Various Approaches towards Cryptanalysis

Shaligram Prajapat
MANIT Bhopal and IIPS DAVV Indore
India

Ramjeevan Singh Thakur
MANIT, Bhopal, India

ABSTRACT
Cryptanalysis is very important step for auditing and checking strength of any cryptosystem. Some of these cryptosystem ensures confidentiality and security of large information exchange from source to destination using symmetric key cryptography. The cryptanalyst investigates the strength and identifies the weakness of the key as well as enciphering algorithm. With the increase in key size, the time and effort required predicting the correct key increases. So, the Trend of increasing key size from 1 Byte to 8 Bytes to strengthen the cryptosystem and hence algorithm continues with compromise on the cost of time and computation.

Automatic Variable Key (AVK) based symmetric key cryptosystem is an alternative to this style by fixing up key size and adding security level direction. Whenever any new cryptographic method is invented to replace existing vulnerable cryptographic method, it's deep analysis from all perspectives (Hacker / Cryptanalyst as well as User) is desirable and proper study and evaluation of its performance is must. New cryptic techniques may exploit benefits of advances in computational methods like ANN, GA, SI etc. These techniques for cryptanalysis are changing drastically to reduce cryptographic complexity. In this paper a detailed survey and direction of development work has been conducted. The work compares these new methods with state of art approaches and presents future scope and directions from the cryptic mining perspectives.

Keywords
cryptanalysis, Hacker, AI, Genetic Algorithm, Swarm Intelligence, cipher, neural network, cryptography, Artificial Neural Networks

1. INTRODUCTION
The Rapid Technological advancement and continuous learning in the field of cryptography have given birth to learning based cryptic algorithm to prevent against various smart cryptographic attacks. In the game of race between attacker and security expert, advance learning based study of cryptanalysis is also improving the cryptosystem and increasing prevention mechanism against the attacks. In fig. 1 the entire scheme has been presented. Since past several decades various work has been carried out in this direction.Machine learning, ANN based system, Genetic Algorithms etc. are recent disciplines which are contributing towards design of effective and efficient cryptosystem. In the subsequent sections of this paper detailed survey study has been done on the basis of following keywords:

Artifical Neural Network (ANN), Genetic Algorithm (GA), Swarm Intelligence (SI)

This work of cryptography will help to identify the nature of research work that has been done so far and to develop a basis of forming any new platform for further research including the trends and scope in the theoretical as well as applied domain.

1. Criteria 1- Applied Technique:{classification: ANN, KNN, SVM, Decision tree, GA, Fuzzy logic }
2. Criteria 2-Type of Algorithm for enciphering {AES, DES, Blowfish, RC6, Two fish, Fibonacci-Q, Sparse key}
3. Criteria 3-Nature and life time of Key: {Symmetric(Private)-life time higher then AVK, Asymmetric (Public) -life time higher then AVK, Symmetric-AVK –for a specific session}
4. Criteria 4-On the basis of Mathematical operations : key based multiple Huffman tables, tree parity machine, Interpolation (Polynomial, fuzzy)

In the subsequent section of this work, we will initially point out the highlights and significance of work and the work carried out in the paper explores various research criteria and techniques employed by a cryptic algorithms. The diagrams and charts are self-explanatory and time saving for the quick reference. Further, this survey paper can be enhanced and updated with identified research directions.

2. BACKGROUND FOR CRYPTANALYSIS
In principle, data mining techniques are concerned with information extraction for application level and for the business and commercial need of the user."Cryptic Mining" is term coined by Shaligram and R.S. Thakur in 2013, for the low level information domain. This domain increases the security level of cryptosystem and also helpful for hackers and cryptanalytic for identification to strengthen the information system. The framework for AVK based cryptosystem and cryptic mining is elucidated in Fig. 1.

Cryptic mining domain broadly applies to the extended traditional mining techniques for the extraction of useful patterns and discovery of key size and strengthening the algorithms. Although, it is assumed that ciphers are 100% random in nature, but in practice, it is not possible. There may be some patterns generated in cipher-text, input plain-text, keys used to encipher it etc.The patterns stored in stored files or flowing in the network can be used to exploit and harness the weakness in the process using cryptic mining algorithms.

