A Study on Enhancing Mobile Banking Services using Location based Authentication

K. Krishna Prasad[1] & P. S. Aithal[2]

[1]Srinivas Institute of Management Studies, Pandeshwar, Mangalore.

[1]Research Scholar, Rayalaseema University, Kurnool, India.

[2]Department of Computer Science, Srinivas Institute of Management Studies, Pandeshwar, Mangalore, India

E-Mail: karanikrishna@gmail.com

Type of the Paper: Research Article
Type of Review: Peer Reviewed.
Indexed in: OpenAIRE.
DOI: http://doi.org/10.5281/zenodo.583230.
Google Scholar Citation: IJMTS

How to Cite this Paper:
Krishna Prasad, K. and Aithal, P. S. (2016). A Study on Enhancing Mobile Banking Services using Location based Authentication. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 1(1), 48-58.
DOI: http://doi.org/10.5281/zenodo.583230.

International Journal of Management, Technology, and Social Sciences (IJMTS)
A Refereed International Journal of Srinivas University, India.

A Study on Enhancing Mobile Banking Services using Location based Authentication

K. Krishna Prasad[1] & P. S. Aithal[2]
[1]Srinivas Institute of Management Studies, Pandeshwar, Mangalore.
[1]Research Scholar, Rayalaseema University, Kurnool, India.
[2]Department of Computer Science, Srinivas Institute of Management Studies, Pandeshwar, Mangalore, India
E-Mail: karanikrishna@gmail.com

ABSTRACT

Every now and then mobile users are increasing in exponentially all over the world, which leads to the growth of mobile-enabled services like mobile banking. The smart phone now available in the market having the ability to do all the functions that people can do olden days using their personal computers. The introduction of mobile communication technology modernization, innovation and globalization are increasingly driving the banking services to become ubiquitous, personalized, convenience, disseminative and secured. Mobile Banking Authentication has evolved over time to include several parameters such as Biometric, Location, Context, History, Profile etc. In this paper, we discuss new mobile banking services like Digital deposit apps, advanced bill payment apps, and Electronic meeting for mini loan services and Mobile payment apps. We can provide higher security for these new services through an intelligent multi-modal Authentication with Location Awareness. Here the location, where the mobile banking transaction has been executed is captured giving the additional option for a Bank to verify if the transaction has been executed normally or if the parameters are at variance with normal practice. If the Location happens to be very in a different country, an additional verification process can be introduced adding to the entropy of Authentication. If the Location happens to be a Bank Branch or an ATM, where there is a proper iBeacon or GPS providing additional information about identification, then in such a situation the Authentication can be further simplified based on the type of transaction. In this paper, we discuss in detail location based authentication and how these can be effectively applied in enhancing the mobile banking services.

Keywords: Location Based Authentication, iBeacon, GPS, Biometric, Digital deposit apps.

1. INTRODUCTION :

The drastic development of mobile telecommunication system leads to increased mobile phone users all over the globe. The smart phone style, functions, and facilities are continuously changing, which leads to drastic development and incorporation of innovative services in mobile banking services. Mobile Banking (m-banking) is considered to be one of latest and widest online banking services to its customers. Even though Automated Teller Machine (ATM), Telephone, and Internet banking are banking services outside the banks and offers successful delivery channels for traditional banking products, mobile banking is the another innovative distribution channels established by the banks with more emphasis on ubiquitous nature of service availability [1]. Researchers used various terms for mobile banking, Amin et al., (2006) referred mobile banking as pocket banking, Ivatury and Mas, (2008) as branchless banking, while Donner and Tellez, (2008) called m-payments, m-transfers, m-finance and Liu et al., (2009) named as m-banking [3-6].

Even though mobile personal devices, typically with a fixed display and keyboard, are well-positioned to provide a practical solution for reducing fraud, security is considered to be one of the biggest hindrance

or challenges for the widespread usage of mobile banking services [7-9]. In order to improve the security of mobile banking transactions lot of research works are carried out. Technology is in for front to improve mobile transaction security. In recent years lot of research work has been carried out on biometric identity. Biometrics is unique metrics related to human characteristics, which can be used for identification or authentication purpose as individual's claimed identity [10].

