International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

PRIVACY PRESERVATION SCHEME OF FACE IDENTIFICATION WITH MULTIPARTY ACCESS IN NET BANKING ENVIRONMENTS

Mr.R.Gopikrishnan [1], Anitha.P [2], Thulasi.S [3] ,Uththira.R[4]

[1] *Assitant professor, Department of CSE, University college of engineering, Thirukkuvalai*
[2 .3.4] *Student, Department of CSE, University college of engineering, Thirukkuvalai,*

Abstract - *The providers of Internet banking services must be more responsive towards security requirements. Now days with the network world, the way for cybercrime is become easier for hacking purpose. Because of this reason, network security has become one of the biggest facing today's IT departments security. While there is no doubt that Internet banking transaction should have layered protection against security threats, the providers should approach security considerations as part of their service offerings. And heard a lot about hackers and crackers ways to steal any logical password or pin code number character, crimes of ID cards or credit cards fraud or security breaches. In existing framework, Identification can be equated to a username and is used to authorize access to a system. As usernames can be lost or stolen, it is necessary to validate that the intended user is really the person he or she claims to be – the authentication process. Biometric based authentication and identification systems are the new solutions to address the issues of security and privacy. The Face Recognition is the study of physical or behavioral characteristics of human being used for the identification of person. These physical characteristics of a person include the various features like fingerprints, face, hand geometry, voice, and iris biometric device. So implement real time authentication system using face biometrics for authorized the person for online banking system. The general objective of the paper is to develop fully functional face recognition, verification system provide and understand the key aspects of these major technologies, namely those relating to the technological, application entity domain, social environmental system and performance aspects. And also provide multiparty access system to allow the multiple persons to access the same accounts by providing access privileges to original account holders. Experimental results show that the proposed system provide high level security in online transaction system than the existing traditional cryptography approach.*

Key Words*: *Internet banking, Face biometrics, Authentication system, Multi party access

1. INTRODUCTION

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are then distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behavior-metrics to describe the latter class of biometrics. Fig 1 shows the block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.

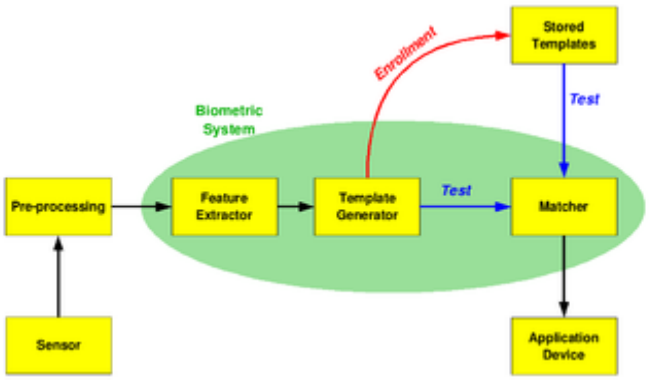

Fig – 1 Block diagram of biometric system

Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for

'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption

1.1 MULTIMODAL BIOMETRIC:

Multimodal biometric systems use multiple sensors or biometrics to overcome the limitations of unimodal biometric systems. For instance iris recognition systems can be compromised by aging irises and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken pass-code).

Multimodal biometric systems can fuse these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively. Fusion of the biometrics information can occur at different stages of a recognition system. In case of feature level fusion, the data itself or the features extracted from multiple biometrics are fused. Matching-score level fusion consolidates the scores generated by multiple classifiers pertaining to different modalities. Finally, in case of decision level fusion the final results of multiple classifiers are combined via techniques such as majority voting. Feature level fusion is believed to be more effective than the other levels of fusion because the feature set contains richer information about the input biometric data than the matching score or the output decision of a classifier. Therefore, fusion at the feature level is expected to provide better recognition results

2. RELATED WORK

Luigi Atzori, et.al,…[1] a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals. Actually, many challenging issues still need to be addressed and both technological as well as social knots have to be untied before the IoT idea being widely accepted. Central issues are making a full interoperability of inter-connected devices possible, providing them with an always higher degree of smartness by enabling their adaptation and autonomous behavior, while guaranteeing trust, privacy, and security. Also, the IoT idea poses several new problems concerning the networking aspects. In fact, the things composing the IoT will be characterized by low resources in terms of both computation and energy capacity. Accordingly, the proposed solutions need to pay special attention to resource efficiency besides the obvious scalability problems.

