Fuzzy Rule Based Enhancement of Patten Lock Security System

[1]Pawan Kumar and [2]Prof. Vipin Saxena
[1]pawan0871@gmail.com, [2]profvipinsaxena@gmail.com
Department of Computer Science, Babasaheb Bhimrao Ambedkar University Lucknow, (U.P.), 226025, INDIA

ABSTRACT

Pattern lock system is a graphical password system. In earlier, pattern lock system used only Android operating system but now days many platforms offer pattern lock system such as some websites, Unified Payment Interface (UPI) and mobile applications. The use of pattern lock to access to any hand-held device is increasingly because of simple to use and extremely easy to remember. Therefore, many of user of hand-held devices systems, mainly in Android-based mobiles. In the proposed work, fuzzy concept is used to secure the pattern lock and further Pseudo Random Number Generator and Elgamal Encryption and decryption are used and computed results are depicted in the form of graphs.

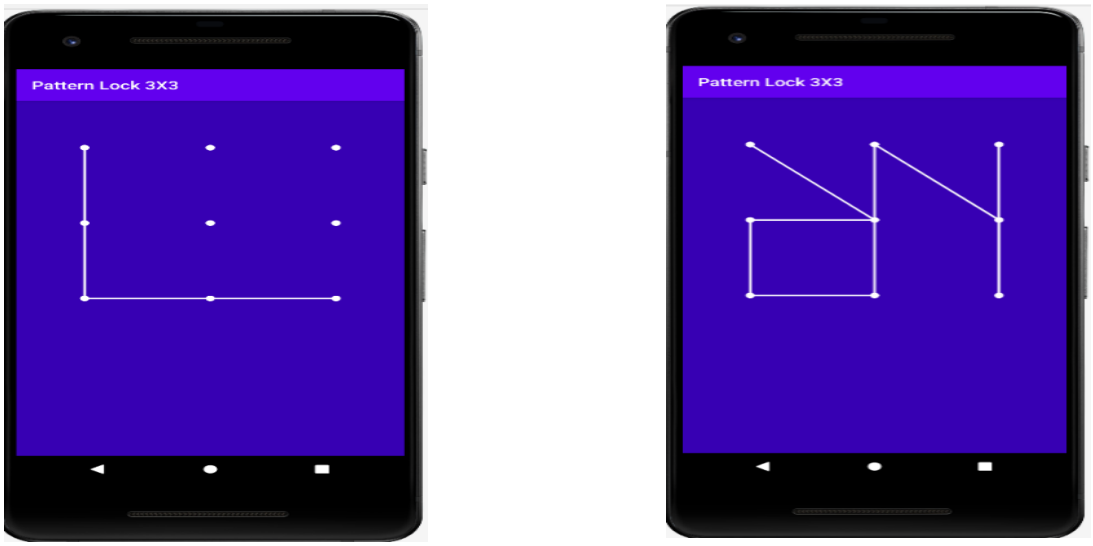
Keywords: **Pattern Lock, Fuzzy, Pseudo Random Number Generator, Elgamal, Encryption and Decryption.**

DOI Number: 10.48047/NQ.2022.20.16.NQ88164 **NeuroQuantology2022;20(16):1651-1661**

1. INTRODUCTION

In the present scenario, use of electronic gadgets has become an integral part of the life of everyone. Due to digitization in every field, the uses of hand-held devices has been increased for accessing the simple and complex information in terms of the text, audio and video formats. Since, the gadgets are attached across the distributed network system, hence security of the devices play an important role, when, one is accessing the device in online mode. Users can use the different services in terms of financial and social networking. The numbers of smart devices applications have already been increased in terms of Apps for faster access of the applications by the use of smart devices. One of the kinds of smart devices is the mobile device and daily users on the mobile devices are increasing and using the smart phone applications. On the other hand, smart phone applications are extremely diverse and sometimes misunderstood, particularly in terms of privacy and security related to various activities. Due to this reason, there is always fear of data theft and other security issues across the network while using the smart devices.

For the security purpose of the smart device, pattern lock is the most popular security aspect for identification of the valid user. It contains the graphical pattern which may be simple in which all nodes may or may not covered and complex pattern in which all nodes must be covered. Authorised users can set the pattern on the smart device while sometimes textual authentication is also used by the users. The simple and complex patterns are shown below in the Fig. 1(a) and (b), respectively.