Mobile Banking Authentication has evolved over time to include several parameters such as Biometric, Location, Context, History, Profile etc. Some biometric authentication methods even consider keystroke dynamics and typing patterns are the implicit and continuous observation of the user behavior makes authentication based on the observations [11-13]. Herzberg, A., (2003) argue that mobile personal devices effectively used to perform secure banking and utility bill payments. He believes that mobile personal devices with some biometric mechanism will play an important role in many financial transactions including micropayments [14].

In this paper, we discuss different mobile banking services, which include Digital deposit Photo bill payment, Electronic meeting for mini loan services and Mobile payment. We discuss how to provide higher security for these services through an intelligent multi-modal Authentication with Location Awareness. Here the location, where the mobile banking transaction has been executed is captured giving the additional option for a Bank to verify if the transaction has been executed normally or if the parameters are at variance with normal practice. If the transaction carries out in very remote or in different countries, then extra security parameter is considered. In this paper, we discuss in detail location based authentication with its merits and demerits and how this can be effectively applied in mobile banking security.

2. Biometric Authentication :

Biometrics is unique metrics related to human characteristics, which can be used for identification or authentication purpose as individual's claimed identity. Every human being can be recognized through observation of particular characteristics, which mainly involves different types as visual biometrics, chemical biometrics, auditory biometrics, behavioral biometrics, Olfactory or odour biometrics and spatial biometrics. There is few research work carried out around the world in the context of authentication security purposes. Aloul, F. et.al., (2009) explains that two-factor authorization gives more security for mobile based financial transactions other than usual username and password, by utilization biometric identification mechanism. They develop One Time Password (OTP) which is valid for only short duration of time which is generated based on IMEI number, IMSI number, username, hour, pin, minute etc and can be effectively used for online banking, ATM or mobile banking services [15]. Jakobsson, M. et.al., (2009) introduces a new concept implicit authentication which is based on some actions carried out by the mobile user. They developed a model to implement implicit authentication and their preliminary investigation found that the approach is meaningful for usability or security purposes [16]. Some biometric authentication methods even consider keystroke dynamics and typing patterns are the implicit and continuous observation of the user behavior makes authentication based on the observations [17-19]. Herzberg, A., (2003) argue that mobile personal devices effectively used to perform secure banking and utility bill payments. He believes that mobile personal devices with some biometric mechanism will play an important role in many financial transactions including micropayments [20].

Angulo, J., & Wästlund, E. (2011) studied a lock pattern dynamics as a secure and user-friendly two-factor authentication method for giving security to user mobile phone's private and secret information. They modeled this on an android mobile phone based on user lock pattern and used Random Forest machine learning classifier and achieved an average Equal Error Rate (EER) of approximately 10.39% [21]. Delac, K., & Grgic, M. (2004, June) surveyed different biometric recognition methods and found that unimodal biometrics more vulnerable to attacks compare to multimodal biometrics. Biometric recognition system provides a consistent personal identification schema either to confirm or

decide the identity of an individual, which can be effectively used on any computer or mobile systems [22]. Seo, H.et.al., (2012) proposes a very special method of biometrics for intelligent mobile devices for which existing physical and behavioral biometrics are unsuitable, by analyzing users input patterns such as finger's touch duration, pressure level and the touching width of the finger on the touch screen. They found using the empirical method that the new method identifies the user with 100% efficiency [23].

De Marsico, et.al., (2014) suggested a new method of biometrics for mobile engagement, using face and iris recognition, multimodal biometrics referred as "FIRME" which is specially designed and embedded in mobile devices using the android operating system. Both design and implementation of face and iris are considered as the separate module, whose flow of work separate and finally two modules are fused. They claim that this multimodal authentication can be effectively used to find the identity of the user [24]. Adesuyi, F, et.al.,(2013) proposed a secure authentication for mobile banking using facial recognition. The number of online banking users rapidly increased in Nigeria and this made the researchers find some convenient and secure method for customers to do banking transactions remotely, keeping this aspect in mind they proposed new authentication method. The proposed system is expected to provide the higher level of authentication, which is multifactor authorization and makes the system vulnerable to attacks bare minimum [25]. Kumar, D., & Ryu, Y. (2009) surveyed biometric payment system used for various kinds of payment systems, in contrast to username and password no need of remembering anything. They also suggest in their study that when more and more customer uses the biometric system, cost of biometric reader will decrease and even small business firms also can use biometric systems [26].

