A critical insight into the identity authentication systems on smartphones

Tehseen Mehraj[1], Mir Aman Sheheryar[2], Sajaad Ahmed Lone[3], A. H. Mir[4]
[1,2]Department of Information & Technology, Central University of Kashmir, Srinagar, India
[3]Department of Computer Science & Engineering, Islamic University of Science & Technology, Awantipora, India
[4]Department of Electronics & Communication, National Institute of Technology, Srinagar, India

Article Info

Article history:

Received May 1, 2018
Revised Nov 17, 2018
Accepted Dec 15, 2018

Keywords:

Behavioural biometrics
Multimodal biometrics
Physiological biometrics
Smartphones
User authentication

ABSTRACT

The advancement of computing power on mobile devices and their popularity among people in performing sensitive data exchange is uncovering an urgent need for a highly secure solution than the existing ones. The need for such a security solution persists that should be able to thwart not only the contemporary threats but also offer continued support without bowing down to progression in technology. Though some security solutions have been contemplated, a lack of standardised or absolute security solution which can provide a feasible and secure solution to mobile phones exists. In this paper, a survey based on various biometric and non-biometric access management schemes has been performed. The copious solutions put forward by researchers so far were discovered to fail in traits like user adaptability and efficiency. Each of the works put forward by various researchers has been single-handedly contemplated followed by analysis. Ultimately, open problems and challenges were inferences from the survey conducted.

Corresponding Author:

Tehseen Mehraj,
Department of Information & Technology,
Central University of Kashmir,
Nowgam, 190015, Srinagar, India.
Email: TehseenBhat02@gmail.com

1. INTRODUCTION

Security and privacy on smart mobile devices have become the prime concerns due to their increasing popularity resulting in their high usage for accessing sensitive information and as a critical platform for business transactions [1]-[5]. With time, mobile devices are offering numerous novel functions of high quality which further increase the consumers' interest besides rising user's susceptibility to fraud [6]-[8]. Research has revealed that 82% of people in the age group 25-35 years along with 70% of household users make use of mobile phones to perform online banking [9]. Furthermore, it can be inferred from Figure 1 that millennials prefer the usage of a browser or app on mobile devices in comparison to other existing banking options [10]. Performing secure transaction and accessing such sensitive information demands security measures which must deliver strong security against impending threats as well as offer better user adoptability [2].

Security modernisation in the current era still finds the use of single-factor or password-based approach for access management across digital channels as they offer affordable deployment, easy revocation in the event of a compromise. Existing digital application services require a multitude of credentials in the form of PINs and passwords to be remembered by individual users resulting in higher proclivity of unsafe password selection by users for easy memorisation, which proves to be as one of the considerable concerns associated with it [11]. However, in the current era, rapid modernisation and development in computing technology, susceptibility to dictionary attacks [12], copious key-logger [13] and password hacking tools are available [14], [15], making password retrieval an easier task for intruders. Further, passwords can be shared, forgotten or observed thus forming an impractical authentication solution.

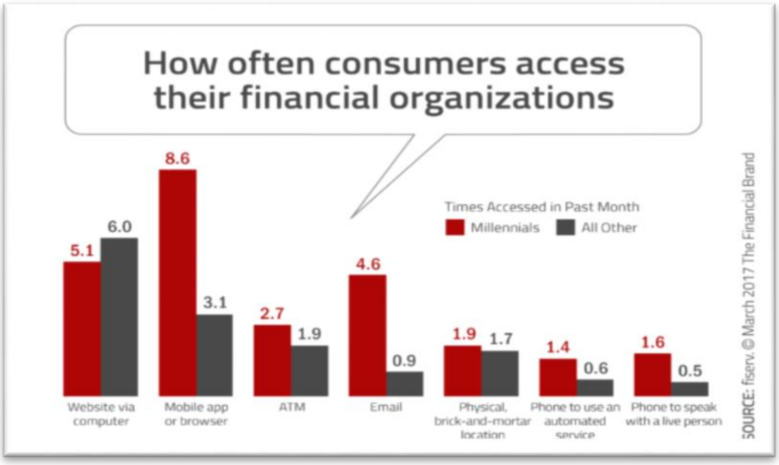

Figure 1. A preferred device for sensitive information access [Adopted from [10]]