(a) Simple Pattern **(b)** Complex Pattern

Fig. 1: Representation of Graphical Pattern

Behavior-based human authentication scheme is proposed by Shahzad et al. [1]. The proposed method identifies the typical or potential pattern lock which has been obtained through security concept. In the year 2017, Ye et al. [2] developed a technique for cracking the pattern lock based on the android operating system and applied only five attempts to crack the pattern lock. Cha et al. [3] have employed a technique which can boost guessing the attack performance on the mobile devices which has android operating system. In the technique, smudges are detected and applied for computation of all potential segments which form the pattern locks. Ku et al. [4] have proposed a method for designing the pattern locks based upon the behavior of human being and it is only applicable on the mobile devices and can construct the own pattern lock. The algorithm clearly constructs and authenticates the public pattern by using the segments, angles, orientations, etc. The acoustic signals are used for cracking the android device through fingertip motion. The concept of ciphering and deciphering were used by the android for removing dynamics, static interface and splitting acoustic [5]. Li et al. [6] have proposed a technique based on the authentication over the screen of android handheld device. The proposed concept has high-performance rate with unique biometric qualities and best suited for individual identification. Khan et al. [7] have developed a Wake-Lock system in the year 2021 for android device and the concept of machine learning were used in the Wake-Lock system through Application Programming Interface (API).

Vazirani and Impagliazzo [8, 9] proposed the six theorems for generation of random number sequences by the use of XOR state and pseudo random numbers which are generated in such a way that these numbers can be safeguard. Boyer [10] proposed a linear congruential technique for security of the linear congruences with n terms in the repetition and quadratic congruences, and also find out that whetherPseudo-Random Number may be weak or strong. Barak and Halevi [11] developed a formal model for reliable pseudo random number generator which can be used for development of private authenticate model. Petit et al. [12] proposed a block cipher-based technique for secure generation of pseudo number and can be used as a side-channel key recovery. In the year 2010, Pseudo-Random Number Generator had improved efficiency by use of Chaotic Tent Map [13, 14]. A new quantum logisticmap-based approach for

generating excellent PRNG was proposed by Akhshani et al. [15]. Dodiset et al. [16] employed a cryptographic algorithm that produces the random numbers from a constant inner state and which are updated with an outer random source. This method enhanced the Barak and Halevi (BH) prototype to incorporate a latest safety feature. Hybrid Pseudo-Random numbers (HPRN) were presented and can be used for the cryptography technique. Since these numbers are based upon the non-linear system. Therefore, it has less danger by adding extra inputs to the transition and outcome mechanisms included in a raw PRNG [17]. Rastogi et al. [18] have developed an algorithm to generate Linear Congruential Pseudo-Random Number Generator with encryption and decryption technique which can be employed for the multi-layered strategy. In the outer layer, a randomly generated sequence has implanted in the text file and thereafter the contents were sent to produce the encrypted text file. Encryption for the message which are received in the first layer. Baldanzi et al. [19] have proposed a cryptography secure pseudo-random number which can be digital hardware used to accelerate in the generation of random numbers and further those can be used in the cryptography method. For better timing performance and greater throughput one can use a random number generator with cryptography algorithm pseudo-random number.

Elgamal [20] has developed a public-key cryptography method based on the key exchange technique and revealed the discrete logarithms over the finite fields. Hwang et al. [21] have combined Diffie-Hellman and Elgamal algorithms together for encryption and decryption which worked for large-size of messages, while Grewal [22] has suggested an approach that employed over the three-dimensional chaotic maps to generate keys for the use in the Elgamal algorithm for encryption and decryption. The time spent encryption and decryption were evaluated and compared to approach using one and two-dimensional chaotic maps. The help of Elgamal and Chaotic map generated the public and private keys. Ara et al. [23] have proposed a method which has data gathering efficiency and data confidentiality and further improved by the use of secure privacy-preserving information sets. Arboleda[24] has also proposed a technique to enhance the system that combines two current encryption schemes and the development hybrid cryptography method with the help of Elgamal and fast chaos cryptography.

In the present work, a secure Pattern lock technique is proposed for opening the hand-held devices and transfer of encrypted information from one device to another device. A system model is proposed and results have been obtained through Python programming language.

2. METHODOLOGY

In the present work, a user is registered on the new mobile device and for the security of device, a graphical pattern is to be set by the registered user. Therefore, the first step is to register the authentic mobile user and thereafter authentication and validation of pattern are applied. A system model is developed and shown below in the following Fig. 2.