Yoo, J. H. et.al., (2007, December) describe the design of the embedded biometric system that authenticates the person by using face-fingerprint or iris-fingerprint multimodal biometrics technology which is a new system compared to existing embedded system that time. The existing embedded system had problems like low computational resource and memory space. They implemented the system and also found execution time and also found the equal error rate for face, iris, and fingerprint as 1.50%, 1.68%, and 4.53% respectively [27]. Xi, K., & Hu, J. (2009, June) proposed a new fingerprint fuzzy vault based on multiple or composite features which are affective, reliable, distortion tolerant and registration free. They modeled and tested their results on the public database and found that the new schema can improve verification performance considerably [28]. Tao, Q., & Veldhuis, R. N. (2006, July) proposed an authentication method using facial recognition for the mobile personal device in a personal network and found that authentication method is the effective method with an equal error rate 1.2% [29]. Thirumathyam, R., & Derawi, M. O. (2010, May) proposed a nontraditional XML-database which supports biometric template and due to the large use of biometrics system, template are vulnerable to attacks. This research points out the requirement for template protection and analyses it using various template protection schema [30]. Usually, finger prints are unique for every human being means there will not be two people finger print identical. But researchers at New York University, Tandon School of Engineering found that there is a partial similarity between finger print two persons if that is used in Mobile or other electronic device for the security or authentication purposes is more vulnerable to security threats [31].

3. Location Authentication :

Location authentication is used in mobile users to retrieve user's current location and further process that data to acquire more information near to their current location and to authenticate against individual's claimed identity. In order to know the current location of the users GPS and GPRS used in phone and web services respectively [32]. Location based authentication is the special procedure to prove individual person’s identity or authenticity on emergence by identifying or detecting its presence at a separate locations. In order to accomplish location authentication some prerequisites components are essential; (i) The persons whom want to identified and

authenticated should present some symbol or icon of identity, (ii) The person needed to identified should carry at least one human authentication factor that should be able to recognize from any location, (iii) The distinct location must be already known or identified location.

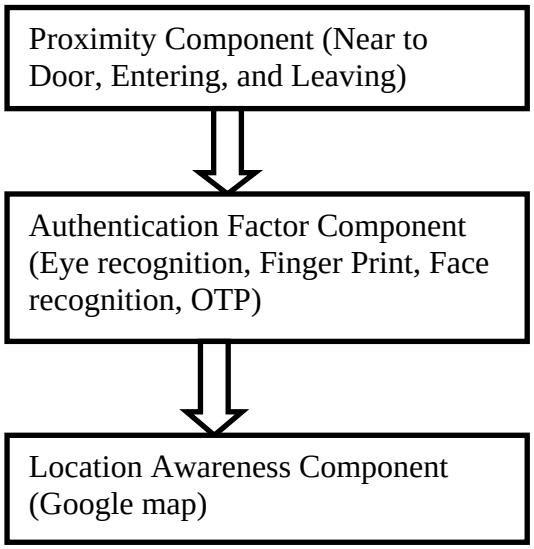

Figure 1: Primary Components of Location Authentication

As shown in Figure 1, primary components of Location Authentication are Proximity component, Authentication Factor Components and Known Location Components. Proximity Component is used to identify the person when person comes to proximity of certain area or location. This includes person comes to near the door, leaving a room and entering room etc. If iBeacon is used then proximity component coverage is very limited say 100 meters or 200 meters. On the other hand if GPS is used proximity component coverage will be very wide. Authentication Factor Components is used to identify the user or person using human authentication factors. Human authentication factors include any one factor like facial recognition, iris recognition, face recognition and OTP etc. Location Awareness Components is used to know the distinct location, which must be already known or identified location with the help of Google maps or any other location identification software.