Shanzhi Chen, et.al,…[2] implemented a technology and economic wave in the global information industry after the Internet. The IoT is an intelligent network which connects all things to the Internet for the purpose of exchanging information and communicating through the information sensing devices in accordance with agreed protocols. It achieves the goal of intelligent identifying, locating, tracking, monitoring, and managing things. It is an

extension and expansion of Internet-based network, which expands the communication from human and human to human and things or things and things. In the IoT paradigm, many objects surrounding us will be connected into networks in one form or another. RF identification (RFID), sensor technology, and other smart technologies will be embedded into a variety of applications. Using RFID, sensors, and two-dimensional barcode to obtain the object information at anytime and anywhere, it will be a new opportunity. Using it, information and communication systems can be invisibly embedded in the environment around us. Sensor network will enable people to interact with the real world remotely. Identification technologies mentioned here include objects and location identifications. Identification and recognition of the physical world is the foundation of implementing overall perception. Through a variety of available radio networks, telecommunication networks, and Internet, objects information can be available in any time. Communication technology here includes a variety of wired and wireless transmission technologies, switching technologies, networking technologies, and gateway technologies. IoT further creates the interaction among the physical world, the virtual world, the digital world, and the society.

Huansheng Ning, et.al,…[3] analyzed paradigm to realize universal interactions among the ubiquitous things through heterogeneous spaces. The future IoT is expected to be characterized by the comprehensive perception, reliable transmission, and intelligent processing to achieve pervasive interconnections, intelligence, and efficiency. It enables things to establish dynamical and seamless interconnections across heterogeneous spaces. During the things' interactions, it brings out a series of explosions of connection, information, service, and intelligence.Smart connectivity and effective interactions for addressinga certain task with an ultimate performance are highly demandingtrends. It will bring an inevitable reconfigurable combination ofemerging science and technology issues to launch a new researcharea.To trace the derivation of the IoT, it is originated from thenetworks of computers, which realizes the connections amongmultiple devices in the computer networks. Afterwards, the Internetof Computers (IoC) emerges to address the cyber entities'data exchanging in the cyber space.

Tie Qiu,et.al,…[4] providedpeer to peer networks and each node has functions of data collecting, storage, processing and forwarding. It is the cost-effective solution for the short-range communication in some particular scenarios, such as battlefield, disaster rescue, environment sensing, etc. In order to improve the Quality of Service (QoS) among different heterogeneous network units, HANETs become the research focus in recent years. HANETs usually consist of wireless sensor networks (WSNs), smart ad hoc networks, wireless fidelity networks, telecommunication networks, vehicular ad hoc networks (VANETs), etc. The heterogeneous network units are accessible and interconnected through the gateway nodes. WSNs comprise a large number of specialized sensor nodes, which can dynamically set up a self-organizing communication network. With the development of the Internet of things, heterogeneous wireless sensor networks have been rapidly growing. There are two kinds of nodes in heterogenous wireless sensor networks, regular nodes and super nodes. They have equal opportunity to access to the network, but have different functions. The regular nodes are responsible for monitoring the surrounding environment, sending and forwarding the sensing data to the super nodes. Super nodes mainly collect the data from regular nodes and connect the other types of networks by gateway nodes. The sensing data can be sent to the cloud-based data center which processes the data and manage the network.