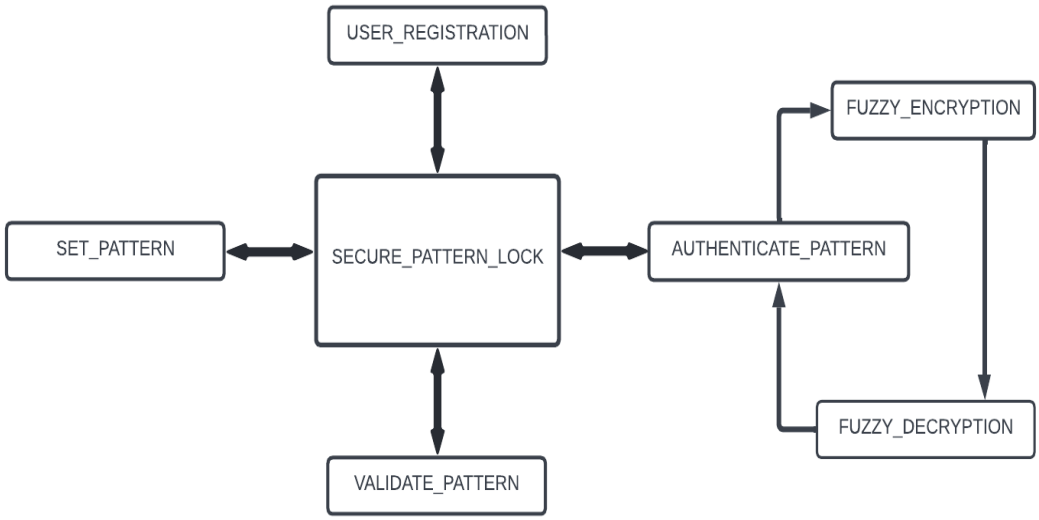


Fig. 2: System Model for Secure Pattern Lock

In the above Fig., securing the pattern lock contains the following major activities.

- Registration of User [USER_REGISTRATION ( )]
- Setting the Device Pattern [SET_PATTERN ( )]
- Authentication of Pattern [AUTHENTICATE_PATTERN ( ), FUZZY_ENCRYPTION ( ), FUZZY_DECRYPTION ( )]
- Validate of Pattern [VALIDATE_PATTERN ( )]

The above four activities are described below in brief:

2.1. USER_REGISTRATION ( )

User may have any hand-held device which may be laptop, tablet, mobile or any touch screen devices, etc. and these devices are well connected via distributed network system having internet services. The connected devices under the distributed environment are shown below in Fig. 3. Normal desktop may be attached through distributed environment in which users can set pattern through mouse.

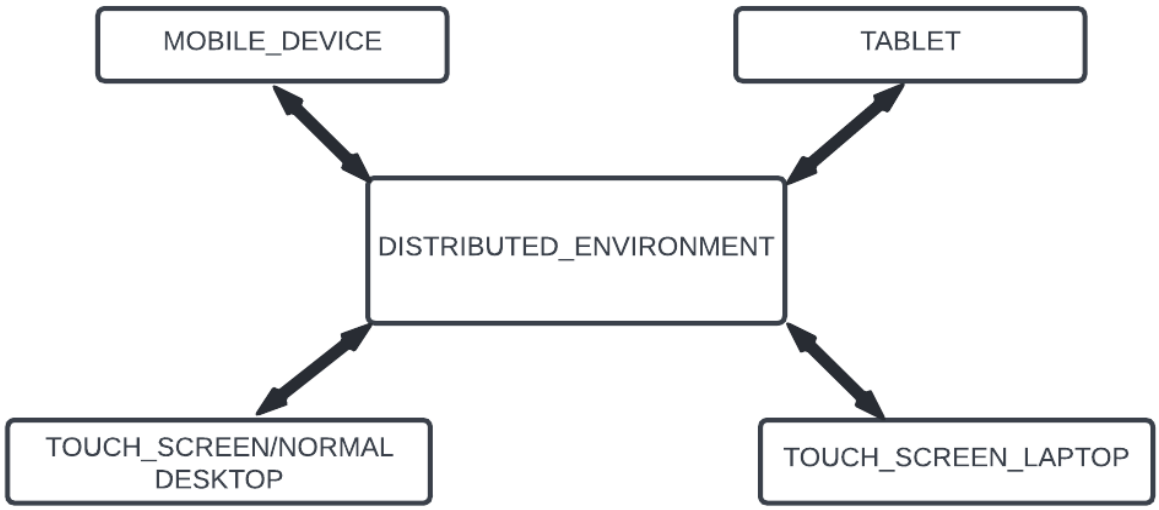


Fig. 3: Distributed Environment of Hand-held Devices

In the above Fig., the devices have different configuration in term of ram, disk space (internal / external storage) etc. The user can register the identity on any of these devices by the use of following Fig. 4.