The proximities or coverage of location identification is based on technology used for identification purpose if GPS is used it will be having more coverage or identification capacity compare to iBeacon. The application of location authentication or identification is extended to different applications like grant access to the particular nearby location by detecting the person at an entrance or at door. The system must have the capacity to discriminate between person entering and leaving. SolidPass security token combines the feature of location authentication along with two-factor authentication for the purpose of high-security solutions. In GPS-enabled mobile devices where there is a continuous track of locations. Location authentication adds an extra feature for security as "Where you Are", for the already existing features like "What you Know", "What you Are", "What You Have".

Global Positioning System (GPS) is presently used in all most all smart phones for the purpose of entertainment and sports and games. However, in future, we can witness GPS system used for security problems that are encountered in an online transaction like internet banking or mobile banking [33-35]. With the explosive growth of smart phones based payment system location based authentication technique can be used as key authentication technique along with multifactor authentication, relating user location with transactions in order to successively reduce fraud. Location information can be successively correlated with credit card transaction in order to enhance security.

4. Enhanced Mobile Banking Services :

With the aid of One Time password, Location authentication, Global Positioning System and some other advanced technology, banks can make some innovation and customization in mobile banking services [6]. These services can be accessible for users as omnipresent. Location based ID is the main component of location based authentication, which is responsible for storing user location and authorization policies or regulations. As shown in figure-2, in Enhanced Mobile Banking Services, we discuss mainly six attributes as Digital Deposit, Mini loan services, Advanced ATM Security, Advanced Bill Payment, Credit Card Security and Auxiliary Services.

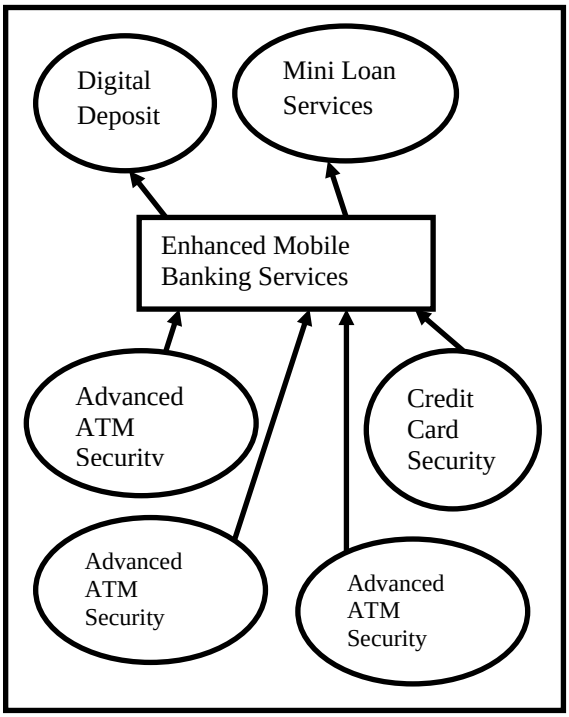

Figure 2: Enhanced Mobile Banking Services

Digital Deposit:

The rapid growth of internet, wireless and mobile communication technologies made depositing a cheque very simple compared to hassle task of waiting in a long queue in order to deposit a cheque. In digital deposit, user can deposit a cheque through online by sending the image of a cheque to the bank through their mobile phone. The image is scanned copy or photo of two sides of the cheque previously taken through the mobile camera or any other digital image capturing method. Here user location information is captured through iBeacon or GPS and which acts one more added level of security. If the parameters are in variance from normal practice a secret question answer is validated before further processing transaction request.

Mini Loan Services:

Usually, almost all banks find some constraints to provide Loan services through online or through mobile banking. A loan requires several documents and which should be verified and processed carefully before sectioning loan to a customer. The bank should study the customer income and also should check the repayment capacity. In order do all these things; there is a need for multiple sittings or conversations between Bank representative person and customer. In this paper, we discuss a new approach to process Mini Loan services. The different steps are;

(1) The customer has to first fill the personal details like salary details expenditure and some other details other than the details provided at the time of opening an account. Loan details also provide to the bank.