Various schemes replacing complex passwords with hardware tokens, chip modules and smart cards have been introduced [16]-[18] which provide higher degree of security but lack user ergonomics, prove inconsistent, can be lost, duplicated, stolen, expensive and unmanageable, therefore hampering their adoptability [19], [20]. Also, there exist security schemes like [21], [22] which failed to operate on limited resource devices such as smart mobile phones that are exceedingly used for sensitive information exchange thereby making them extremely vulnerable [1], [23]. Furthermore, a variety of facilities exist like cloud technology, which aim at offering many services to its customers. But, the data sharing approach utilized by the cloud technology uncovers many flaws and hence results in its susceptibility to numerous attacks [24]-[27].

User adoptability is a prime concern for digital vendors. Currently, users desire for convenient and simple experiences. The confluence of user adoptability and security challenges developed a momentous rise in biometric security solutions. According to a report by the World Economic Forum (WEF) [28], biometrics can provide a potential solution offering security and user conveniences, particularly in financial services. Nevertheless, there exist multiple points where biometric systems can be breached [29]. Some threats have been addressed by researchers in [30], and still, biometric systems remain susceptible to spoofing and smudge attacks. Even if there exist systems offering protection to biometric templates by revoking biometric credentials, such solutions have limited availability, and underdeveloped standards exist to evaluate such solutions. Unfortunately, biometric systems appear to be highly susceptible to replay attacks [19]. Hence, security solutions based on biometrics alone offer weaker security even if they provide high user adoptability.

The ultimate goal of the paper is to contemplate numerous security solutions in access management offered in the past. The remaining paper is organised as: Section 2 is entirely devoted to a detailed survey of biometric authentication and non-biometric authentication. Section 3 emphasises the potential challenges and open issues as revealed by the research work reviewed. Finally, Section 4 concludes the paper with clinching remarks.

2. BACKGROUND WORK

This section involves the detailed study of numerous security solutions prevalent in the field of secure user authentication. The research further involves security schemes sectioned into two categories: biometric-based and non-biometric based schemes.

2.1. Biometric-based Systems

A large number of security mechanisms are based on biometrics which includes both the behavioural and physical/physiological characteristics of a person. Some security solutions based on biometrics have been reviewed as under.

2.1.1 Authentication based on Physiological Characteristics

The physical features or characteristics of an individual form the basis for physiological based authentication biometric schemes. Face, retina/iris, palm/hand geometry, fingerprint form the physical features which are relatively unchanged with the passage of time.

a. Fingerprint recognition

Fingerprint authentication is a hot research area for authentication on mobile phones. The authentication schemes based on fingerprints have been already implemented on mobile phones and can be seen as a user adoptable solution for identifying an individuals' identity. In [31], a fingerprint authentication scheme has been proposed, which is being implemented as an Android application and running on actual mobile devices. Three authentication algorithms for fingerprint processing have been introduced each of which is evaluated according to their accuracy rate and speed. While in [32], a secure, low-cost, and robust fingerprint authentication scheme on mobile phone devices has been proposed. The system has been implemented using an OpenCV (Computer Vision) library and Android. The RGB matching algorithm has been utilised. These fingerprint-based authentication schemes appear cheap, easy to use without consuming much battery power on resource-constrained mobile phone devices. Nevertheless, the lack of hardware on mobile devices capable of complete acquisition of entire fingerprint along with incompatibility of fingerprint matching algorithms in the presence of dirt or cuts, makes security solutions based on fingerprint appear as a weak contender in the field of forming a secure and adoptable user solution.

