the transactions are related to money i.e. in financial transactions. One of the common authentication scheme used in financial services or transactions is using ahardware token like smartcards, credit/debit cards etc., but using these cards to authenticate the user identity is also not very sure in providing the security to the transactions. They are vulnerable to some frauds like swindlers (attackers) make use of skimmers that are devices used to capture data from the magnetic stripe of the card issued by the bank or any financial institution [11]. However, Multi- factor authentication is important in hardening the security of not only financial services but security of databases in other sectors [12]. The widespread adoption ofMFA would improve database security and help reduce fraud. MFA is not a new idea. Consider a Roman soldier guarding the Senate door and requiring senators to show a ring and speak a password. This is an example of two-factor authentication. MFA has been implemented in online systems for many years. Until recently, however, MFA has rarely been deployed successfully in verylarge-scale websites intended for

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 4, April 2019

communities such as consumers. In the light of the increasing password attacks, practices are beginning to change. In this article, we discuss multifactor authentication and different methods to implement MFA [7]

II. AUTHENTICATION ATTACKS

Attacks regarding authentication are those which target a web site's method of validating the identity of a user, service or application. These are of the following types.

a. Brute force attack
b. Insufficient authentication
c. Weak password recovery validation
d. Information verification
e. Password hints
f. Secret question and answer
g. Shoulder surfing attack
h. Phishing attack
i. Reconnaisance attack.

III. LITERATURE REVIEW

Uymatiao, Mariano Luis T., and William Emmanuel S. Yu [2] **(2014)** collectively developed a mobile TOTP scheme using TLS seed exchange and encrypted offline keystroke. The main objective of this research is to build a model which combine differentauthentication systems together, compare them based on some parameters and recommend which method is best at a particular time. It involves seed exchange to a software-based token through a login-protected Transport Layer Security (TLS/SSL) tunnel, encrypted local storage through a password-protected keystroke (BC UBER) with a strong key derivation function, and offline generation of one-time passwords through the TOTP algorithm. Authentication occurs through the use of a shared secret (the seed) to verify the correctness of the one-time password used to authenticate.

Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin and Jean-Pierre Seifert [3] (2014) have worked on SMS-based One Time Passwords that were introduced to counter phishing and other attacks against various internet services like in Banking Services. Now days, these OTPs are used for authentication and authorization in various other applications. But they are also prone to very heavy attacks especially to Smartphone Trojans. Thus, they collectively study the security architecture of SMS OTP systems and study attacks. Also, they proposed a mechanism to secure SMS OTPs against common attacks and specifically against Smartphone Trojans.

Michiel Appelman, Yannick Scheelen[4] (2012) have analysed on Google's 2-step verification login system. In which, Google asked for a verification code in combination with username and password. This unique verification code can be generated via three methods i.e. verification code can be sent via email or to the mobile phone through voice call or a text message. Another way is Google introduces a special Smartphone application that generates verification codes on users Smartphone that are valid only for 30 seconds of time.

Subashini K., and G. Sumithra [5] (2014) have worked on Secure multimodal mobile authentication using one time password. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords. Most systems today rely on static passwords to verify the user's identity. However, such passwords come with major management security concerns. Users tend to use easy-to-guess passwords, use the same password in multiple accounts, write the passwords or store them on their machines, etc.

Himika Parmar, Nancy Nainan, and Sumaiya Thaseen [8] (2012) have collectively analyse on phishing attack and provides the need to prevent such phishing attacks. Thus based upon all this proposes not to use passwords and to authenticate a user without a text password. They proposed an authentication service that is image based and eliminates the need of text passwords. In which a user will receive OTPthrough the instant messaging service available in internet after image authentication. The OTP then can be used by user to access their personal accounts. It integrates Image based authentication and HMAC based one time password to achieve high level of security in authenticating the user over the internet.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 4, April 2019