Classification: Useful in detecting cipher-text scanners to decide the nature and class of algorithm.(refer table 1)

Clustering: It groups the cipher-text based on similarity into groups for predicting the algorithm and pattern of the groups.(refer 2)

Association Rule: These set of algorithm investigates rules for associating parameters based relationships together with (plain-text,cipher-text) paired associations.[48,49]

Pattern discovery: These set of algorithm works as scanners and input them to high-end analysis tools like Markov model[48], ANN, GA, ACO etc. These cryptic mining techniques finds applications in detecting behavior of malware, ad-ware analysis, classes of attacks using honey-pot and honey-net systems.

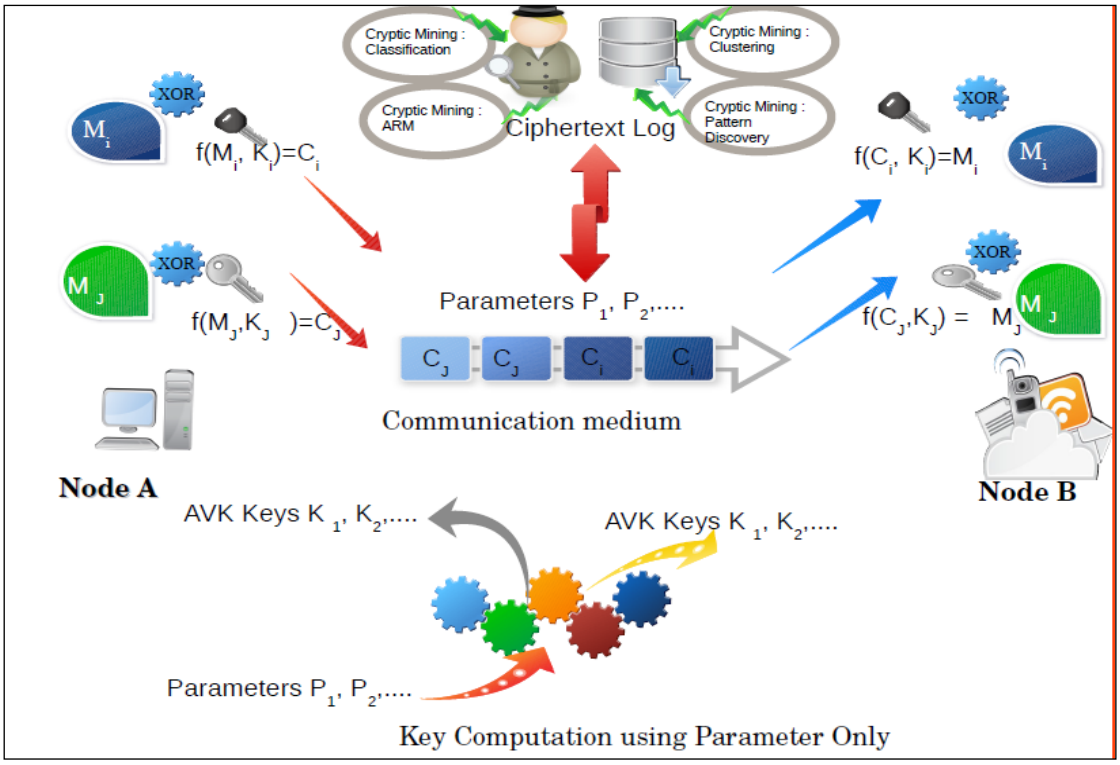

Fig 1: A framework for Cryptosystem and Cryptic Mining with AVK

2.1 Cryptic Classification using ANN

Enabling Cryptanalyst with advanced tools is ever demand for identification of weakness and flaws of cryptosystem. In polynomial time, Cryptanalyst is interested to extract useful hints for detecting original information, from huge corpus. Cryptanalyst may have captured large database and corpus containing variety of ciphers and hash files. When a ciphertext is inserted into this dataset, it might be mixed within other ciphers generated from various other schemes including variations in key size, protocol, type of ciphers generation algorithm, degree of exposures of information about key space and many other information related to plaintext, ciphertext, relationship between them. The cryptanalyst may develop a mechanism that will classify/sort/ group according to cipher type. One such method is demonstrated in fig.2. A scanner algorithm may be developed which measures three properties of ciphers; x, y, and z. If the cipher or key is generated with contribution with parameter-1 then it outputs 1 else -1(if it is not through x

The sensor algorithm will output 1 corresponding to second parameter y if it is through y. Similarly, sensor algorithm will work for parameter z. The three output of sensor will be input to neural network. This neural network (classifier) will decide which kind of cipher is in the database, so that the cipher can be directed to the correct class. Consider following model for classifying minimal two types of class say class-1(For AES: C_1, C_3,C_4) and class-2(For DES C_2,C_5).There are only two kind of ciphers in the captured-database-log. As each cipher passes through the sensor it can be represented by 3-D vector of parameter set P = [x y z] .