b. Face recognition

The face recognition-based authentication schemes involve the use of facial features obtained from video frames or digital image for verification or identification of an individual. The face recognition also forms a potential research area in the field of mobile authentication. The authors in [33] have introduced an efficient open face recognition system on the Android platform. The proposed system implements face, eye detection, LBP (Local Binary Pattern) for feature extraction, pre-processing for Region of Interest (ROI), feature dimensionality reduction based on Linear Discriminant Analysis (LDA) referred to as Fisherface and Principal Component Analysis (PCA) referred to as Eigenface, and Euclidean distance as a minimum distance classifier. The experimental results have attained 96.0% accuracy in face recognition by implementing the Fisherface algorithm and 93.8% accuracy with the Eigenface algorithm. Face forms the leading biometric trait to be considered on mobile phone devices [6], [34] in comparison to fingerprint and iris. Even though the authentication scheme is mostly acceptable by mobile phone users still there exists issues regarding the performance of the security solution regarding certain conditions like face angles, poor lighting conditions, and diverse expressions.

2.1.2 Authentication based on Behavioural Characteristics

Keystroke dynamics or typing rhythm, signature, voice, gait and behaviour profiling form the behavioural traits for the authentication systems based on behavioural biometrics.

a. Behaviour Profiling

How the individuals interact with their mobile devices to avail numerous services form the basis of identification in such techniques; examples include applications usage, location etc. In [35], behavioural biometrics data has been collected and analysed from different Android mobile devices to provide a solution for active authentication aimed to verify the identity of a legitimate user continuously. Four biometric parameters: i) text entered through a soft keyboard, ii) device's physical location as per GPS (outdoors) or Wi-Fi (indoors) iii) used applications, iv) visited websites have been considered. A classifier has been implemented and tested for every modality, and these classifiers have been organised in a parallel binary-decision fusion design. Further, A novel access control mechanism based on particular user context has been implemented in [36], which dynamically grants or revokes privileges to users. The authors have worked on the Android restriction techniques. The context implementation is capable of differentiating between various closely located sub-areas within the same location. The setting in this paper has been defined in terms of time and location, the location is specified in terms of visible Wi-Fi access points together with their signal strengths, in addition to cellular triangulation and GPS as per availability. Even though, such security schemes seem to be feasible on mobile phone devices. Nevertheless, performance inconsistency resulting from unexpected interaction by users' is the primary weakness experienced by such systems.

b. Keystroke Dynamics

An individuals' typing rhythm and manner are being utilised by this approach. Keystroke dynamics found their place on mobile phone devices the long time ago. The authors in [37] aim to improve the existing systems based on the keystroke dynamics authentication to enhance the security of smartphones by increasing user ergonomics, allowing a user to change the PIN without Keystroke-Dynamics-Based-Authentication (KDA) system to be retrained. The system can distinguish between an imposter and a legitimate user, notably when the users change their passwords. Overall in contrast to physiological authentication-based schemes, behavioural biometrics offer a solution to attain transparent active authentication without any additional hardware requirements. Thus, forming a cheaper solution as compared to physiological authentication schemes. From the survey conducted, the physiological authentication schemes emerge to be vulnerable to replay attacks, where the intruder can exploit the images of the physical features by replaying them later. Moreover, in the case of behavioural authentication schemes compulsion for enhancing the security exists. Several approaches can be adopted to thwart such susceptibilities at the same time strengthen security.

In [38], a framework combining the permuted sequence forming a behavioural fingerprint with the physiological fingerprint to bring together the reliability and accuracy of each has been proposed. Behavioural fingerprint acts as a firewall which delays or blocks unauthorised access to the system in case the user's fingerprint was compromised. The proposed behavioural fingerprint framework identifies the root of a fingerprint and its fingerprint sequence. It is more efficient than the multimodal biometric approaches without requiring any additional hardware. Further, in [39], a biometric multimodal system has been proposed, which utilises biometric characteristics like iris, face and periocular for access control. Multi-modal fusion has been performed using iris, face and periocular data and weighted fusion approach have been utilised for fusing comparison score of distinctive feature extraction schemes. This method explores numerous score-level fusion to use the complementary information from the three modalities. Table 1 has formulated the various contributions and allied weaknesses.

2.2. Non-Biometric-based Systems

Other than biometric-based security solutions, researches have been directed on security schemes centred on modified passwords, social networks, location information, public key cryptography, smart devices and permission control on mobile devices.

