MAPLE TREE PUBLISHING HOUSE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION (IRJMT)

http://www.mapletreejournals.com/index.php/IRJMT
Received 09 August 2019 ISSN 2582-1040
Accepted 12 September 2019 2019; 1(6); 26-34
Published online 02 November 2019

A highly secure Multi- Factor authentication system using biometrics to enhance privacy in Internet of Things (IOT)

M. Vijay[1*], G. Indumathi[2]

[1]*Assistant Professor, Department of ECE & V.S.B. Engineering College, Karur,Tamil Nadu, India.*

[2] *Professor, Department of ECE & Mepco Schlenk Engineering College, Sivakasi,Tamil Nadu, India.*

**Corresponding author E-Mail ID: vijaymepcoece@gmail.com*

Doi: https://doi.org/10.34256/irjmtcon4

ABSTRACT

Authentication is becoming critical in the Internet of Things (IoT) environment because of its many applications and services have been emerging in the areas such as smart city, healthcare, industry etc. Security and privacy plays a vital role in IoT because their services can be accessed through smart device applications by the user from everywhere and at any time. Hence a multi-factor based authentication can provide high security in IOT environment. This security system incorporates most of the valuable methods such as cryptography, steganography and pattern recognition for authentication process. Among various biometric traits, palm vein is more efficient because it has essential sufficient features points for individual unique identification. The system employs registration phase and authentication phase. The registration phase enrolls person privacy data with their biometric and the obtained data's are encrypted with the help of Elliptical Curve Cryptography (ECC) and this confidential information is embedded into person palm print image using bits substitution procedure. In authentication phase, recognition will be performed through three levels such as password, palm print and One Time Password (OTP). Using these three levels the matching can be done. The texture features can be obtained by using Multi Block Local Binary Pattern (MB-LBP) and Gabor filter. To afford high authentication, OTP method is also appended. This system provides better information security and texture analysis rather than previous approaches. Thus this multiple level approach ensures a fool proof and a reliable way for data access. Results are in terms of some validation parameters like false acceptance ratio, false rejection ratio and recognition rate. Observing from results, it is clear that the proposed approach outperform many existing methods. As a result, the proposed scheme has strong security, reliability and enhanced computational efficiency.

Keywords: Biometrics, ECC, MB-LBP, OTP.

1. INTRODUCTION

Internet of things (IoT) is the internetworking of the physical devices that embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange useful data and meaningful information. The IoT incorporates everything so security in IOT plays a major role. Breach of privacy in a network is the most serious threat in the modern era where every bit of information is vital. Access of personal or private data needs to be secure, smart and safe. Authentication generally verifies the identity of a user who wishes to

access it. In general, there are three approaches to authentication, they are 1) Something we have (card, token, key) 2) Something we know (PIN, Password) 3) Something we are (biometric traits).

Passwords & PINs may be forgotten and token-based identification methods such as passports driver's licenses may be forged, stolen, or lost. Thus, biometric based identification play a bigger role in authentication process.

Biometric is an act of recognition of a person using personal or behavioral features. This set of features can be extracted from biometric characteristic like face, finger print, iris, ears, vein, palm, voice etc. The fingerprint recognition is cheapest, fastest, and most convenient yet forgery can be done. The face recognition is useful in automation systems but still more expensive and complex than other methods. Iris recognition is an unique one however a person who has a color blindness have difficulties to overcome this method. Retinal scan recognition has also unique features better than iris but disease such as cataracts affects the measurement accuracy. Simple, inexpensive recognition method namely hand geometry is easy to use but it's not unique and cannot be used in identification systems.

Hence, palm vein method is used as secured than others traits because of the distinctive blood vein pattern lies under the human skin. It also gives many additional benefits of stable line features, low intrusiveness and high user acceptance hence this recognition method has attained very good results.

Elliptical Curve Cryptography (ECC) offers improved security with a smaller key size than any other cryptographic techniques. Hong and Yanbing Liu (1) gave a cryptanalysis of image encryption scheme and identified that known-plain text attack. An image encryption algorithm (2) using ECC to obtain the cipher image, point multiplication is performed for each pixel value and for decryption, and a mapping table is required. By using Jacobian elliptic map (3) the plain image data matrix is transformed into one dimension matrix after operating with the key.