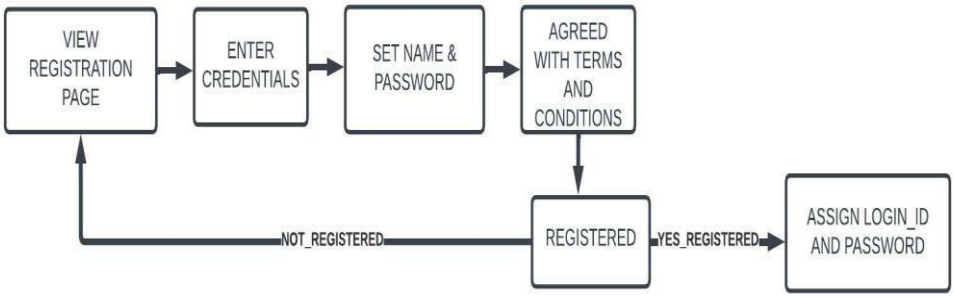


Fig.4: User's Registration Process

2.2. SET_PATTERN ( )

After completing the registration process on any of hand-held device**,** the user has to set pattern by the use of 3*3 matrix. In the present work, user selected the mobile device and after entering the credentials in term of LOGIN_ID and PASSWORD, user has to set pattern as represented below.

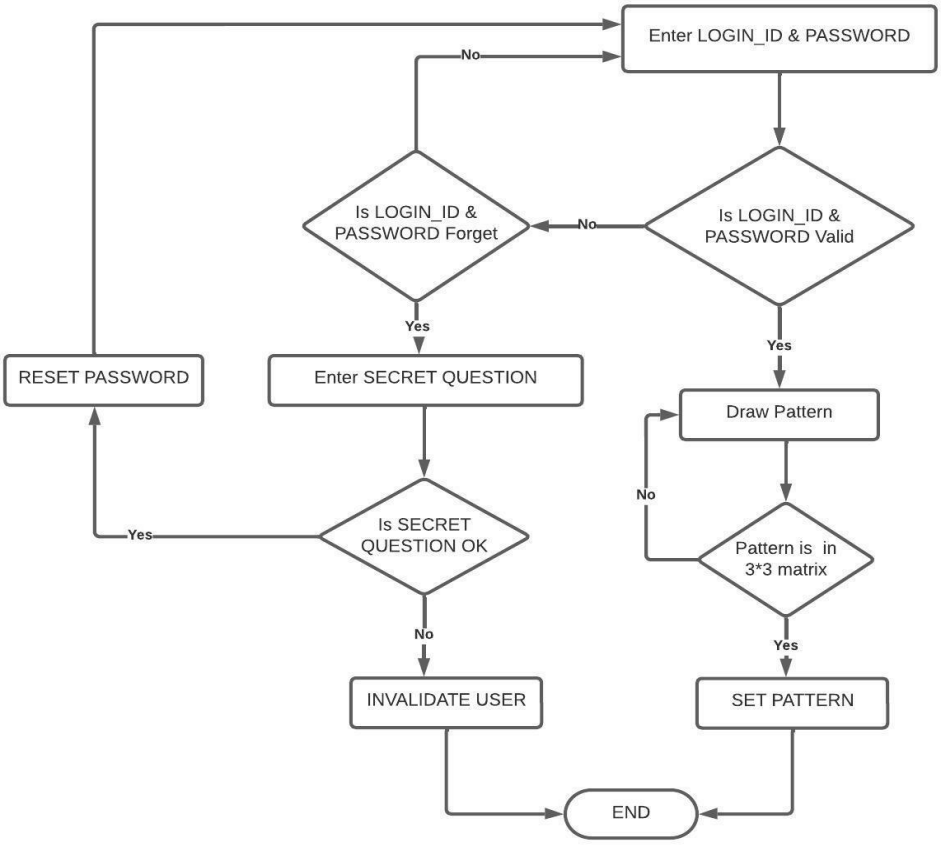


Fig. 5: Set Pattern Process

2.3. AUTHENTICATE_PATTERN ( )

This activity checks the information about the user, which wants to access the connected device and it must be connected via distributed network system having internet services. This activity checks the user's credentials such that the LOGIN_ID, PASSWORD, and pattern.