(2) By verifying the customer details, the bank should provide details of different document required for availing the loan services through an email.

(3) One or two level of Electronic meeting will be conducted between the user and bank representative.

(4) A copy of the document is submitted to the bank through email.

(5) By verifying all the documents a message is delivered to customer from the bank stating that whether the loan can be sectioned or not.

(6) Bank Persons will do the inspection of sight if required

(6) Customer will submit original document are to the bank.

(7) After final document verification loan is sectioned.

Here we can effectively use Location information before providing the loan. If the customers are only within the particular geometric circle loan is provided or they should have very good financial status. The user Location histories of three months are analyzed before sectioning loan.

Advanced ATM Security:

Security of the ATM machine is the biggest challenge for the bank to in order to accomplish a smooth and safe transaction of its customers. Every ATM machine will be having iBeacon or in the bank if its bank is nearby. When the user comes near to the door of ATM machine, iBeacon recognizes and a message is sent to the respective bank, where customers having his/her account. After matching the details bank will send a request to user mobile to enter secret question answer that customer only knows. Here iBeacon will extract customer location information and basic account details to know the identity of the user. Account Number is passed to the respective bank as a parameter and response will be requested to enter the answer for the secret question.

Advanced Bill Payment:
Initially, user's credit or debit card details are stored in mobile. If users are having multiple cards, then all card details are stored in the mobile or mobile app. Out of Multiple cards, one card is selected by the user in their mobile phone. This information is given to mobile and in-store reader of the mobile reads these details. These details are encrypted and stored in mobile. The location information of the user is extracted through iBeacon or GPS and secret answer or OTP is entered by the user, which is verified and finally, the transaction is completed.

Credit Card Security:
When credit card or debit card is read by the scanner or reader of the retailer or seller, there are more chances of security loopholes like extracting or hacking the password and misusing it for different purposes. In this paper, a new approach is explained for reading the credit card information. Through mobile payment apps specified amount of money is transferred from user account to seller's account. Here also location information of the user can use as an added security for the transactions.

Auxiliary Services:
The mobile phone can be used for multiple auxiliary purposes like mobile recharge, D2H recharge or for paying grocery and vegetable or for any other shopping purposes. Before authenticating the transaction Location information of the user are extracted and used as an added level of authentication.

5. Analysis of Enhanced Mobile Banking Services using location Authentication :

Enhanced Mobile Banking Services, which includes different attributes as Digital Deposit, Mini loan services, Advanced ATM Security, Advanced Bill Payment, Credit Card Security and Auxiliary Services is analyzed using its advantages, Benefits constraints, and disadvantages [36-46].

Advantages:

- All the services are authenticated with the help of location information which acts as added security for already existing security technologies.
- Location authentication can be easily flexible and integrated to any other type of security solutions.
- Existing Smart phone and GPS technologies can be affectively used for location information and authentication and user does not have to use some specific or extra devices or hardware.
- Digital images of the cheque and bill act as a proof for the transactions.
- Automatic bill payment through mobile phone avoids waiting in a queue.
- The use of existing technologies in smart phone avoids additional hardware cost.
- The customer can find eligibility for mini loan and loan request is processed online saves customer valuable time.
- With the help of Auxiliary service, the smart phone acts as multipurpose gadgets for all electronic payment, which act as add-on services other than mobile banking services.
- The security of the ATM can be effectively enhanced with the help of Advanced ATM security of enhanced mobile banking services.
- Credit Card can be secured from unauthorized access, cloning and password hacking with the help of location information and authentication.
- All bills can be paid through the finger-tip ubiquitously without any constraint of time, place and location.
- The Advanced security improves user trust over ATM machines or ATM transactions.

Benefits:

- Expansion Smart phone banking services in all areas globally.
- The number of users and usage of mobile banking can be improved due to ubiquitous services, higher security, innovative services and user friendliness.
- The ability to take advantage of new technologies like iBeacon, GPS, and smart phone through the digital deposit and mini loan services.
- Improves and enhances reputation or name and fame of the banking

organization with the help of secured and user-friendly services.