Jianhua Ma, et.al,..[5] designed an efficient TRE solution for services that are deployed in the cloud and dominated by the data transfer from the cloud servers to the clients. We propose a Cooperative end-to-end TRE solution, named as CoRE, with capability of removing both short-term and long-term redundancy such that traffic redundancy can be eliminated to the highest degree. CoRE involves two layers of cooperative TRE operations. The first-layer TRE performs prediction-based Chunk-Match similar to PACK to capture long-term traffic redundancy. The second-layer TRE identifies maximal duplicate substrings within an outgoing chunk compared with the previously transmitted chunks in a local chunk cache at the sender, referred to as In-Chunk Max-Match. If the redundancy detection at the first-layer fails, CoRE turns to the second-layer to identify finer-granularity redundancy, i.e., short term redundancy, inside chunks. With the consideration of the requirements of cloud environment for TRE, CoRE incorporates several careful designs and optimizations to reduce CoRE's operation cost and improve its TRE efficiency. First, CoRE uses a temporary small chunk cache for each client to reduce the storage cost of In-Chunk Max-Match at a server. It requires cache synchronization between the sender and receiver, but it only detects the traffic redundancy in short-term and thus cloud elasticity does not have much effect on the TRE efficiency. Second, a single-pass scanning algorithm is used in CoRE to determine chunk boundaries in the TCP stream while at the same time obtaining the fingerprints within chunks used to find maximal duplicate substrings in chunks. It efficiently integrates two layers of TRE operations.

3. EXISTING METHODOLOGIES

Online security remains a challenge to ensure safe transacting on the internet. User authentication, a human-centric process, is regarded as the basis of computer security and hence secure access to online banking services. The increased use of technology to enforce additional actions has the ability to improve the quality of authentication and hence online security, but often at the expense of usability. Today, there are a number of technologies in use to combat fraud in the banking industry. One of these is the use of One Time Passwords (OTPs), which is a fraud prevention technology specific for e-banking transactions. The most

basic method displays a time-dependent code that a user is required to input into the banking interface. Smart cards and USB tokens are other security measures employed by banks that work by verifying the user through their possession of a smart card or USB device. The problem is that all existing security measures present one challenge or the other. Transaction monitoring is a different type of approach that comes from an adaptation of credit/debit card fraud prevention systems. This approach analysis the sender and receiver of the transaction and compares with identified fraud patterns. Any similarity results in the transaction being declined or transferred to a call center for manual verification. This approach requires no additional hardware for the user as all analysis is done in the background. However, this too comes with its disadvantages, as there will be a loophole in the system when new fraud patterns occur before they are detected. Also, occasionally genuine transactions will be forwarded to call centers which then inconvenience customers

4. PROPOSED METHODOLOGIES

Online banking is now very popular among consumers because it provides a convenient way to perform transactions from anywhere using smart devices. Now a days thieves are using high tech methods to gain access to user information such as passwords, PINs and security questions. This project aims at enhancing the security of Internet banking system with additional face biometric Authentication combination. Internet banking now uses Static User ids and passwords along with OTP-One time Passwords to mobile number. Although this is the best security feature available to date, this security method is still vulnerable and it is very important to enhance the existing security. The term biometrics refers to the emerging field of technology devoted to the identification of individuals using biological behaviors. Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information. Biometrics is not into Internet banking applications yet. It is because of the practical difficulties and it is very expensive to implement and execute this technology. But, now with technology advancement and cost of Biometric devices coming down, we have probabilities to integrate Biometric Technology to Online Banking. Face biometric can be used to provide cost effective rather than other biometric features such as fingerprint, iris and other features. And also extend the process to implement the system with multiparty access. The user of the account is considered as primary user. The primary user provides the permission to access account to other persons considered as secondary users. The primary user set the limit for secondary access. At the time of login verification, face can be recognized as whether it is primary or secondary. The OTP based password can be send at the time transactions. Finally SMS alert send to primary user with detail description of user name, time of access, amount details. Session time analysis can be used prevent from infrequent access.

4.1 ITERATIVE CLOSEST POINT ALGORITHM:

In The Iterative Closest Point or, in some sources, the Iterative Corresponding Point, one point cloud (vertex cloud), the reference, or target, is kept fixed, while the other one, the source, is transformed to best match the reference. The algorithm iteratively revises the transformation (combination of translation and rotation) needed to minimize an error metric, usually the distance from the source to the reference point cloud. ICP is one of the widely used algorithms in aligning three dimensional models given an initial guess of the rigid body transformation required. Given 2 points r_1 and r_2 , the Euclidean distance is:

$$d(r_1, r_2) = \|r_1 - r_2\| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}$$

The sceneshape S is aligned to be in the best alignment with the model shape M.

$$d(r_1, A) = \min_{i \in 1..n} d(r_1, a_i)$$

The distance of each point s of the scene from the model is:

Algorithm steps as follows:

function ICP(Scene,Model)

begin

E` ← + ∞;

(Rot,Trans) ← In Initialize-Alignment(Scene,Model);

repeat

E ← E`;

Aligned-Scene ← Apply-Alignment(Scene,Rot,Trans);

Pairs ← Return-Closest-Pairs(Aligned-Scene,Model);

(Rot,Trans,E`)←Update-Alignment(Scene,Model,Pairs,Rot,Trans);

Until |E`- E| < Threshold

return (Rot,Trans);

end

$$d(s, M) = \min_{m \in M} d\|m - s\|$$

4.2 KNN CLASSIFIER:

In face recognition, the KNN algorithm is a method for classifying objects based on closest training examples in the feature space. KNN is a type of instance-based learning, or lazy learning where the function is only approximated locally and all computation is deferred until classification. The KNN is the fundamental and simplest classification

technique when there is little or no prior knowledge about the distribution of the data. This rule simply retains the entire training set during learning and assigns to each query a class represented by the majority label of its k-nearest neighbors in the training set. The Nearest Neighbor rule (NN) is the simplest form of KNN when K = 1. In this method each sample should be classified similarly to its surrounding samples. Therefore, if the classification of a sample is unknown, then it could be predicted by considering the classification of its nearest neighbor samples. Given an unknown sample and a training set, all the distances between the unknown sample and all the samples in the training set can be computed. The distance with the smallest value corresponds to the sample in the training set closest to the unknown sample. Therefore, the unknown sample may be classified based on the classification of this nearest neighbor. The algorithm steps as follows:

for all the unknown samples UnSample(i)

for all the known samples Sample(j)

compute the distance between

Unsamples(i) and Sample(j)

end for

fing the k smallest distances

locate the corresponding samples

Sample(j1),….,Sample(jK)

assign UnSample(i) to the class which appears more frequently

end for

The performance of a KNN classifier is primarily determined by the choice of K as well as the distance metric applied. The estimate is affected by the sensitivity of the selection of the neighborhood size K, because the radius of the local region is determined by the distance of the Kth nearest neighbor to the query and different K yields different conditional class probabilities. The proposed work is shown in fig 2.

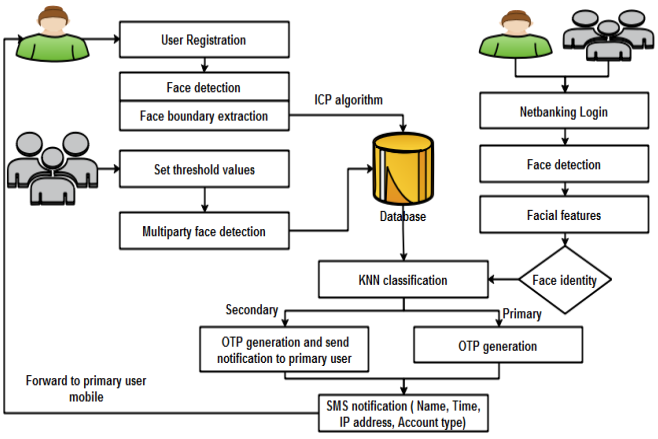

Fig - 2 Proposed Framework

5. CONCLUSION

As the level of security breaches and transaction frauds increase day by day, the need for highly secure identification and personal verification information systems is becoming extremely important especially in the banking and finance sector. In this paper, we can implement face recognition system to online net-banking application in IOT environments. Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking based security systems. The ID can be stolen; passwords can be forgotten or cracked but the physical characteristics of a person cannot be stolen or hacked. The Face Recognition identification overcomes all the above. And also provide multi-person access control to provide access privileges to users with improved security. Real time alert system about unauthorized access and multi person access.

ACKNOWLEDGEMENT

The authors can acknowledge any person/authorities in this section. This is not mandatory.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer networks, vol. 54, no. 15, pp. 2787-2805, 2010.

[2] S. Chen, H. Xu, D. Liu, and B. Hu, “A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective,” IEEE Internet of Things Journal, vol. 1, no. 4, pp. 349-359, 2014.