2.4. VALIDATE_PATTERN ( )

After authentication activity is completed, next activity is validation of the pattern. This activity validates that the user draws correct pattern or not.

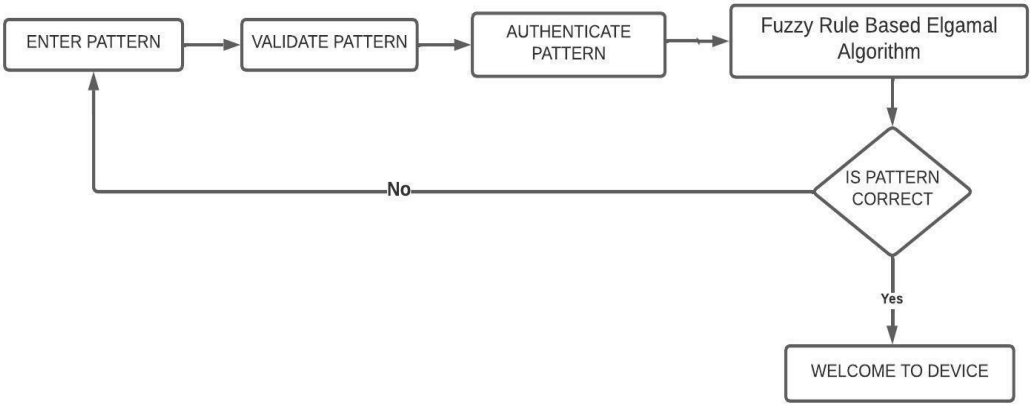


Fig. 6: Validation Process of Pattern Lock

The proposed model provides secure pattern lock mechanism, and the proposed technique two type of encryption and decryption technique which are well explained in the subsequent section.

3. FUZZY RULE-BASED VALUE COMPUTATION

The Triangular membership function for generates the fuzzy value, which is based on number of selected dots while entering the pattern given by the user. The resultant of this will be Pseudo Random Number which is generated through following algorithm.

Fuzzy_computation(SD, $M_{function}$, M_{rule})
SD ← number of selected dots
$M_{function}$ (M_{low}, M_{medium}, M_{high})
F_{rule} ← set of rule
fuzzy_compute_value ← TMF(SD)
END

Based on antecedent (input) variables define membership function as M_{low},M_{medium}, M_{high} and fuzzy rules. All of the defined variables and set of rules given *TMF(SD)* function. *TMF(SD)* function produce result based on number of selected dots and output value stored in *fuzzy_compute_value*variable. The *fuzzy_compute_value*variable value sent to next sub- section.

The activity diagram for fuzzy rule based value computation shown below:

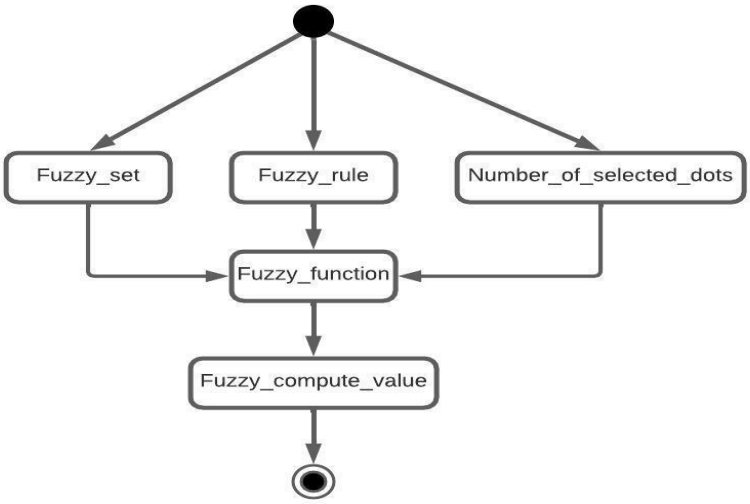


Fig. 7: Activity Diagram of Fuzzy Rule Based Value Computation

This algorithm has three main parts, first is fuzzy set, second is fuzzy rule and third is number of

selected dots. In the first step, all three functions are defined then give these value give Fuzzy function for fuzzy compute value.

To generate the pseudo random number, Linear congruential generator technique is used. In used the seed value is taken by the selected dots value during pattern draw and also replaced the modules value by the final output of fuzzy rule base value computation. The pseudo random number generator runs the fixed number of times which is 5 in this test for each selected dot.