- Due to the innovative and new services passion for the smart phone can be improved.
- The bank can able to provide services to business man's software engineers or any other people, who finds difficult to get free time.
- Retails, sellers, customers and all parties involved in transactions are get benefited by new services.
- Indirectly new technology innovators also get their product popularity due to the use of technology in Location authentication.

Constraints:

- When GPS is used for providing location authentication many satellite related information are extracted which not easy to implement.
- Lack of skills and experience while implementing the services, reflects in robustness and reliability of services.
- Due to new technologies non-acceptance by the customers leads to possible failure of new technology or model.
- General competitiveness of the payment technology by the Mobile payment apps provider.
- Mini loan services will some constraints due to a necessity of various documents.

Disadvantages:

- Processing time or response time will increase due to additional security mechanism.
- Fixing time slot for an electronic meeting in case of mini loan services becomes tedious and which may lead to customer dissatisfaction.
- Lack of new technology support.
- Maintaining customer satisfaction in the electronic meeting is very difficult for bank representatives.
- Only location authentication will not give full security for a transaction, it will act as an added authentication above other authentication like password, one-time password, biometrics etc.

6. CONCLUSION :

The advanced wireless communication technologies and new authentication techniques like Location information made Smartphone banking transactions innovative, expansive and widespread. The introduction of new technologies in mobile banking services and globalization are increasingly driving the banking services to become ubiquitous, personalized, convenience, disseminative and secured. In this paper, we have discussed on Location information for processing different banking transaction which involved different attributes as Digital Deposit, Mini loan services, Advanced ATM Security, Advanced Bill Payment, Credit Card Security and Auxiliary Services.

In Digital Deposit the scanned image of the two sides of the cheque is processed by the bank and credited payees account. Mini loan services are one of the innovative services proposed in this paper, which works mainly based on an electronic meeting. Advanced ATM security controls the locking of the ATM doors based on location authentication and which are extracted using GPS or iBeacon and already existing features of the smart phone. Advanced bill payment extracts the card information details of multiple card or single card and processes the request. Here also lactation details or authentication acts as one of the major parameters in authentication. A credit card scanner explains how we can control some security loopholes. Auxiliary services are used for different bill payment like grocery, vegetables and much more. All of these services or attributes uses location information as an added security for mobile banking financial transaction or services. If the Location happens to be a Bank Branch or an ATM, where there is a proper iBeacon or GPS providing additional information about identification, then in such a situation the Authentication can be further simplified based on the type of transaction. In this paper, we discuss in detail location-based authentication and how these can be affectively applied in enhancing the mobile banking services.

REFERENCES :

[1] Safeena, R., Date, H., Kammani, A., & Hundewale, N. (2012). Technology adoption and Indian consumers: study on

mobile banking. *International Journal of Computer Theory and Engineering*, *4*(6), 1020.

[2] Amin, H., Hamid, M. R. A., Tanakinjal, G. H., & Lada, S. (2006). Undergraduate attitudes and expectations for mobile banking. *Journal of Internet Banking and Commerce*, *11*(3), 2006-12.

[3] Ivatury, G., & Mas, I. (2008). The early experience with branchless banking. *CGAP Focus Note*, (46).

[4] Donner, J., & Tellez, C. A. (2008). Mobile banking and economic development: Linking adoption, impact, and use. *Asian journal of communication*, *18*(4), 318-332.

[5] Liu, Z., Min, Q., & Ji, S. (2009, May). An empirical study on mobile banking adoption: The role of trust. In *Electronic Commerce and Security, 2009. ISECS'09. Second International Symposium on* (Vol. 2, pp. 7-13). IEEE.

[6] Krishna Prasad, K., & Aithal, P. S. (2015). Massive Growth of Banking Technology with the Aid of 5G Technologies. *International Journal of Management, IT and Engineering*, *5*(7), 616-627.

[7] Krishna Prasad, K., & Aithal, P. S. (2016). The Growth of 4G Technologies in India-Challenges and Opportunities. *International Journal of Management, IT and Engineering*, *6*(1), 543-351.