An another encryption scheme (4) using Elliptic curve ElGamal based homomorphic image for sharing secret images and (5) describes the implementation, related security and interoperability issue of Elliptic Curve Digital Signature Algorithm. Two ECC based encryption (6) on image are presented based on selective quantized DCT coefficients and on selective bit plane.

As compare to other feature extraction methods Local binary pattern (LBP) always suits best for extracting features in terms of texture. Additionally a multi block local binary pattern is implemented in our system to improve the results. The two dimensional Gabor (7) has been used for the development of a high performance palm print identification. In (9), a multimodal authentication system is presented so that segmented ROI are preprocessed using DCP (Differential Code Pattern) to obtain robust corner features. Pixel level fusion (10) is applied by using simple averaging method before bit-plane feature extraction and Principal Component Analysis is also used on the hybrid face-palm bit planes. By implementing, Local Derivative Pattern (LDP) (11) as feature extraction algorithm and Histogram Intersection matching algorithm in a palm vein-based biometric identification system and it has best accuracy of 98.3%, FAR and FRR of 0.01 and 0.01. Various methods (12) like Box counting (BC), the Mass Radius (MS) and the Cumulative Intersection (CumInt) methods extracted the palmprint texture information and it obtained recognition rates of about 96.35%. A Minutiae matching and Edge detection technique (13) is used by combining finger print and iris of a person at the matching-score level. By using repeated line tracking method, (14) the features are extracted from the finger knuckle and finger vein images afterwards feature-level fusion using FFF optimization is used to find out the optimal weight score to fuse the extracted feature sets of both finger knuckle and finger vein images. A new approach (15) is proposed for extracting critical features from the dorsal hand vein pattern using the concepts of Walsh transform and Euclidean distance similarity measure. Then a new adaptive threshold technique (16) makes the possibility to verify and authenticate with 15 degree of movement of hand while capturing vein pattern for authentication and has a false acceptance rate 0.0001% of and false rejection rate of 0.1%.A new extraction technique (17) coupled with the

feature selection technique has an improved identification performance. A combination of Gabor filters and histograms calculations (18) is investigated as a method for creating biometric templates and it has a FAR of 0.32%, a FRR of 1.58% and an EER of 1.45%.

So here our proposed security system combines most of the valuable techniques such as cryptography, steganography and pattern recognition for authentication process. The system involves two phases registration phase and authentication phase. After enrolling person privacy data with their biometric, the obtained data's are encrypted using Elliptical Curve Cryptography (ECC) and embedded this confidential information into person palm print image using bits substitution method. In authentication phase, recognition will be performed through three levels such as password, palm print and One Time Password (OTP). Using these three levels, the matching can be done. The texture features can be obtained by using Multi- Block Local Binary Pattern (MB-LBP) and Gabor filter. To afford high authentication, OTP method is also appended. This proposed system provides better information security and texture analysis rather than previous approaches. Results are in terms of some validation parameters like false acceptance ratio, false rejection ratio, recognition percentage and accuracy. And from results, it is clear that the proposed approach outperform many existing methods. As a result, the proposed scheme has strong security, reliability and efficiency.

The paper is organized as follows. Section II introduces Elliptic Curve Cryptography. Feature extraction techniques are discussed in Section III. In Section IV, Proposed model is discussed. The Section V presents the experimental results and discussion while concluding remarks are given in Section VI.

II. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Among various encryption schemes, the major reason to choose ECC is the key size. The Keys (1, 2) available in ECC are significantly smaller than other cryptosystems.ECC is a an asymmetric key cryptography as different key is used for generating public key and private key, which was first developed by NealKoblitz and Victor S. Miller independently in the year 1985. ECC (3) gains wide acceptance around 2004.When compared to other cryptographic schemes (4) such as DH, RSA, ElGamal, and DSA, ECC uses mathematical approach. A shorter key implies(5,6) easier data management, lower hardware requirements, low computation cost, less bandwidth, faster implementation when transmitting the keys over a network, and low power consumption. RSA using 1024 bit key size whereas the same level of security can be achieved through ECC using only 160 bit key. Similarly, when the bit size is 128, the length of key length of RSA is 3072 bits whereas in ECC is (256-283) bits.