The steps for pseudo random number generator are given below:

PRNG(pattern$_{sequence}$[p], fuzzy_compute_value,)
Seed$_{value}$←Pattern$_{Sequence[p]}$
Modlus$_{Parameter}$←fuzzy_compute_value
Define multiplier, increment term and number of rounds
A←Multi$_{Value}$
Inc←Inc$_{Term}$
Round ←Number of rounds
FOR 1 to round
RandNum[] ←[A Seed$_{Value}$+C] MOD Modlus$_{Parameter}$*
END FOR
END

In the first step given seed *Seed$_{value}$* and taken *fuzzy_compute_value*from *Fuzzy_computation*function.The*fuzzy_compute_value*value is assign to *Modlus$_{Parameter}$*. defined multiplier *A,* increment term *Inc* and number of rounds as *round*. Run five times for each seed.

The activity diagram for pseudo random generator is given below:

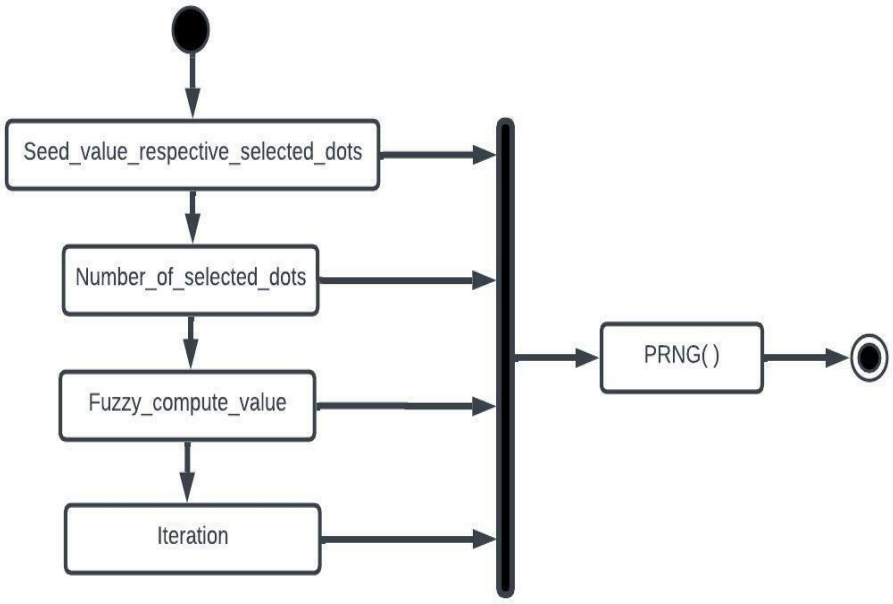


Fig. 8: Activity Diagram for Pseudo Random Number Generator

The Elgamal algorithm is a public key cryptography which use the different keys for encryption and decryption. In this algorithm we have used the output of pseudo random number generator algorithm is connected as a input of Elgamal Cryptosystem. The pseudo code of this algorithm given below:

Elgamal_algo(msg)
*P←Large prime number, (Q ∈ group G <Z*p, A>)*
*X ←Y, (X ∈ group G <Z*p, A>& 1 ≤ X ≤ P -2)*

*Pr ←Primitive root in G <Z*p, A>*
B =Pr^X MOD P
Pub_Key=(Pr, B, P)
Pri_Key = X
ENCRYPTION
*Rdmn←Random Number, (R ∈ group G <Z*p, A>& 1 ≤ Rdmn ≤ P-1)*
Ctext1=Pr^{Rdmn} MOD P
Ctext2= (msg × B^{Rmdn}) MOD P
DECRYPTION
MSG= [Ctext2(Ctext1^X)$^{-1}$] MOD P
END

Define large prime number *P*, choose any random number *X* and primitive root *Pr* in cyclic group *G <Z*p, A>.* After all the parameter defined then calculate *B = Pr^X mod P.* Public key is *(Pr, B, P)* and private key is *X.* For encryption, taken a random number *Rdmn* which belong to *group G <Z*p, A>.* Then calculate *Ctext1 = Pr^{Rdmn}mod P* and *Ctext2 = (msg ×B^{Rdmn}) mod P*. In decryption, calculate *MSG = [Ctext2(Ctext1^X)$^{-1}$] mod P*.

4. RESULTS AND DISCUSSION

The primary goal of the proposed work algorithm is provided high level of access control to avoid illegal activities from the hand-held devices. In the proposed model, we have used three phases to enhance the security. In the first phase, fuzzy rule base value computation is used to get fuzzy value for number of selected dots during pattern set. The generated fuzzy value send to the next phase random number generator. This model pseudo random number generator selects dots value. In the next phase, encryption and decryption are perform to receive output of value pseudo random generator using Elgamal cryptosystem.

