On atypical approaches for privacy preserving using multi-dimensional geometric object based intelligent cryptography for modern applications

Pruthvi Kumar K R
Assistant Professor, Department of ISE,
Jyothy Institute of Technology, Bengaluru, Karnataka, India

Anjan Krishnamurthy
Associate Professor, Department of CSE,
BMSIT&M, Bengaluru, Karnataka, India

Harsha S
Associate Professor, Department of ISE,
Jyothy Institute of Technology, Bengaluru, Karnataka, India

Khalid Nazim S A
Assistant Professor, Department of CSI,
College of Science, Majmaah University, Majmaah 11952,Saudi Arabia,

Abstract - A nature of network in communication and data collection from the age of microchip to latest cloud stores. The present storage in the data collection is very huge in quintillion bytes of data every day. A machine learns by itself to perform intelligent operation to solve modern day problem. The application used in mundane activities like E-mail, Banking, Medical, Facial Recognition, weather report and so on needs large data storage. The feature extraction on the above data needs machine learning techniques to train and test the outcome for better visualization. The search space and large data processing are the common attributes in machine learning. These features are shared by most powerful and popular field of cryptography, which focuses on data integrity, authenticity, and security. The main focus of cryptography is to secure data with huge volume using standard security algorithms either in symmetric or asymmetric approach. This paper mainly focuses on blend of cryptography with machine learning as new approach to provide better and intelligent security. The approach used here is using geometric shapes in multi-dimension for cryptologic purpose. The paper proposes an intelligent cryptosystem which can evolve overtime and suitably take decision on environmental conditions. The system is theoretical explained through modern applications illustrating the need for such approach.

Index Terms— Cryptography, Intelligent cryptosystem, Machine learning, Multi-dimensional geometry.

I.INTRODUCTION

In recent years, since the advent of Machine learning as a branch of artificial intelligence, every field has extended demand to use it for one or the other application to enhance their performance or domains. Cryptography is no exception. Many researchers over the past decade have attempted combining cryptography with machine learning at some level. However, most of the works done in this area have concentrated on having multiple cryptosystems and using them through a machine learning framework.

The applications of these domains have a demand created by its volume and its features. The machine learning will provide optimum solution for any application for example the spam detection algorithm will not generate 100% accurate results in searching spam. The data files which are spam and non-spam are fed into machine in large scale to obtain optimal solution. So in general the machine needs more training to learn and provide accurate results. there are many applications of machine learning techniques are used in business, trade market, Walmart's to find the best prediction based on analysis.

The mark of cryptography in the field of science is to prove that any data of any form (Text, Image, Audio, Video, Numerical ... etc) in data communication is secured. The hallmark of cryptosystem is to conversion of data from plain to cipher and cipher to plain with or without the support of key. The key generation is done using two either symmetric approach (private key system), or asymmetric approach(public key system). The holy grail of this cryptosystem uses a new geometric approach to provide long lasting environment.

In this research an attempt has been made to extend the reach of machine learning into cryptosystem, by developing a seamless integration of the two using multi-dimensional geometric shapes.

II. RELATED WORKS

The Environment of secured intelligent system should have a collaboration and understanding for mutual learning in communication 1], this nature of learning helps in generating symmetric key which makes impenetrable of eavesdroppers. This phenomenon of mutual learning in cryptography makes it impossible to break the keys at either ends.

A "Boosting" Technique[2] in both machine learning and cryptography is mainly introduced to extract more potential data from the learning algorithm and merge them to a intelligent device in a secured form to build the reliable environment. The homomorphic encryption Approach [3] in both the domains was introduced for perform high speed activity in Machine learning by maintaining confidentiality by implementing Cloud for large data storage.

The cryptography when combined with machine learning can use symmetric or asymmetric approach for encryption and decryption. In symmetric approach[4] where the common key the data is converted in to cipher text in the form of bits and sent through neural networks as plain text the output is extracted by applying Machine learning unsupervised technique which helps in classifying the plain text in an efficient manner.