A. Point Multiplication

By repeating addition of the base coordinate point, multiplication is performed. Many algorithms have been developing to perform point multiplication swiftly. *k*L=L+ L+ L+ . . . +*k* times.

B. Encryption and Decryption Using ECC

The communicating parties agrees upon the Elliptic curve equation and a Generator (G)

$$y^2 = \{x^3 + ax \text{ mod}[l] \qquad (1)$$

Suppose the sender want to encrypt a message '*Lq*' and send to receiver. The cipher text is given by *Lc=[kG, Lq+kLb*] where '*k*' is random integer and '*Lb*' is the public key of receiver computed using the private key of receiver '*rB*', *Lb= rBG*. Receiver decrypts the cipher message as, message = *[Lq+kLb-rBKG]*.Since *Lb=rBG*, kLb and *rBkG* cancel each other and '*Lq*'remains, which is the message sent by sender.

ECC operation is done by grouping the pixel and explained how many pixels can be grouped according to their parameters. Pairing of the grouped pixel value was performed instead of using mapping table for encryption and decryption. While using ECC, our method generates a low correlated cipher image even with an image which is made up of same pixel value. Even though other encryption has a faster time response, ECC based encryption performs better under noise analysis and hence it is useful for remote authentication applications and fewer number of bytes to generate the key.

III. FEATURE EXTRACTION

There are various types of feature extraction techniques and they are broadly classified into line based, appearance based, Texture based and code based. Here in our proposed work texture based method is taken into account and the features are extracted using Gabor Wavelet Transform &MB-LBP (Multi Block-Local Binary Patterns) Gabor filters (8) has a band pass filter having an orientation selective and frequency-selective features and optimal joint resolution in both spatial and frequency domain.

A two-dimensional Gabor filter (7) is a combine function of two components namely a complex plane wave and a Gaussian shaped function. In a 2-D case, the absolute square of the correlation between an image and a Gabor function provides the spectral energy density and is defined by,

$$g_{\alpha,\xi}(x) = g_{\alpha,\xi_0}(x_0)\, g_{\alpha,\xi_1}(x_1) \qquad (2)$$

For $\xi = (\xi_0, \xi_1)$ and $x = (x_0, x_1)$.

Whereas $g_{\alpha,=} \sqrt{\alpha/\pi}\, e^{-\alpha x^2} e($ is a variance and ξ is a frequency.)

The responses of the respective filters can be modeled by Gabor functions of different frequencies and orientations.

$$G(x, y) = \exp\left[-\frac{x}{}\right] \exp[j\varphi(x \quad c + y \quad s)] \quad (3)$$

Where σ is the standard deviation of the Gaussian function in the x and y directions and ω denotes the spatial frequency. Family of Gabor kernels can be obtained from the above equation by selecting different center frequencies and orientations. These kernels are used to extract features from an image.

LBP (8,12) is a gray-scale texture operator that characterizes the local spatial structure of the image texture. Given the central pixel in image, a pattern code is computed by associating it with its neighbors and its clearly shown in Fig 1

$$LBP_{P,R} = {}_p - {}_c)2^{p-1} \qquad (4)$$

$$v(x) = \begin{cases} 1, x \geq 0 \\ 0, x < 0 \end{cases}$$

Local binary pattern (18) is always a good method to extract features in terms of texture as compare to other feature extraction methods but still to get clear output; Multi Block-Local Binary Pattern is implemented. The original LBP is defined for each pixel by thresholding the neighborhood pixel value with the center pixel value. But MB-LBP operator correlates the central rectangle's average intensity with those of its neighborhood rectangles. Then a binary sequence is obtained and the output value of the MBLBP operator can be obtained as follows:

$$\text{MB-LBP} = \sum_{i=1}^{y} {}_i - {}_c)2^i \qquad (5)$$

$$v(x) = \begin{cases} 1, x \geq 0 \\ 0, x < 0 \end{cases}$$

By identifying LBP pattern of each pixel (i, j), a histogram is built to represent the whole texture image and is given by:

$$T(k) = \sum_{i=1}^{N} \sum_{j=1}^{M} f({}_{S,R}(i,j),k),k \quad [0,k] \qquad (6)$$

$$f(x, y) = \begin{cases} 1, x = y \\ 0, otherwise \end{cases}$$

Where 'K' denotes the maximal LBP pattern value and 'U'represents the number of the spatial transitions (bitwise changes) in that pattern. It is defined by:

$$U(\mathrm{LBP}_{S,R}) = \left(\begin{matrix} |v(g_{s-1}-g_c)-v(g_0 \quad -g_c)| + \\ \sum_{s=1}^{s-1} |v(g_s-g_c)|-v(g_{s-1}-g_c)| \end{matrix} \right) \quad (7)$$