In [41], the authors have put forward a novel method to strengthen the access control mechanism based on passwords. The level of difficulty in breaching the password is increased by adding free random text which further makes the system immune against pre-computed rainbow and dictionary attacks in addition to shoulder surfing and replay attacks. In [42], a suitable and effective scheme for LAN has been proposed, which solves complex issues such as authentication, management, and authorisation, thus simplifying the various network security measures and policies internal to the network. A novel access control scheme has been introduced which makes use of User-Access-Control-Table (UAT) and USB in Local-Area-Network (LAN). It provides privilege management in LAN at smaller costs.

A novel Wi-Fi authentication mechanism has been presented in [43] implementing social networks as the criteria for providing more user-friendliness and secure authentication. The system abandons the centralized approach which entrenches social networks for Wi-Fi authentication instead the system has introduced a decentralized approach EAP-Soc-TLS, for authorization and authentication of Wi-Fi access points and numerous additional devices, thus providing a much better solution in terms of scalability than the conventional centralized approaches which face single point failure problems and raise privacy concerns. A practical and secure authentication mechanism founded on smart cards has been proposed in [21]. The proposed system delivers protection against various susceptibilities while at the same time improving existing security schemes. The mechanism permits users to select their passwords conveniently with the privilege of modifying it offline. The smart card doesn't hold any crucial information, thus safeguarding against stolen user smartcard risk.

In [44], the authors proposed a bilateral recurring authentication method namely Zero-Effort-Bilateral-Recurring-Authentication (ZEBRA). The system utilises a hardware token in the form of a bracelet which has built-in radio, gyroscope, and accelerometer to provide continued authentication. The signals sent from the bracelet worn on the user's wrist are correlated with the terminal's operations to confirm the continued presence of the user if the two movements correspond according to a few coarse-grained actions. In [45], location information has been used as a modality for user authentication. The paper has presented a novel algorithm as Hidden Markov Model accompanied with marginal smoothing method for location authentication. The proposed scheme outperforms other methods regarding the Equal Error Rate (EER) of 20.73%. However, the requirement to possess information related to genuine user routine leaves the arrangement vulnerable to attacks plus the scheme should consider fusion with other modalities to achieve better performance. In [46], sensitive data leakage prevention mechanism for Android mobile devices has been proposed. Malicious applications are detected which are responsible for the leakage of critical data utilising J8-classification algorithm. The scheme achieved 98.6% accuracy in detection of benign and malicious apps. Table 2 has framed the pros and cons of numerous non-biometric schemes discussed earlier as follows:

Table 1. Review of biometric schemes

Author	Contribution	Limitations
(Andreeva et al., 2012) [21]	Proposes Continuous access control mechanism exploiting heart sounds.	• Prolonged authentication can't be expected by the system as the heart sound conditions of humans do not remain the same with time. • A system is established on BAN engages complex construction and several sensors, hindering adequate user adoptability. • Risk of intrusion exists during data transmission.
(Kavita et al., 2013) [32]	Proposed a secure, low cost, and robust biometric authentication scheme on mobile phones.	• Lacks in obtaining crucial features as low definition camera is considered. • Factors like background, lighting, and orientation need to be considered hindering user adoptability. • Performance analysis regarding the accuracy of the system and the resources consumed on mobile devices has not been done. • Higher false acceptance rate while contemplated smaller data-set.
(Conti et al., 2014) [31]	Presented a biometric authentication scheme as an Android application in real-time mobile devices.	• Lacks in a complete acquisition of the fingerprint thus reducing recognition rate and hence user adaptability.
(Darwaish et al., 2014) [2]	Introduced offline face-recognition mechanism on mobile devices.	• Comparison with various available state-of-art algorithms is desired.
(Tsai et al., 2014) [37]	Proposed an improved keystroke dynamics authentication mechanism.	• Discards the retraining phase. • Authentication failure is not being handled appropriately leading to reduced user ergonomics. • Susceptible to smudge attacks, accelerometer, timing attacks, keystroke inference attacks.
(Daniel et al., 2015) [19]	Proposed a mechanism to thwart reply attack aiming face recognition on smart devices.	• Various factors such as environmental conditions, and camera settings etc., are not considered. • Implementation on computer systems only.
(Fridman et al., 2015) [33]	Designed an active authentication mechanism on mobile devices.	• Utilized GPS as Location classifier, which fails to deliver precise authentication.
(Javier et al., 2015) [40]	Designed a novel software-based fake detection technique thwarting fraudulent access to numerous biometric systems.	• Implementation is performed on computer systems and not on mobile devices. • The state-of-art algorithms not specified.
(Jiawei et al., 2015) [33]	Presented a face recognition system titled XFace aimed for the Android platform.	• The small dataset has been contemplated.
(Kiran et al., 2015) [39]	Proposed a biometric multi-modal system incorporating biometric characteristics like iris, face and periocular for access control.	• Different distances to a camera, camera properties, face angles and expressions have not been contemplated. • Requires high definition camera and incurs a high computation cost. • Performance analysis regarding the limited resources of a smartphone such as memory and battery consumption has not been done.
(Maria et al., 2015) [6]	Introduced a biometric multimodal security mechanism on mobile devices.	• Acquisition under extremely controlled situations to acquire iris hindering user adoptability.
(Meng et al., 2015) [22]	A novel authentication framework implementing multi-modal biometric user authentication.	• Have considered touch screen dynamic demanding high performance and accuracy, which is difficult to achieve on mobile devices. • Susceptible to touch logger detection attacks.
(Shebaro et al., 2015) [36]	Presented a novel access control mechanism dynamically granting or revoking privileges to users.	• 16% of false positives have been found. • Suffers from memory overhead.
(Yang et al., 2015) [11]	Addressed two possible complications related to implicit authentication.	• Performance on smartphones on which the implicit authentication is widely implemented is not shown. • The dataset with weak modalities has been contemplated. • Vulnerable to mimic attacks, synthetic attack, sensor-sniffing attacks.
(Teo et al., 2017) [38]	Designed a new framework combining the permuted sequence forming a behavioural fingerprint with the physiological fingerprint.	• Usability needs to be taken into consideration as the sequence must be memorised by the user. • Additional hardware requirements as the primary sensor for fingerprint acquisition is desired.

Table 2. Review of non-biometric schemes

Author	Contribution	Limitations
(Zhang et al., 2010) [42]	A novel scheme LAN's access control centred on UAT and USB in LAN.	• USB as additional hardware. • Lacks in maintaining user ergonomics.
(Aboud et al., 2014) [17]	Presented an effective and secure authentication mechanism founded upon smart cards.	• Usage of an additional token shall prove expensive for service provider and cause difficulty to users.
(Durmus et al., 2014) [43]	Presented a novel Wi-Fi authentication mechanism implementing social networks as the criteria for providing a more user-friendly and secure authentication mechanism.	• Demands profile of owner on the social network. • Privacy concerns exist as complete friendship information is anticipated to be open for all. • Security concerns arise as worn-out caches used to perform offline authentication. • Ownership related issues are not contemplated.
(Shrirang et al., 2014) [44]	Proposed an active authentication scheme ZEBRA.	• Lacks in user adoptability. • Bracelet as an additional hardware requirement.
(Upal and Rama., 2016) [45]	Presented an active authentication system employing trace history.	• A requirement to have information related to genuine user routine leaves the arrangement vulnerable to attacks.
(Chowdhury et al., 2017) [41]	Forwarded a novel technique to strengthen the access control mechanism based on passwords.	• An authentication failure occurs from the passwords cached in various newest browsers. • User adoptability is not up to the mark as more things need to be remembered by the user, unlike the existing system. • Susceptible to keystroke attack.
(Yavuz et al., 2017) [46]	Presented a sensitive data leakage prevention mechanism.	• Small data-set has been contemplated.