The history of different types of attacks on multiple environment has led to build more complex secured intelligent system. If there is a side-channel attack using machine learning algorithm[5] was based on system implementation rather than algorithm like software bug. can be secured using Least Squares Support Vector Machine(LS-SVM) learning algorithm instead of using AES. A same problem of side-channel attack which rely on hardware implementation[6] can be relaxed using machine learning algorithm to improve the accuracy of a channel.

An approach of cryptanalysis[7] where the hacker proved intelligence to neural network where the cipher text is decrypted without decryption key which reduced time and the network configuration was also modified to get high accuracy. The encrypted network traffic is where there is eavesdrop on encrypted Traffic[8].the collection is then analyzed by applying advanced machine learning algorithms to achieve highest accuracy level in identifying the user activity.

The machine learning builds a model where it learns from training data and is been tested with implementing many techniques to visualize the output. The attacks on machine learning techniques are listed in taxonomy[9]which can attack against targeting spam and statistics filters. The evasion attack[10] which injects adversarial data to training data in machine learning to extract statistical information. The meta- classifier was build and trained to hack other classifiers and obtain information. This kind of attack drives to extract information of others engaged with the current technology drivers.

The adversarial settings [11] attacked the privacy and integrity of the system this are few attacks where we need to build a new model that achieves robust and privacy preserving features.

III. METHODOLOGY

In this paper, we have adopted an ikert scale from 1 to 3 for a solution being weak or strong respectively. The table shows the method with which the scale is allotted to different methods. As it can be seen most of the research focused only on combining machine learning and cryptography but not enough effort has been put on, introduction of complex yet faster computation into cryptography based on various requirements.

Table 1. Comparative analysis of existing cryptosystems

Title	Author	Year	ML based Technique	Crypto graphy	Level
Mutual learning in a tree parity machine and its application to cryptography	M. Rosen-Zvi, E. Klein, I. Kanter, and W. Kinzel,	2002	Yes	Yes	2
Machine learning based encrypted traffic classification: Identifying ssh and skype	R. Alshammari and A. N. Zincir-Heywood	2009	Yes	Yes	2
Adversarial machine learning,	L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. Tygar	2011	Yes	No	1
Machine learning on encrypted data	T. Graepel, K. Lauter, and M. Naehrig	2012	Yes	Yes	2
Machine learning classification over encrypted data	R. Bost, R. A. Popa, S. Tu, and S. Goldwasser	2015	Yes	Yes	2
Power analysis attack: an approach based on machine learning	L. Lerman, G. Bontempi, and O. Markowitch	2014	Yes	Yes	2
"Neuro-cryptanalysis of DES and triple-DES	M. M. Alani	2012	No	Yes	3
Breaking cryptographic implementations using deep learning techniques,	H. Maghrebi, T. Portigliatti, and E. Prouff	2016	Yes	Yes	2
Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers	G. Ateniese, G. Felici, L. V. Mancini, A. Spognardi, A. Villani, and D. Vitali	2013	Yes	No	1
Towards the science of security and privacy in machine learning,	N. Papernot, P. McDaniel, A. Sinha, and M. Wellman,	2016	Yes	Yes	2
Pythocrypt- A Crypto System For Medical Images	Harsha S ,N Bhaskar, Chandan CM	2013	No	Yes	1
Performance Analysis of Hybrid Cryptographic Algorithm- A 3D Algorithm	Anjan K Koundinya , Abhijith C , Arunraj , Deekshith N4, Srinath N K , Jibi Abraham	2016	No	Yes	1
A 3-d advancement to Pythocrypt for any file type [12]	Harsha S, N Bhaskar, Sheshaprakash M N, G Raghavendra Rao	2016	Yes	Yes	3

The Secured intelligent system is categorized in to three level where the level 1 to 3 (weak, moderate, strong) as shown in table 1. The combination of machine learning and cryptography is assigned to level 2 and is set to level 1 if focused on one area. The level 3 is best suited only in the case of complex operation on data visualization in an infrangible Environment.