Here the dissimilarity between a test sample V and a class model L is measured by the chi-square distance and is given by:

$$D(V, L) = \sum_{n=1}^{N} \frac{(v_n - }{(v_n} \quad (8)$$

Where, N is the number of bins, Vn is the values of the sample, and L$n$are model images at the nth bin. Hence by using Gabor wavelet, sharp filtered features which are converted into unique texture using this multi-block LBP method so accuracy of the method is improved.

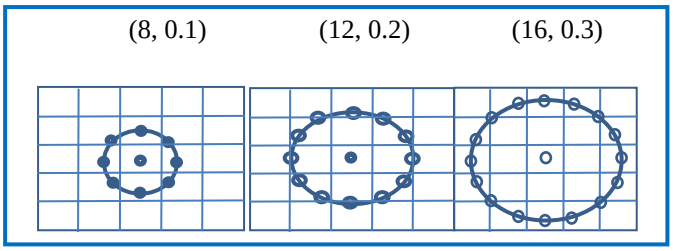

Fig. 1 Multi Block –LBP

IV. PROPOSED METHOD

Breach of privacy is the most serious threat in the modern era where every bit of information is vital. Access of personal or private data needs has to be secure, smart and safe. This method discusses a model for secure data access via Biometrics and Elliptic Curve Cryptography (ECC).The process can be broadly divided into 2 sequential phases - Registration & Authentication phase.

In Registration phase, (shown in Fig.2) the first time user should enroll their unique identities into the server. The trifecta identities are input palm print image, user id number and a unique 4 digit alphanumeric pass code. The registration process begins with the palm print of the user, either right or left palm, being imprinted. It undergoes chaos encryption (19) and stored as input palm print image. Before the data is hidden it is being encrypted using Chaos encryption.

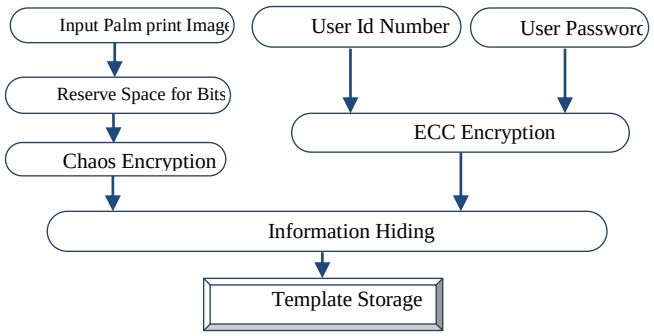

Fig. 2 Registration Phase

The data is being hidden inside the palm print using bits wrap algorithm. Alongside, user's unique id number and password are also entered, undergoing ECC Encryption. In Registration phase, (shown in Fig.2) the first time user should enroll their unique identities into the server. The trifecta identities are input palm print image, user id number and a unique 4 digit alphanumeric pass code. The registration process begins with the palm print of the user, either right or left palm, being imprinted. It undergoes chaos encryption (19) and stored as input palm print image. Before

the data is hidden it is being encrypted using Chaos encryption. The data is being hidden inside the palm print using bits wrap algorithm. Alongside, user's unique id number and password are also entered, undergoing ECC Encryption. The above added authentic data is stored as templates. All the information gathered from the users is stored in vast database in the server.

In the authentication phase, (shown in Fig. 3) the stored data is used to verify the credentials of the user. The process consists of initial input of user id followed by the ternary levels of authentication. The three levels being, user password, input palm print image and one time password (OTP).This intense three level process of verification enables the consumer to ensure proper and precise scrutiny of the users' identity. Initially, when the user enters the unique user id, the system checks for the availability in the pre-registered database, if available, the further steps of authentication begin.