[8] Krishna Prasad, K., & Aithal, P. S. (2015). Mobile system for Customized and Ubiquitous Learning by 4G/5G.*International Journal of Management, IT and Engineering*, *5*(7),63-71.

[9] Krishna Prasad, K., & Aithal, P. S. (2016). Changing Perspectives of Mobile Information Communication Technologies towards Customized and Secured Services through 5G & 6G. *International Journal of Engineering Research and Modern Education (IJERME), 1(2), 210-224.*

[10] Krishna Prasad, K., & Aithal, P. S. (2016). An Online Comparative Study on 4G Technologies Service Providers in India. *International Journal of Advanced Trends in Engineering and Technology (IJATET). 1(1), 96-101*.

[11] Leggett, J., Williams, G., Usnick, M., & Longnecker, M. (1991). Dynamic identity verification via keystroke characteristics. *International Journal of Man-Machine Studies*, *35*(6), 859-870.

[12] Monrose, F., & Rubin, A. (1997, April). Authentication via keystroke dynamics. In *Proceedings of the 4th ACM conference on Computer and communications security* (pp. 48-56). ACM.

[13] M. Nisenson, I. Yariv, R. El-Yaniv, and R. Meir.(2003). Towards behaviour metric security systems: Learning to identify a typist. In PKDD, 2003.

[14] Herzberg, A. (2003). Payments and banking with mobile personal devices. *Communications of the ACM*, *46*(5), 53-58.

[15] Aloul, F. A., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In AICCSA (pp. 641-644).

[16] Jakobsson, M., Shi, E., Golle, P., & Chow, R. (2009, August). Implicit authentication for mobile devices. In Proceedings of the 4th USENIX conference on Hot topics in security (pp. 9-9). USENIX Association.

[17] Leggett, J., Williams, G., Usnick, M., & Longnecker, M. (1991). Dynamic identity verification via keystroke characteristics. International Journal of Man-Machine Studies, 35(6), 859-870.

[18] Monrose, F., & Rubin, A. (1997, April). Authentication via keystroke dynamics. In Proceedings of the 4th ACM conference on Computer and communications security (pp. 48-56). ACM.

[19] M. Nisenson, I. Yariv, R. El-Yaniv, and R. Meir.(2003). Towards behaviour metric security systems: Learning to identify a typist. In PKDD, 2003.

[20] Herzberg, A. (2003). Payments and banking with mobile personal devices. Communications of the ACM, 46(5), 53-58.

[21] Angulo, J., & Wästlund, E. (2011, September). Exploring touch-screen biometrics for user identification on smart phones. In IFIP PrimeLife International Summer School on Privacy and Identity Management for Life (pp. 130-143). Springer Berlin Heidelberg.

[22] Delac, K., & Grgic, M. (2004, June). A survey of biometric recognition methods. In Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium (pp. 184-193). IEEE.

[23] Seo, H., Kim, E., & Kim, H. K. (2012). A novel biometric identification based on a users input pattern analysis for intelligent mobile devices. International Journal of Advanced Robotic Systems, 9, 1-10.

[24] De Marsico, M., Galdi, C., Nappi, M., & Riccio, D. (2014). FIRME: face and iris recognition for mobile engagement. Image and Vision Computing, 32(12), 1161-1172.

[25] Adesuyi, F. A., Oluwafemi, O., Oludare, A. I., Victor, A. N., & Rick, A. V. (2013). Secure Authentication for Mobile Banking Using Facial Recognition.

[26] Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. International Journal of advanced science and Technology, 4, 25-38.

[27] Yoo, J. H., Ko, J. G., Chung, Y. S., Jung, S. U., Kim, K. H., Moon, K. Y., & Chung, K. (2007, December). Design of embedded multimodal biometric systems. In Signal-Image Technologies and Internet-Based System, 2007. SITIS'07. Third International IEEE Conference on (pp. 1058-1062). IEEE.