3. OPEN ISSUES

After presenting the study of various security schemes available in access management as complemented by researchers, it can be concluded that there still happen to be loopholes in the offered security solutions. The challenges identified range from security vulnerability to computational complexity to user adoptability. Conclusively, the progressive review conducted will end with the following open issues:

a) Reduced user adoptability persists due to extra hardware requirements existing in the form of smart cards, specially featured hardware [13], [21], [40], [38], [43].

b) Prominent processing power and execution time subsist [21], [22], resulting in subsequent incompatibility to operate on generic mobile devices.

c) Databases used to train the biometric recognition schemes are far from the data that exists in the real world [33], [39], [40], [46], thus, offering reduced accuracy when such solutions are exposed to realistic data.

d) Behavioural biometrics ease a user in terms of user adoptability [11], [33], [36]; however, the accuracy of such systems drops abruptly when user behaves inversely.

e) Inability to protect against various threats [11], [22], [37], [42], [44], which smart mobile devices are susceptible to, like touch-logger/key-logger, liveness detection, mimic attacks, etc.

f) Choosing a suitable set of biometric characteristics is a critical challenge in case of biometric authentication particularly when considering multi-modal biometric security schemes [13], [22], [33], [39], [46]. Designing reliable authentication systems capable of selecting or deciding on an appropriate biometric set exists.

g) Performance analysis on the mobile platform has not been conducted yet [11], [36], [39] [40]-[44] resulting in a lack of benchmark. Thus, impeding the implementation of such schemes on generic mobile devices.

4. CONCLUSION

In this paper, an appraisal of prior authentication techniques centred on biometric and non-biometric approaches have been performed. The substantial contributions and drawbacks of the respective security solutions have been particularised explicitly. All the authentication schemes reviewed were found to be lacking in one context or the other. The need for such a security solution persists that should be able to thwart not only the contemporary threats but also offer continued support without bowing down to progression in technology. At the same time, user ergonomics should not be ignored and treated with equal importance. Besides, open problems and challenges need to be deliberated while designing such systems with the hope to drive further research in the area.

REFERENCES

[1] Islam SH, Biswas GP. “A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem”. *Journal of Systems and Software* 1;84(11):1892-8. Nov. 2011.

[2] Darwaish SF, Moradian E, Rahmani T, Knauer M. “Biometric identification on Android smartphones”. *Procedia Computer Science*. 35: 832-841.1. Jan. 2014.

[3] Khan BUI, Olanrewaju RF, Baba AM, Langoo AA, Assad S. “A compendious study of online payment systems: Past developments, present impact, and future considerations”. *International Journal of Advanced Computer Science and Applications*; 8(5): 256-271. 1 May 2017.

[4] Pampori BR, Mehraj T, Khan BUI, Baba AM, Najar ZA. “Securely eradicating cellular dependency for e-banking applications. *International Journal of Advanced Computer Science and Applications*.385-398, 2018.

[5] Hussain S, Khan BUI, Anwar F, Olanrewaju RF. “Secure annihilation of out-of-band authorization for online transactions”. *Indian Journal of Science and Technology*.11(5): 1-9, 11 Feb 2018.

[6] De Marsico M, Galdi C, Nappi M, Riccio D. Firme: “Face and iris recognition for mobile engagement”. *Image and Vision Computing*.32(12): 1161-1172, 1 Dec 2014.

[7] Masihuddin M, Khan BUI, Mattoo MM, Olanrewaju RF. “A survey on e-payment systems: elements, adoption, architecture, challenges and security concepts”. *Indian Journal of Science and Technology*.10(20) 1-19, 25 May 2017

[8] Olanrewaju RF, Khan BUI, Mattoo MM, Anwar F, Nordin AN, Mir RN. “Securing electronic transactions via payment gateways–a systematic review”. *International Journal of Internet Technology and Secured Transactions*.7(3): 245-269, 2017.

[9] Buriro A, Gupta S, Crispo B. “Evaluation of Motion-based Touch-typing Biometrics for online Banking”. *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)* : 1-5, 2017.