Nitin Mujal, R. Moona [11] (2009) described a secure and cost effective transaction model for financial services. As with the advent of the e-commerce, it has become much easier for the intruders or attackers to sit in non-descriptive location and quietly siphon away the money from the service users. Thus also the financial service outlets like Automated Teller Machine (ATM), Point of sale (PoS) terminal, online payments have also been an easy target. As the users are forced to trust a service outlet to be authentic but actually they can be spoofed and also a spoofed outlet can collect the account information of the users and can use the same to do financial transactions. These outlets are also very expensive to implement. Thus a secure and cost effective model has been proposed to overcome various securities and cost related issues of financial service models. It is cost effective such that financial services can also reach to the rural population and contribute to rural development.

M.M. Mohammed, M. Elsadig [26](2013) provided a multi-layer of multi factors authentication model for Online Banking Services. The security risks of internet banking have always been a matter of concern for the service providers as well as for the users. Various online environments like internet banking, electronic transactions and financial services have been analyzed to identify the characteristics and issues of existing authentication methods in order to present a user authentication level system model that is suitable for different online services. Multi-factor Authentication has been integrated with multi layer authentication techniques in order to produce a standard layered multi factor authentication model suitable for different online banking services suitable based on risk assessment criteria. The proposed model includes 5 levels such that each level contains one or combination of various authentication factors such as knowledge-based, possession based, or biometric based factors. The standard model is compared to multi layering guidelines and it shows improvement and fulfilment of authentication needs.

Hojin Seo, Huy Kang Kim [13] (2011) proposed a novel approach to prevent e-financial incidents by analyzing the input patterns of mobile banking users such as how long it takes by the user to input data into a mobile phone, and the normal finger pressure levels when user inputs through a touch screen. This can help in distinguishing the differences between the legitimate user's usage pattern and an attacker's usage pattern. This proposed method shows high accuracy and is effective in preventing e-financial incidents.

IV. AUTHENTICATION TECHNIQUES

A) SINGLE FACTOR/KNOWLEDGE-BASED AUTHENTICATION

This type of authentication technique consists of text based that uses passwords or Personal Identification Numbers (PINs) and graphic based authentication that uses graphics for authentication. Knowledge based authentication uses secret information [1]. When user provides some information to authenticate himself as a legitimate user, the system processes this information and suggests whether the user is legitimate or not. Knowledge based authentication is based on " Something You Know " assumption, in which the user types a password to login to a computer or enters his Personal Identification Number (PIN) to access his/her bank account from an ATM [15]. The classic form of single factor authentication is userID and Password. Where the user claims his/her identity by presenting a userID to the IT access control system. The system then checks the password for the claimed identity against its secure list of known identities and passwords. If the userID and Password pair, entered by the user, match the UserId and password stored in the IT access control system, then the user is judged to be authentic and given access to the system.

B) TWO-FACTIOR/TOKEN BASED AUTHENTICATION

This scheme uses some physical items called tokens such as smart cards, passports and physical keys. Authentication token or simply a token may be a physical device that an authorized user of computer is given to aid in authentication. Such a token may be physically connected or plugged into the client system. The term may refer to software token as well. Hardware tokens are typically small enough to be carried out in a pocket or purse and often are designed to attach to the user's keychain. Some may store cryptographic keys such as a digital signatures or biometric data such as a fingerprint. Other may include small keypads to allow the entry of a PIN [18].Token based authentication is based on " Something You Have " assumption, in which the user carries a wallet full of credentials (a driver's license, credit card, a university IDcard) to certify his/her identity (as a driver, as a credit worthy consumer, or as a student).

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 4, April 2019

This system uses both forms of authentication. i.e. it involves using " Something You Know"(i.e. a PIN) and " Something You Have"(i.e. a token). Most widely used forms of two factor authentication are.
(i) Automated Teller Machine(ATM) or Cashpoint Machine Card and PIN.
(ii) Access Control Token and PIN.
At an ATM, the user puts his/her Cashpoint/ATM card into the ATM and the ATM requests the user to enter his/her PIN. The information held on magnetic stripe of the card together with the PIN, encrypted in a secure block of data, is sent to the Bank's Central Authentication System, where the PIN entered by the user, is compared with the PIN held on file against the user's account number and details [11]. However, in this scheme, personally designed unique information is used as token. Each user is registered against that unique token which becomes his identifying label of the token. Stored information is presented to the system (e.g. ATM card) as well as PIN code to authenticate a user.