Lets take an example of proposed model if any user set a pattern sequence [11, 21, 31, 32,22, 23, 12, 13, 33] which is given in Fig. 9.



Fig. 9: Complex Pattern Lock and selected each dot

The model counted number of selected dots which is nine. The Triangular membership function take nine as an input, and generate crisp value 6.

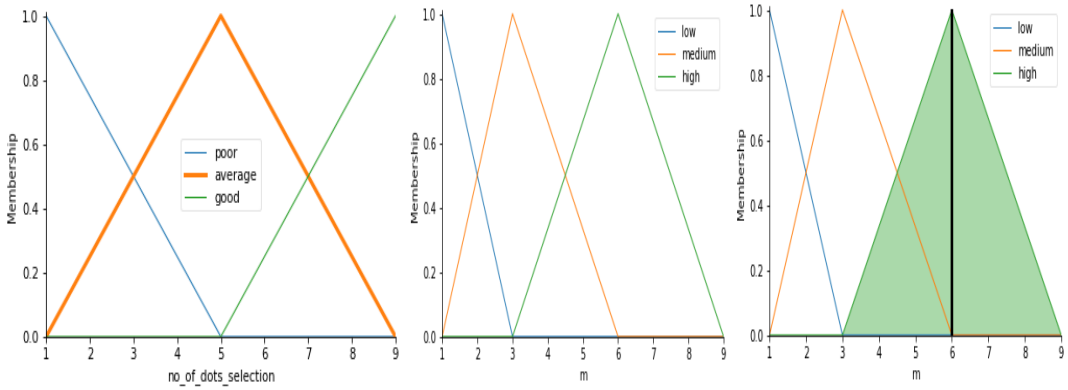


Fig. 10: Triangular Membership Function (A) Fuzzy Set, (B) Fuzzy Rule and (C) Fuzzy Computation

The PRNG takes value as input and generate a random number for every selected dot. The generated random number encrypted by the Elgamal algorithm and get the final ciphertext of selected dots. Hence as per comparison with the previous provided algorithms, the proposed

algorithm high level of security and better performance.

5. CONCLUSIONS AND FUTURE SCOPE

In this paper, we proposed fuzzy rule basedElgamal algorithm. Which provides Elgamal cryptosystem with the help of fuzzy logic and pseudo random number generator for patten lock system. The proposed algorithm improves security and useability of hand-held devices. In the future this algorithm can be used in text based password system. In text based password system, number of characters given as input in fuzzy computation and iteration term can be increased in pseudo random number generator.

REFERENCES

1. Shahzad M, Liu AX, Samuel A. Behavior based human authentication on touch screen devices using gestures and signatures. *IEEE Transactions on Mobile Computing*. 2016 Dec 7;16(10):2726-41.DOI: 10.1109/TMC.2016.2635643
2. Ye G, Tang Z, Fang D, Chen X, Kim KI, Taylor B, Wang Z. Cracking android pattern lock in five attempts. *In Proceedings of the 2017 Network and Distributed System Security Symposium 2017 (NDSS 17) 2017 Feb 26*. *Internet Society.https://doi.org/10.14722/ndss.2017.23130*
3. Cha S, Kwag S, Kim H, Huh JH. Boosting the guessing attack performance on android lock patterns with smudge attacks*. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. 2017 Apr 2 (pp. 313-326).https://doi.org/10.1145/3052973.3052989
4. Ku Y, Park LH, Shin S, Kwon T. Draw it as shown: Behavioral pattern lock for mobile user authentication. *IEEE Access*. 2019 May 23;7:69363-78.https://DOI: 10.1109/ACCESS.2019.2918647
5. Zhou M, Wang Q, Yang J, Li Q, Jiang P, Chen Y, Wang Z. Stealing your android patterns via acoustic signals. *IEEE Transactions on Mobile Computing*. 2019 Dec 19.https://DOI: 10.1109/TMC.2019.2960778
6. Li Q, Dong P, Zheng J. Enhancing the security of pattern unlock with surface EMG-based biometrics. *Applied sciences.* 2020 Jan;10(2):541.https://doi.org/10.3390/app10020541
7. Khan MU, Lee SU, Abbas S, Abbas A, Bashir AK. Detecting Wake Lock Leaks in Android Apps Using Machine Learning. *IEEE Access.* 2021 Sep 3;9:125753-67. https://DOI:10.1109/ACCESS.2021.3110244 0/app10020541
8. Vazirani UV, Vazirani VV. Efficient and secure pseudo-random number generation*. In Workshop on the Theory and Application of Cryptographic Techniques.* 1984 Aug 19 (pp. 193-202). *Springer, Berlin, Heidelberg*.https://doi.org/10.1007/3-540-39568-7_17
9. Impagliazzo R, Levin LA, Luby M. Pseudo-random generation from one-way functions. *In Proceedings of the twenty-first annual ACM symposium on Theory of computing*. 1989 Feb 1 (pp. 12-24).https://doi.org/10.1145/73007.73009
10. Boyar J. Inferring sequences produced by pseudo-random number generators*. Journal of the ACM (JACM).* 1989 Jan 1;36(1):129-41.https://doi.org/10.1145/58562.59305
11. Barak B, Halevi S. A model and architecture for pseudo-random generation with applications to/dev/random. *In Proceedings of the 12th ACM conference on Computer and communications security.* 2005 Nov 7 (pp. 203-212).https://doi.org/10.1145/1102120.1102148
12. Petit C, Standaert FX, Pereira O, Malkin TG, Yung M. A block cipher based pseudo random number generator secure against side-channel key recovery. *In Proceedings of the 2008 ACM symposium on Information, computer and*