[28] Xi, K., & Hu, J. (2009, June). Biometric mobile template protection: a composite feature based fingerprint fuzzy vault. In 2009 IEEE International Conference on Communications (pp. 1-5). IEEE.

[29] Tao, Q., & Veldhuis, R. N. (2006, July). Biometric authentication for a mobile personal device. In Mobile and Ubiquitous Systems-Workshops, 2006. 3rd Annual International Conference on (pp. 1-3). IEEE.

[30] Thirumathyam, R., & Derawi, M. O. (2010, May). Biometric template data protection in mobile device environment using XML-database. In Security and Communication Networks (IWSCN), 2010 2nd International Workshop on (pp. 1-7). IEEE.

[31]Aditi Roy, Nasir Memon, Arun Ross. MasterPrint **(**2017)**:** Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems**.** *IEEE Transactions on Information Forensics and Security*; 1 DOI: 10.1109/TIFS.2017.2691658.

[32] YounSun Gho, L. Bao, M.T. Goodrich, "LAAC: A Location-Aware Access Control Protocol", Mobiquitous, *Third Annual International Conference on Mobile and Ubiquitous Systems, Networking, and Services*, pp.1-7, 2006.

[33] Zhang, F., Kondoro, A., & Muftic, S. (2012, June). Location-based authentication and authorization using smart phones. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* (pp. 1285-1292). IEEE.

[34] M. Balakrishnan, I. Mohomed, and V. Ramasubramanian(2009), "Where's that phone?: geolocating IP addresses on 3G networks," in Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference. ACM, 2009, pp. 294–300.

[35] Anon, IP Address Geolocation to Identify Website Visitor's Geographical Location. Available at: http://www.ip2location.com/ [Accessed April 29, 2017].

[36] Aithal, P. S., Shailashree V. T & Suresh Kumar P. M., (2016). Analysis of ABC Model of Annual Research Productivity using ABCD Framework. *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 846-858. DOI : http://doi.org/10.5281/zenodo.62022.

[37] Aithal P. S. & P.M. Suresh Kumar, (2016). Opportunities and Challenges for

Private Universities in India. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 88-113.

[38] Sridhar Acharya P. And Aithal P. S., (2016). Concepts of Ideal Electric Energy System FOR production, distribution and utilization. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 367-379.

[39] Padmanabha Shenoy, and Aithal P. S., (2016). A Study on History of Paper and possible Paper Free World. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 337-355.

[40] Aithal, P. S., (2015). Comparative Study on MBA Programmes in Private & Public Universities - A case study of MBA programme plan of Srinivas University, *International Journal of Management Sciences and Business Research (IJMSBR)*, 4(12), 106-122.

[41] Aithal P. S., & Shubhrajyotsna Aithal (2016). Impact of On-line Education on Higher Education System. *International Journal of Engineering Research and Modern Education (IJERME)*, 1(1), 225-235.

[42] Aithal P. S., and Suresh Kumar P. M., (2016). Analysis of Choice Based Credit System in Higher Education. *International Journal of Engineering Research and Modern Education (IJERME)*, 1(1), 278-284.

[43] Varun Shenoy and Aithal P. S., (2016). Changing Approaches in Campus Placements - A new futuristic Model, *International Journal of Scientific Research and Modern Education (IJSRME)*, 1(1), 766 – 776.

[44] Prithi Rao, and Aithal, P.S. (2016). Green Education Concepts & Strategies in Higher Education Model, *International Journal of Scientific Research and Modern Education (IJSRME)*, 1(1), 793-802. DOI : http://doi.org/10.5281/zenodo.160877.

[45] Aithal, P. S. & Shubhrajyotsna Aithal (2016). Ekalavya Model of Higher Education – an Innovation of IBM's Big Data University. *International Journal of Current Research and Modern Education (IJCRME)*, 1(2), 190-205. DOI: http://dx.doi.org/10.5281/ZENODO.198704.

[46] Aithal, P. S. & Shubhrajyotsna Aithal, (2016). A New Model for Commercialization of Nanotechnology Products and Services. *International Journal of Computational Research and Development*, 1(1), 84-93. DOI : http://doi.org/10.5281/zenodo.163536.