C) MULTI-FACTOR/BIOMETRIC-BASED AUTHENTICATION

Multi-factor authentication or Biometric based authentication involves using an access control token such as smart card, a PIN to access the smart card and a biometric value held in the central database. The card is entered into a reader, the PIN is entered, the biometric is read and encrypted under a cryptographic key held on the smart card. The userID read from the smart card together with the encrypted biometric are sent to the central database, where the biometric can be decrypted and compared with the value on the central access control system/database [24]. It is to be noted that the user's PIN is not sent to the central access control system but is checked locally by the smart card. Biometrics is the technologies that analyze human characteristics for automated personal authentication. In this scheme, behavioral characters (i.e. voice signature, gait of a human) as well as psychological characters (i.e. Fingerprint, Hand, Iris, Retina, Face) describing human characteristics are used for authentication. Biometric based authentication is used for both authentication as well as for identification. In short, this system uses some physical or behavioral traits of a human for authentication [7]

V. COMPARISON AMONG AUTHENTICATION TECHNIQUES

Knowledge based authentication has the following flaws.
(i) It is harder to remember passwords for a long time. With the passage of time, as the user's need, when user involves in more than one password based authentication systems, it becomes difficult for the user to distinguish among passwords used for different applications and to correctly remember those passwords. As time goes on, and by using many password based applications, forgetfulness of passwords is more probable to occur [28].
(ii) When a user may have more than one account with different passwords, the leakage of one or more of them are just possible.
(iii) A password that is written down can be seen by others and can be stolen.
(iv) Passwords invented by people are devised to be easy to remember- a word in dictionary or a loved one's name, a telephone number or a keyboard pattern (i.e. "asdf") or some combination thereof. Unfortunately, a password drawn from that significantly smaller space will be considered easier to guess. This form of authentication is relatively weak because, the same password is used over and over again, giving many opportunities for it to be illicitly captured[8]

Two factor/ Token based authentication is considered to be stronger than Single factor/Knowledge based authentication system, where user's confidence can be increased beyond what Single factor/Knowledge based authentication method provides by requiring that multiple independent method be used to authenticate individuals. This is known as multi factor authentication and the combination of two independent methods is known as Two Factor authentication. Here ignorance of the " Something You Know" (a PIN) makes it difficult for an attacker to benefit from stealing the " Something You Have"(a bank card). As knowledge based and token based authentication techniques are considered to be very effective, but for the reason that passwords and tokens are liable to be stolen, forgotten or shared with some un-authorized users due to which credibility reduces [23]. On the one hand, software tokens are flexible and less expensive than the hardware based solution. But on the other hand, software tokens have the following flaws.
(i) Software tokens are inherently vulnerable to maleware and keylogger attacks. They typically try to retrieve the user's credentials when they are typed in.
(ii) Software tokens are vulnerable to visual spoofing attacks.
(iii) They need installation of token driver on the system.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 4, April 2019

These problems are difficult to solve. However, keylogger attacks can be partially solved by displaying a keyboard on the client's screen having the user type in his credentials using this keyboard in a client-server architecture.Taking hardware token in consideration, carrying token all the times is inconvenient for users. Since biometric data cannot be readily changed, a user whose data has been leaked might be compelled to use different finger for authentication (e.g. in fingerprint authentication system) and so the possibility of reuse due to leakage of enrolled data is impossible as to impersonate the legitimate user for illegitimate purposes.[22]

VI. BIOMETRIC COMPARISON

As human present biometric data, a number of features extracted from that data are responsible for recognition process. The different biometric consists different biometric features, so this table representing biometrics with its features.