The output prototype for class-1 is [1 -1 -1] and output for class-2 will be [1 1 -1].

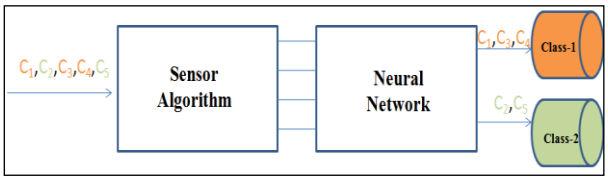

Fig 2 : ANN model fop Classifier for cryptanalysis

The neural network will receive one 3D input for each cipher from captured log and makes a decision to whether the cipher is from class-1 or of class-2.A simplified single layer perceptron can be depicted to solve it. The output of perceptron must be 1 when a cipher of class-1 is input and -1 when cipher of class-2 is supplied as input.

$a = hardlims([w_{1,1} \quad w_{1,2} \quad w1,3] * [x \quad y \quad z]^t + b)$

The choice of bias b and the elements of weight matrix is such that the perceptron will be able to correctly distinguish ciphers of class-1 and class-2.Linear separator that can separate ciphers of class-1 and class-2 can be pictorially denoted by XZ- plane and acts as decision boundary with equation Y = 0.

$[0 \quad 1 \quad 0]*[x \quad y \quad z]^t + 0 = 0$

The weight matrix w=[0 1 0]and bias will be b=0. w is orthogonal to the decision boundary and points towards the region that contains the prototype patter of class-1 for perceptron o/p of 1.As the decision boundary passes through origin so bias=0. Y=0

$[0 \quad 1 \quad 0]*[x \quad y \quad z]^t + 0 = 0$

Testing of perceptron based classifier can be done as follows. As this classifies ciphers of class-1 and class-2 correctly:

For class-1{C_1,C_3,C_4}

$a=hardlims([0 \quad 1 \quad 0]*[1 \quad 1 \quad -1]^t+0) = 1$

For class-2 {C_2,C_5}
a=hardlims([0 1 0]*[1 -1 -1]^t +0) = -1
if any non distinguishable cipher is supplied as input to the classifier (Cipher with confusing pattern) may be of class-1 or class-2 through the output of sensor with i/p vector = [-1 -1 -1]^t

a = hardlims([0 1 0]*[-1 -1 -1]^t + 0)=-1 (class-2)

Any input cipher that is closer to class-2 with respect to class-1 will be classified as a member of class-2, and vice versa. Thus perceptron based cipher classifier may separate cipher patterns with linear decision boundary. The issue with the approach requires deep digging for higher dimension and learning of algorithm. In addition, complexity will also increase when ciphers cannot be separated by linear boundary. The next section provides detailed survey conducted for finding out alternative approaches like multilayer perceptron and others. Apart from this perceptron model, numerous other techniques also exist. Next section will illustrate them briefly

2.2 Exploration of Other approaches in literature

In literature various state of art approaches are available for analysis of cipher-text and mining useful patterns. following are some significant work and brief insights of the technology used.

According to Khadivi, P and Momtazpour, [1], cryptography is essential building block for information and network security and needs advancement with increasing growth in internet. They used block cipher generation algorithm by information recording techniques. Features from this information can be extracted to distinguish from others. In addition, these features can be used to transform from these information into cipher-text.

S. Mishra and Bhattacharya, in [2] suggested that, cryptanalysis can be done by combining various algorithms simultaneously to transform cipher-text into plaintext information especially for the set of problems like:{Block Length detection, stream detection, entropy analysis, recurrence analysis, dictionary based analysis, decision tree based problems}.

Sharif and Mansoor in [3],presented pattern recognition based enciphering algorithms for the identification of patterns using different classification techniques like SVM, Naïve Bayesian , ANN, Instance based learning , Bagging , AdaBoostM1, Rotation Forest, and Decision Tree .It is noted here that, these approaches provides less accuracy with increase in number of encryption keys and needs extension and improvements .