[10] Marous J. “Millennials Are Leading the Digital Banking Revolution [Internet]”. The Financial Brand 2017. Available from: https://thefinancialbrand.com/64369/millennials-mobile-banking-digital-engagement-trends/. 30 April 2018

[11] Yang Y, Sun JS, Zhang C, Li P. Retraining and dynamic privilege for implicit authentication systems. *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). IEEE*: 163-171, 19 Oct 2015.

[12] Narayanan A, Shmatikov V. *“*Fast dictionary attacks on passwords using time-space tradeoff”. *Proceedings of the 12th ACM conference on Computer and communications security. ACM*: 364-372. 7 Nov 2017.

[13] Online fraud happened hacking my icici bank credit card [Internet]. 2013 [cited 30 April 2018]. Available from: http://www.grahakseva.com/complaints/130310/online-fraud-happened-hacking-my-icici-bank-credit-card

[14] Goel CK, Arya G. Hacking of passwords in windows environment. *International Journal of Computer Science & Communication Networks*.2(3): 430-435, 2012.

[15] Adhikary N, Shrivastava R, Kumar A, Verma SK, Bag M, Singh V. “Battering keyloggers and screen recording software by fabricating passwords”. *International Journal of Computer Network and Information Security*. 1; 4(5): 13-21, Jun 2012.

[16] Lee WH, Lee R. “Implicit sensor-based authentication of smartphone users with smartwatch”. *Proceedings of the Hardware and Architectural Support for Security and Privacy.* ACM. 2016

[17] Aboud SJ. “Secure Password Authentication System Using Smart Card”. *Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* 2014; 3(1): 75-79.

[18] Jeong J, Chung MY, Choo H. “Integrated OTP-based user authentication and access control scheme in home networks”. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences. Springer,* Berlin, Heidelberg. Waikoloa, HI, 2008; 1-7.

[19] Smith DF, Wiliem A, Lovell BC. “Face recognition on consumer devices: Reflections on replay attacks”. *IEEE Transactions on Information Forensics and Security,* 2015; 10(4): 736-745.

[20] O'Gorman L. “Comparing passwords, tokens, and biometrics for user authentication”, *Proceedings of the IEEE*, 2003; 91(12): 2021-2040.

[21] Andreeva E. “Secret sharing in continuous access control system, using heart sounds”. *2012 XIII International Symposium on Problems of Redundancy in Information and Control Systems (RED), IEEE*, 5: 5-6, Sep 2012

[22] Meng W, Wong DS, Furnell S, Zhou J. “Surveying the development of biometric user authentication on mobile phones”, *IEEE Communications Surveys & Tutorials*, 17(3): 1268-1293, 1 Jul 2015.

[23] Mehraj T, Rasool B, Khan BUI, Baba A, Lone P. “Contemplation of Effective Security Measures in Access Management from Adoptability Perspective”. *International Journal of Advanced Computer Science and Applications*. 2015; 6(8): 188-201.

[24] Olanrewaju RF, Khan BUI, Mattoo MM, Anwar F, Nordin AN, Mir RN, Noor Z. “Adoption of Cloud Computing in Higher Learning Institutions: A Systematic Review”. *Indian Journal of Science and Technology*. 2017; 10(36): 1-19.

[25] Olanrewaju RF, Khan BUI, Baba A, Mir RN, Lone SA. “*RFDA:* Reliable framework for data administration based on split-merge policy”. *SAI Computing Conference (SAI). IEEE*. 2016 Jul 13: 545-552.

[26] Khan BU, Baba AM, Olanrewaju RF, Lone SA, Zulkurnain NF. “SSM: Secure-Split-Merge data distribution in cloud infrastructure”. *2015 IEEE Conference on Open Systems (ICOS). IEEE*. 2015 Aug 24: 40-45.

[27] Mir MS, Suhaimi B, Adam M, Khan BUI, Mattoo MMUI, Olanrewaju RF. “Critical security challenges in cloud computing environment: an appraisal”. *Journal of Theoretical & Applied Information Technology*. 2017 May 31; 95(10): 2234-2248.

[28] McWaters R. “A Blueprint for Digital Identity”. *World Economic Forum*. 2016.