In the first level of authentication, the user should enter the alphanumeric password, if accepted, and then the second level of authentication begins. Here, the user imprints his/ her palm print on the sensor, which is then verified in the database for the correct match. If the image is precisely matched, then the final and third level of authentication begins, where the user enters the one time password (OTP). The OTP is sent through mobile number and/ or email address. On entering the OTP, he/ she unlock the entire system, thereby earning the complete access to the data. An OTP (17) is appropriate for single login session. It will be sent directly to the user's mobile phone. It is a dynamic password that will differ for each and every transaction and mainly used for authentication based services. As mentioned above, the registration phase enrolls person privacy data with their biometric and the obtained data's are encrypted with the help of Elliptical Curve Cryptography (ECC) and this confidential information is embedded into person palm print image using bits substitution procedure (10). In authentication phase, recognition will be performed through three levels such as password, palm print and One Time Password (OTP). Using these three levels the matching can be done. The texture features can be obtained by using Multi- Block Local Binary Pattern (MB-LBP) and Gabor filter. To afford high authentication, OTP method is also appended. This system provides better information security and texture analysis rather than previous approaches.

V. RESULTS & DISCUSSION

In the proposed system the biometric data's are taken from the CASIA database.
Experiments using Local Derivative Pattern (11), Multimodal Biometrics (13), K-Support Vector Machine classifier (14), Thresholding Technique (16), Gabor based (18) and the proposed method are conducted on the biometric data's taken from the CASIA database and implemented in MATLAB R2016 with a PC of 4 GB RAM and 2.10 GHz Intel i-7processor and windows 7 operating system. Initially five different cases are taken and the test data's are 160, 200, 100, 300 and 250 respectively. FAR is 0.000015 and FRR is 0.00012 in case1. In test case 2 FAR is 0.00002 and FRR is 0.00023, in case3 FAR is 0.00001and FRR is 0.00015, in test case 4 FAR is 0.00003 and FRR is 0.00029 and in test case 5 FAR is 0.00025 and FRR is 0.0021.(shown in Fig 4).The average values of all set of case are calculated and the values of FAR and FRR values are 0.0001 and0.001 respectively. Subsequently, the proposed method is compared with some recent popular methods such as Local Derivative Pattern (11), Multimodal Biometrics (13), K-Support Vector Machine classifier (14), Thresholding Technique (16), Gabor based (18)and their comparison values are tabulated. (Shown in Fig 5)