Biometrics	***Feature Description***
Iris	Texture of the iris such as freckles, coronas, strips, furrow, and crypts
Retinal	Vessel pattern in the retina of the eye as the blood vessels at the back of the eye
Finger Print	A friction Ridge curves-a raised portion, pore structure, indents and marks
Palm Print	Principal lines, wrinkles (secondary lines) and epidermal ridges
Hand Geometry	Estimation of length, width, thickness, shape and surface area of the hand.
Face	Distance of specific facial features (eyes, nose, mouth)
Ear	Dimension of the visible ear
Shape of X-Rayed Teeth	Shape of continuous teeth
DNA	DNA code can be extracted from blood, hair, skin cells and other bodily substances
Voice	Words, tone
Signature	It measures pressure, direction, timing, acceleration and the length of the strokes
Typing Rhythm	Keystroke time interval

Table 6.1: Summary of Biometric Features Used for Authentication

Each biometric technology has its merit and shortcoming; it is difficult to make a comparison directly. Researchers have identified several factors for it (Jain et al, 1999). In table 6.2, High, Medium, and Low are denoted by H, M and L respectively. We can define first six characteristics as essential characteristic of biometric entities and last four as system dependent characteristic of biometric entities [18].

Uniqueness: Each individual should have features but different with other. It means distinctive information content.
Permanence: The biometric should be sufficiently invariant over a certain period of time
Universality: The population coverage. Each individual should have the biometric feature.
Measurability: Measurable with simple technical equipment. It means simplicity of extraction.
Comparability: Simplicity of comparison between two templates as one is stored and second one is live template.
Collectability: How well can the identifiers be captured and quantified
Invasiveness: Introduction of instrument into a body part. For example DNA required blood for testing.
Performance: Accuracy, speed, security.
Acceptability: To which extent society is supporting.
Circumvention: The act of cheating someone.

Based on the above discussions, the researcher here under, built a table which summarizes Characteristics of Biometric Entities.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 4, April 2019

	Uniqueness	Permanence	Universality	Measurability	Comparability	Collect ability	Invasiveness	Performance	Acceptability	Circumvention
Iris	H	H	H	M	M	H	M	H	M	L
Retina	H	H	H	L	M	M	H	H	L	L
Fingerprint	H	H	M	H	M	M	M	M	H	M
Palm Print	H	H	M	H	M	M	M	M	H	M
Hand geometry	M	L	H	H	M	H	M	M	M	M
Face	M	M	H	M	L	H	L	L	H	H
Ear	M	M	H	M	L	M	L	L	M	L
Shape of X-rayed teeth	L	L	M	L	L	M	H	L	L	H
DNA	H	H	H	L	L	L	H	H	H	L
Voice	L	L	M	M	L	M	L	L	H	H
Signature	H	L	L	M	M	H	M	M	H	H
Typing Rhythm	L	L	L	L	L	M	M	L	L	M

Table 6.2: Summary of Characteristics of Biometric Entities

VII. RECOMMENDATION

From the tables above, we can conclude that combination of Biometrics with other authentication methods will go a long way in securing our databases. This is because Multi-Factor based authentication is considered to be the best and strongest form of authentication techniques.It is far better than traditional authentication systems like knowledge based and token based authentication systems because physiological or behavioral traits/ characteristics of a human cannot be easily stolen. Biometrics is the only form of authentication that assures the physical presence of the user. MFA is hereby recommended for safety of database and network systems.

VIII. CONCLUSION

In this paper, we analyzed and compared different authentication systems and conclude that Multi-Factor/Biometric-based authentication technique is convenient, safe and reliable. It consists of password/PIN, username and one or more of Biometrics. This system is pattern recognition system in which a person is recognized based on features derived from specific psychological or behavioral characteristics that the person possesses, which are harder to be theft or stolen.