[29] Ratha NK, Connell JH, Bolle RM. “An analysis of minutiae matching strength”. *3rd International Conference on Audio-and Video-Based Biometric Person Authentication (AVBPA). Springer,* Berlin, Heidelberg. 2001 Jun 6: 223-228.

[30] Määttä J, Hadid A, Pietikäinen M. “Face spoofing detection from single images using micro-texture analysis”. *2011 International Joint Conference on Biometrics (IJCB). IEEE.* 2011; Oct 11: 1-7.

[31] Conti V, Collotta M, Pau G, Vitabile S. “Usability Analysis of a Novel Biometric Authentication Approach for Android-Based Mobile Devices”. *Journal of Telecommunications and Information Technology*. 2014 Oct 1; (4): 34-43.

[32] Rathi K, Sawarkar S. “Finger Print Matching Algorithm for Android”. *International Journal of Engineering Research & Technology (IJERT).* 2013; 2(10): 3819-3823.

[33] Hu J, Peng L, Zheng L. “XFace: A Face Recognition System for Android Mobile Phones”. *2015 IEEE 3rd International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), IEEE,* 2015 Aug 19: 13-18.

[34] Lovisotto G, Malik R, Sluganovic I, Roeschlin M, Trueman P, Martinovic I. *Mobile biometrics in financial services: A five factor framework*. Technical Report CS-RR-17-03, Oxford University. 2017.

[35] Fridman L, Weber S, Greenstadt R, Kam M. “Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location”. *IEEE Systems Journal.* 2017 Jun; 11(2); 513-521.

[36] Shebaro B, Oluwatimi O, Bertino E. “Context-based access control systems for mobile devices”. *IEEE Transactions on Dependable and Secure Computing*. 2015 Mar 1; 12(2) :150-63.

[37] Tsai CJ, Peng CC, Chiang ML, Chang TY, Tsai WJ, Wu HS. “Work in progress: a new approach of changeable password for keystroke dynamics authentication system on smart phones”. *2014 9th International Conference on Communications and Networking in China (CHINACOM). IEEE.* 2014 Aug 14; 353-356.

[38] Teo CC, Neo HF. “Proceedings of the 9th International Conference on Bioinformatics and Biomedical Technology. *Behavioral Fingerprint Authentication: The Next Future*. ACM. 2017 May 14: 1-5.

[39] Raja KB, Raghavendra R, Stokkenes M, Busch C. “Multi-modal authentication system for smartphones using face, iris and periocular”. *2015 International Conference on Biometrics (ICB). IEEE.* 2015 May 19; 143-150.

[40] Galbally J, Marcel S, Fierrez J. “Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition”. *IEEE transactions on image processing*. 2014 Feb; 23(2): 710-724.

[41] Chowdhury EW, Rahman MS, Al Islam AA, Rahman MS. “Salty Secret: Let us secretly salt the secret”. *2017 International Conference on Networking, Systems and Security (NSysS). IEEE*. 2017 Jan 5; 115-123.

[42] Zhang P, Pei Y. “A Technology of User Access-Control Table and Identity Authentication Based on USB in LAN”. *2010 International Conference on Biomedical Engineering and Computer Science (ICBECS). IEEE*. 2010; 1-3.

[43] Durmus Y, Langendoen K, “Wifi authentication through social networks—A decentralized and context-aware approach”, *2014 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE,* 2014 Mar 24: 532-538.

[44] Mare S, Markham AM, Cornelius C, Peterson R, Kotz D. “Zebra: Zero-effort bilateral recurring authentication”, *2014 IEEE Symposium on Security and Privacy (SP), IEEE,* 2014 May 18; 705-720.

[45] Mahbub U, Chellappa R. PATH, “person authentication using trace histories”, *IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE,* 2016 Oct 20; 1-8.

[46] Canbay Y, Ulker M, Sagiroglu S. “Detection of mobile applications leaking sensitive data”, *2017 5th International Symposium on Digital Forensic and Security (ISDFS). IEEE.* 2017 Apr 26; 1-5.