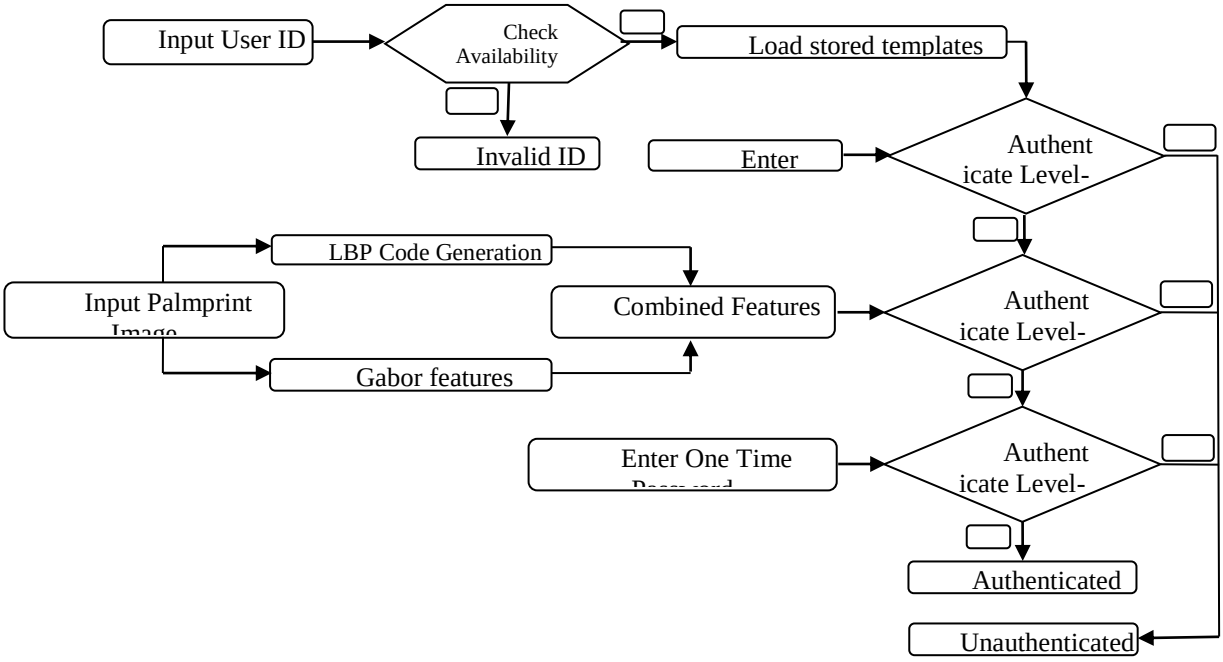

Fig. 3 Authentication Phase

$$FAR = \frac{\text{No.of successful fraud atte}}{\text{Total No.of fraud attemp}} \quad (9)$$

$$FRR = \frac{\text{No.of rejected verification atter}}{\text{Total No.of verification attem}} \quad (10)$$

Input images are taken from CASIA standard palmprint database and the input may contrast with the level and type of texture in a palm image of a person.

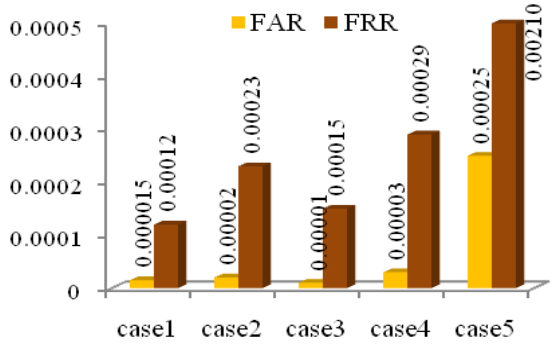

Fig. 4.Performance evaluation of Proposed Method (for different cases)

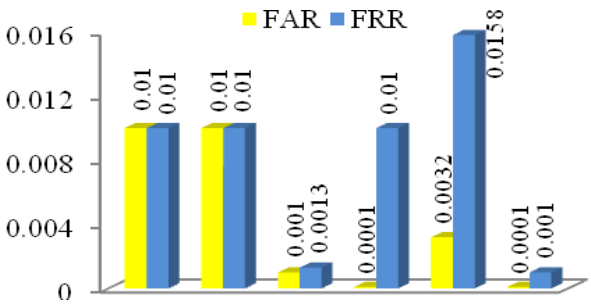

Fig. 5.Comparison of FAR & FRR among Various Method

From the evaluation, it's clear that the proposed system does well at all set of cases and high accuracy is obtained. From the Table 2, it is observed that the proposed method performs well and provides low FAR and FRR.

Table I. FAR & FRR for various cases

Case	No.of Images	FAR	FRR
case1	160	0.000015	0.00012
case2	200	0.00002	0.00023
case3	100	0.00001	0.00015
case4	300	0.00003	0.00029
case5	250	0.00025	0.0021

Table II. Comparison of FAR & FRR among Various methods

Methodology	FAR	FRR
LDP(11)	0.01	0.01
Multimodal (13)	0.01	0.01
K SVM Classifier (14)	0.001	0.0013
Threshold (16)	0.0001	0.01
Gabor based(18)	0.0032	0.0158
Proposed	0.0001	0.001

Table I describes the FAR & FRR values of proposed method for different set of cases. Comparison of FAR & FRR among recent methods are shown in Table II. So it is observed that the proposed method performs well and provides low FAR and FRR

VI.CONCLUSION

This system implements the biometrics, ECC and OTP methodologies to maintain a high level authentication in a network and thus improves the accuracy and efficiency rate. When the performance of the proposed method is compared with some recent methods in term of accuracy and the experimental results show improved performance of the system, effectiveness of our proposed technique. This technique provides the highest accuracy and minimum FAR and FRR.

The future work will be based on the combination of multimodal biometrics (Palm print, fingerprint, Iris) based user authentication using frequency domain approaches.