REFERENCES

[1] Ramamohanarao, K., Gupta, K. K., Peng, T. and Leckie, C. " The Curse of Ease of Access to the Internet ", 2007.
[2] Oppliger, R., Hauser, R., Basin, D., Rodenhaeuser, A. and Kaiser, B." A Proof of Concept Implementation of SSL-TLS session Aware User Authentication (TLS-SA) "
[3] Newman, R. and Beyah, R. " A Permormance Analysis of Authentication using Covert Timing Channels "
[4] Schlaeger, C. and Pernul, G. " Authentication and Authorization infrastructures in b2c e-commerce"
[5] SHU-ren, Z. " Authentication based on Feature of hand-written signature", 2007
[6] Sakata, K., Maeda, T., Matsushita, M., Sasakawa, K. and Tamaki, H. " Fingerprint Authentication Based on Matching Scores with other Data", 2005
[7] ZHANG, Y. and ZHANG, D. " Authentication and Access Control in P2P Network", 2003
[8] Agostini, P.L. and Naggi, R. " Selecting Proper Authentication Mechanisms in Electronic Identity Management (EIDM): Open Issues"
[9] "Web Application Security Consortium: Threat Calssification", www.webappsec.org, version 1.00
[10] "The Web Security Report" www.websecurityreport.com , May 2007 Edition
[11] Noor, A. " Identity Protection Factor (IPF)"
[12] Mc Cune, J. M., Perrig, A., Reiter, M. K. "Seein-is-Believing: Using Camera Phones for Human Verifiable Authentication", November 2004.
[13] Misbahuddin, M., Premchand, P. and Govardhan, A. " A User Friendly Password Authenticated Key Agreement for Multi Server Environment", November 2009.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 4, April 2019

[14] HARBITTER, A. and MENASCE, D.A. ” A Methodology for Analyzing the Performance of Authentication Protocols”, November 2002
[15] Li, S., Zhou, J., Li, X. and Chen, K. ”An Authentication Protocol for Pervasive Computing”
[16] Bhargavan, K. and Corin, R.” Cryptographically Verified Implementations for TLS”, 2008
[17] TSENG, Y.M., YANG, C.C. AND HAUR SU, J.” Authentication and Billing Protocols for the Integration of WLAN and 3G Networks”, 2004
[18] Martinovic, I., Zdarsky, F. A., Bachorek, A., Jung, C. and Schmitt, J. B. ”Phishing in the Wireless: Implementation and Analysis”, 2007
[19] Halpert, B. J.” Authentication Interface Evaluation and Design for Mobile Devices”, 2005
[20] Abe T., Itoh, H. and Takahashi, K. ” Implementing Identity Provider on Mobile Phone”, November 2, 2007.
[21] Saxena, N., Uddin, Md. B. and Voris, J. ” Universal Device Pairing using an Auxiliary Device”, 2008
[22] Teranishi, I., Furukawa, J. and Sako, K. ” K-Times Anonymous Authentication(Extended Abstract)”
[23] Haque, M. M., Ahmad, S. I., Li, H. and Asif, K.M. ”An Authentication based Lightweight Device Discovery (ALDD) Model for Pervasive Computing Environment”, COMPSAC 2007
[24] Sharifi, M., Saberi, A., Vahidi, M. and Zorufi, M.” A Zero Knowledge Password Proof Mutual Authentication Technique Against Real-Time Phishing”, ICISS 2007, LNCS 4812.pp.254-258. 2007
[25] Khan, M. A. and Hassan, M. H.” Personal Authentication System using Hybrid Coding Technique”
[26] Qayum, A. and Latif, R.” Possible Attacks against GSM System Security”
[27] Haq, I. U. and Yahya, K. M.” Heterogeneous Networks
[28] Muliner, C., Borgaonkar, R., Stewin, P.,Seifert, J., “SMS-based One-Time Passwords: Attacks and Defense”, volume 7967,Pp. 150-159 Springer-Verlag Berlin Heidelberg 2013.