IV. CONCLUSION

The future of the modern world is almost dependent on autonomous intelligent system which hardly in need of security at peak level. This paper proposes the idea of integrating intelligent systems with cryptography with the knowledge of mathematical geometry using multi-dimensional feature.

The main reason for choosing the Geometry for cryptography is it computes the encryption and decryption based on geometric attributes and the key size is large when compared with the other cryptographic algorithms like RSA, AES, etc. the cryptanalysis in secured intelligent system proves to reach level 3(ref table 1) by adopting the nature of systems feature.

.

REFERENCES

[1] M. Rosen-Zvi, E. Klein, I. Kanter, and W. Kinzel, "Mutual learning in a tree parity machine and its application to cryptography," Physical Review E, vol. 66, no. 6,p. 066135, 2002

[2] A. Blum, "Machine learning theory," Carnegie Melon University, School of Computer Science, p. 26, 2007.

[3] R. Alshammari and A. N. Zincir-Heywood, "Machine learning based encrypted traffic classification: Identifying ssh and skype," in Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on, pp. 1–8,IEEE, 2009.

[4] V. Sagar and K. Kumar, "A symmetric key cryptographic algorithm using counter propagation network (cpn)," in Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, p. 51,ACM, 2014

[5] G. Hospodar, B. Gierlichs, E. De Mulder, I. Verbauwhede, and J. Vandewalle, "Machine learning in side-channel analysis: a first study," Journal of Cryptographic Engineering, vol. 1, no. 4, p. 293, 2011.

[6] L. Lerman, G. Bontempi, and O. Markowitch, "Power analysis attack: an approach based on machine learning," International Journal of Applied Cryptography, vol. 3, no. 2, pp. 97–115, 2014.

[7] M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, "Analyzing android encrypted network traffic to identify user actions," IEEE Transactions on Information Forensics and Security, vol. 11, no. 1, pp. 114–125, 2016.

[8] H. Maghrebi, T. Portigliatti, and E. Prouff, "Breaking cryptographic implementations using deep learning techniques," in International Conference on Security, Privacy, and Applied Cryptography Engineering, pp. 3–26, Springer, 2016

[9] M. Barreno, B. Nelson, A. D. Joseph, and J. D. Tygar, "The security of machine learning," Machine Learning, vol. 81, no. 2, pp. 121–148, 2010.

[10] B. Biggio, I. Corona, D. Maiorca, B. Nelson, N. Šrndić, P. Laskov, G. Giacinto, and F. Roli, "Evasion attacks against machine learning at test time," in Joint European conference on machine learning and knowledge discovery in databases, pp. 387–402,Springer, 2013.

[11] N. Papernot, P. McDaniel, A. Sinha, and M. Wellman, "Towards the science of security and privacy in machine learning," arXiv preprint arXiv:1611.03814, 2016.

[12] Harsha S. Jois, N Bhaskar and M N Shesha Prakash , "A 3-d advancement of PythoCrypt for any file type", Jois et al. Journal of Open Innovation: Technology, Market, and Complexity (2015) 1:19DOI 10.1186/s40852-015-0022-8

[13] Anjan K Koundinya , Abhijith C , Arunraj , Deekshith N4, Srinath N K , Jibi Abraham," Performance Analysis of Hybrid Cryptographic Algorithm- A 3D Algorithm", International Journal of Innovative Research in Computer and Communication Engineering. ISSN ISBN: 2320-9801 in 2016

[14] Mr. Harsha S, Mr. Shailesh Kumar, Dr. Khalid Nazim Abdul Sattar, Dr. Keshava Prasanna& Mr. Shantanu A D, "Chaotic Sequence based Steganography for Pair-Wise Communication", Global Journal of Computer Science and Technology: ENetwork, Web & Security Volume 16 Issue 2 Version 1.0 Year2016