*e*ISSN1303-5150



*communications securit*y. 2008 Mar 18 (pp. 56-65).https://doi.org/10.1145/1368310.1368322

13. N. K. Pareek, V. Patidar, and K. K. Sud, "A Random Bit Generator Using Chaotic Maps," *IJ Network Security*, vol. 10, pp. 32-38, 2010.
14. A. B. O. López, G. A. Maranon, A. G. Estévez, G. P. Dégano, M. R. García, and F. M. Vitini, "Trident, a new pseudo random number generator based on coupled chaotic maps," in *Computational Intelligence in Security for Information Systems 2010, ed: Springer,* 2010, pp. 183-190.https://doi.org/10.1007/978-3-642-16626-6_20
15. Akhshani A, Akhavan A, Mobaraki A, Lim SC, Hassan Z. Pseudo random number generator based on quantum chaotic map. *Communications in Nonlinear Science and Numerical Simulation.* 2014 Jan 1;19(1):101-11.https://doi.org/10.1016/j.cnsns.2013.06.017
16. Dodis Y, Pointcheval D, Ruhault S, Vergniaud D, Wichs D. Security analysis of pseudo-random number generators with input: /dev/random is not robust. *In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security.* 2013 Nov 4 (pp. 647-658).https://doi.org/10.1145/2508859.2516653
17. Avaroğlu E, Koyuncu I, Özer AB, Türk M. Hybrid pseudo-random number generator for cryptographic systems. *Nonlinear Dynamics*. 2015 Oct;82(1):239-48.https://doi.org/10.1007/s11071-015-2152-8
18. Rastogi R, Mittal S, Shekhar S. Linear algorithm for imbricate cryptography using pseudo random number generator. *In 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom).* 2015 Mar 11 (pp. 89-94). *IEEE*.
19. Baldanzi L, Crocetti L, Falaschi F, Bertolucci M, Belli J, Fanucci L, Saponara S. Cryptographically secure pseudo-random number generator IP-core based on SHA2 algorithm. *Sensors.* 2020 Jan;20(7):1869.https://doi.org/10.3390/s20071869
20. Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory.* 1985 Jul;31(4):469-72.DOI: 10.1109/TIT.1985.1057074
21. Hwang MS, Chang CC, Hwang KF. An Elgamal-like cryptosystem for enciphering large messages. *IEEE Transactions on Knowledge and Data Engineering.* 2002 Aug 7;14(2):445-6.DOI: 10.1109/69.991728
22. Grewal JK. Elgamal: Public-Key Cryptosystem. *Math and Computer Science Department, Indiana State University.* 2015 Sep.
23. Ara A, Al-Rodhaan M, Tian Y, Al-Dhelaan A. A secure privacy-preserving data aggregation scheme based on bilinear Elgamal cryptosystem for remote health monitoring systems. *IEEE Access.* 2017 Jun 22;5:12601-17.DOI: 10.1109/ACCESS.2017.2716439
24. Arboleda ER. Secure and fast chaotic Elgamal cryptosystem. *Int. J. Eng. Adv. Technol.* 2019;8(5):1693-9.

*e*ISSN1303-5150