[3] H. Ning, H. Liu, J. Ma, L. T. Yang, and R. Huang, “Cybermatics: Cyberphysical- social-thinking hyperspace based science and technology,” Future Generation Computer Systems, vol. 56, pp. 504-522, 2016.

[4] T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, “Heterogeneous ad hoc networks: Architectures, advances and challenges,” Ad Hoc Networks, vol. 55, pp. 143-152, 2017.

[5] H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke, Smart Cities: Foundations, Principles and Applications. Hoboken, NJ, USA: Wiley, 2017.

[6] J. Ma, J. Wen, R. Huang, and B. Huang, “Cyber-Individual Meets Brain Informatics,” IEEE Intelligent Systems, vol. 26, no. 5, pp. 30-37, 2011.

[7] J. Miranda, N. Makitalo, J. Garciaalonso, J. Berrocal, T. Mikkonen, C. Canal, et al., “From the Internet of Things to the Internet of People,” IEEE Internet Computing, vol. 19, no. 2, pp. 40-47, 2015.

[8] H. Ning and H. Liu, “Cyber-physical-social-thinking space based science and technology framework for the Internet of

Things," Science China Information Sciences, vol. 58, no. 3, pp. 1-19, 2015.

[9] D. L. Brock, "The electronic product code (epc)," Auto-ID Center White Paper MIT-AUTOID-WH-002, 2001.

[10] N. Koshizuka and K. Sakamura, "Ubiquitous ID: standards for ubiquitous computing and the Internet of Things," IEEE Pervasive Computing, vol. 9, no. 4, pp. 98-101, 2010.

[11] H. Ning, S. Hu, W. He, Q. Xu, H. Liu, and W. Chen, "nID-based internet of things and its application in airport aviation risk management," Chinese Journal of Electronics, vol. 21, no. 2, pp. 209-214, 2012.

[12] H. Ning, Y. Fu, S. Hu, and H. Liu, "Tree-Code modeling and addressing for non-ID physical objects in the Internet of Things," Telecommunication Systems, vol. 58, no. 3, pp. 195-204, 2015.

[13] S. Kwok, O. P. Ng, A. H. Tsang, and H. Liem, "Physimetric identification (Physi-ID)–Applying biometric concept in physical object identification," Computers in Industry, vol. 62, no. 1, pp. 32-41, 2011.

[14] M. Beham and S. Roomi, "A review of face recognition methods," International Journal of Pattern Recognition and Artificial Intelligence, vol. 27, no. 04, pp. 1356005101-1356005135, 2013.

[15] S. Shaikh and J. Rabaiotti, "Characteristic trade-offs in designing largescale biometric-based identity management systems," Journal of Network and Computer Applications, vol. 33, no. 3, pp. 342-351, 2010. and Technical Research, vol. 3, no. 2, pp. 298-300, 2015.

[16] L. Yu, L. Chen, Z. Cai, H. Shen, Y. Liang, and Y. Pan, "Stochastic Load Balancing for Virtual Resource Management in Datacenters," IEEE Transactions on Cloud Computing, 2016. [Online]. Available: https://doi.org/10.1109/TCC.2016.2525984

[17] P. Peer, ˇ Z. Emerˇsiˇc, J. Bule, J. ˇ Zganec-Gros, and V. ˇ Struc, "Strategies for exploiting independent cloud implementations of biometric experts in multibiometric scenarios," Mathematical problems in engineering, vol. 2014, pp. 1-15, 2014.

[18] L. Yu, H. Shen, K. Sapra, and L. Ye, "CoRE: Cooperative End-to-End Traffic Redundancy Elimination for Reducing Cloud Bandwidth Cost," IEEE Transactions on Parallel and Distributed Systems, 2016. [Online]. Available: https://doi.org/10.1109/TPDS.2016.2578928

[19] L. Yu and Z. Cai, "Dynamic scaling of virtual clusters with bandwidth guarantee in cloud datacenters," in IEEE INFOCOM 2016 – IEEE Conference on Computer Communications, 2016, pp. 1-9.

[20] N. N. Khan, "Fog Computing: A Better Solution For IoT," International Journal of Engineering and Technical Research, vol. 3, no. 2, pp. 298- 300, 2015.