Likewise privacy& security is a primary concern in Internet of Things (IOT) hence to achieve high security (confidentiality, integrity, authentication), our expected work will be based on multimodal biometrics (fingerprint, palm-print and hand geometry, Iris).Additionally multimodal biometric traits provide promising solutions for continuous user-to-device authentication in high security Internet of Things (IOT). So our future work aims to provide an enhanced level of security by using authentication & intrusion detection. Also Intrusion detection is deliberated as the prevention based approach for securing the Internet of Things (IOT).

REFERENCES

[1] Hong Liu and Yanbing Liu, "Cryptanalyzing an Image Encryption Scheme based on Hybrid Chaotic System and Cyclic Elliptic Curve", In *Optics and Laser Technology*, Elsevier, vol. 56, pp. 15–19, (2014).

[2] S. Maria Celestin Vigila and K. Muneeswaran, "Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications", in *International Journal of Network Security*, vol. 14, no. 4, pp. 236–242, July (2012).

[3] S. Behnia, A. Akhavan, A. Akhshani and A. Samsudin, "Image Encryption based on the Jacobian Elliptic Maps", In *The Journal of System and Software*, Elsevier, vol. 86, pp. 2429–2438, (2013).

[4] Li Li, Ahmed A. Abd El-Latif and XiamuNiu, "Elliptic Curve ElGamal Based Homomorphic Image Encryption Scheme for Sharing Secret Images", In: *Signal Processing*, Elsevier, vol. 92, pp. 1069–1078, (2012).

[5] Don Johnson, Alfred Menezes and Scott Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", *Certicom Corporation*, (2001).

[6] Lo'aiTawalbeh, MoadMowafi and WalidAljoby, "Use of Elliptic Curve Cryptography for Multimedia Encryption", *IET Information Security*, vol. 7, issue 2, pp. 67–74, (2012).

[7] I KetutGedeDarma Putra, Erdiawan, "High Performance Palmprint Identification System Based On Two Dimensional Gabor" TELKOMNIKA Vol. 8, No. 3, pp.309-318, 2010.

[8] Kai Liu; Seungbin Moon "Robust dual-stage face recognition method using PCA and high-dimensional-LBP" IEEE International Conference on Information and Automation (ICIA), 2016

[9] Aditya Nigam; Phalguni Gupta, "Tri-modal biometric fusion for human authentication by tracking Differential Code Pattern" IEEE Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG),2016

[10] Therry Z. Lee; David B. L. Bong," Face and palmprint multimodal biometric system based on bit-plane decomposition approach "IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2016

[11] AkhmadFaizal Akbar; TjokordaAgung Budi Wirayudha; Mahmud DwiSulistiyo, "Palm vein biometric identification system using local derivative pattern", IEEE International Conference on Information and Communication Technology (ICoICT), 2016

[12] RaouiaMokni; MonjiKherallah "Novel palmprint biometric system combining several fractal methods for texture information extraction" IEEE International Conference on Systems, Man, and Cybernetics (SMC), February 2017

[13] R. Parkavi; K. R. Chandeesh Babu; J. Ajeeth Kumar "Multimodal Biometrics for user authentication" IEEE International Conference on: Intelligent Systems and Control (ISCO), 2017

[14] S. Veluchamy; L. R. Karlmarx "System for multimodal biometric recognition based on finger knuckle and finger vein using feature-level fusion and k-support vector machine classifier", IET Biometrics Volume: 6, Issue: 3, 2017

[15] KrishnasreeVasagiri; SudhakarRaoParvata "Dorsal hand vein Biometric authentication using complex Walsh transform", IEEE International Conference on Applied and Theoretical Computing and Communication Technology (ICATCCT), 2017.

[16] Druva Kumar L; Goutham Reddy Alavalapati "Biometric authentication using near infrared hand vein pattern with adaptive threshold technique", "IEEE International Conference on Applied and Theoretical Computing and Communication Technology (ICATCCT),2017.

[17] John Jenkins; Joseph Shelton; Kaushik Roy "One-time password for biometric systems: disposable feature templates"Southeast Con, 2017 ISSN: 1558-058X.

[18] P. Cancian; G. W. Di Donato; V. Rana; M. D. Santambrogio "An embedded Gabor-based palm vein recognition system",IEEE EMBS International Conference on Biomedical& Health Informatics (BHI), 2017.

[19] A.Maheshwari, M. A. DoraiRangaswamy '"Multimodal Biometrics Security System For Authentication" 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM)

About the License