In [4], Swapna, Dileep, Sekhar and Shri Kant have presented methods using support vector machine to identify block-ciphers (A pattern classification task). These two methods make use of different inputs. The first method takes cipher text and second method takes partially decrypted text derived from a cipher text as input. In second, SVM based method performs regression using hetero -association model to derive the partially decrypted text. The cipher text and partially decrypted text are analogous to documents and the identification task of enciphering method is considered as a document categorization task.

Similarly, towards automation of deciphering of cryptic text the work of Nuhn and Knight, described in [5], have analyzed the large number of encrypted messages found in libraries and archives, and tried to human effort only on a small but potentially interesting subset of it. This work attempts to reduce human effort as well as error in decryption. Also they were interested to develop a classifier (first trained and then predict) to know which enciphering method has been used to generate a given cipher text.

The work of Baragada and Reddy in [6], was focussed for breaking a cryptosystem as a pattern classification problem, with neural networks as a cryptanalysis tool.

In [7], the team of Laskari, Meletio, Stamatiou, and Vrahatis conducted survey on usage of advanced AI techniques to cryptic problems and found that AI based security measures can be developed but their performance will depends on the data representation and problem formulation.

Bagnall, Mckeown and Rayward In [8], worked for deciphering of messages encrypted with rotor machine using genetic algorithm. It searches the key space in encrypted text. The identified limitation of these method are that they didn't work with a two rotor problem in times comparable to those obtained using the iterative technique.

In [9,11], Diffie and Hellman have examined kinds of contemporary developments in cryptography and forecasted that in future, new type of cryptographic system will exist which has reduced need of secure key distribution channel. The key distribution problem is significant in large population size. They suggested two alternatives. (1)Subversion of key-use subversion of several separate key distribution points to compromise the system's security. (2)Public sharing of key-allows to make sender's key information public.

From the perspective of fuzzy logic Jin [10], have focused on fuzzy association rule mining and fuzzy aggregation operator of the rule mining process. They emphasized on selection of an appropriate operator depends on the application context. This work was on exploration of the impact of different operators on fuzzy association rule mining.

In [12], Aysal and Barner have presented an encrypted wireless sensor network or eWSN-model in which, encryption and stochastic enciphers have been applied on output sensor's binary to disguise the sensor outputs. In this e-WSN system they have decentralized estimation of a noise-corrupted deterministic signal in a bandwidth-constrained sensor network communicating through an insecure medium.

Khadivi, Momtazpour [13], have demonstrated classification of attacks for distinguishing cipher text and proposed enhancements in the security of crypto systems.

Visual cryptography based cryptosystem have been discussed, by Yui and Chian in [14] with their Q'tron neural networks prototype uses visual encryption procedure with the integer-programming-type energy function.

In [15], Winterhof has applied interpolation method of the discrete logarithm using finite prime field Fp by polynomials modulo p and modulo p-1 given by Coppersmith and Shparlinski to arbitrary Fpr. Frequency analysis in cipher provides significant direction to cryptanalyst.

According to Ragheb Toemeh and subanagounder Arumugam in [16], frequency analysis is used for framing objective function of cryptography. They studied the applicability of Genetic Algorithms for searching the key space of encryption scheme and presented cryptanalysis of poly alphabetic by applying Genetic algorithm.

Survey based on parameters like queries, heuristics, erroneous information, group key exchange, synaptic depths has been conducted

In [17], by Chakraborty, Dalal, Sarkar, and Mukherjee . These parameters are suggested to improve the time complexity of algorithmic interception or decoding of the key during exchange.

In [18], Barkan, Biham, and Keller have presented method for communication based on GSM Encryption and different attacks on the GSM protocols. But cryptanalysis based study was limited to cipher-text-only.

In [19], Dileep and Sekhar have presented encryption method of block cipher by using the Support vector machine Technique. This task was inspired from techniques of document categorization. Common dictionary based method and the class specific dictionary based method are two proposed approaches for document categorization.

According to Sharbaf [20], quantum cryptography can contribute to the network security. Laws of quantum mechanics are inviolable, thus it will act as the basis for security of network communications.

Enhanced linear cryptanalysis has been discussed in [21]. M. Matsui says that, with the application of linear cryptanalysis weakness in algorithm can be pinpointed, the extended version he was able to break the full 16 round DES from a computer experiment. In this version he has considered the reliability of the key candidates to improve the success rate.

According to Biham and Shamir [22], with widely used DES based cryptosystems,one can identify new kind of attacks which breaks DES in more easier and faster for present exhaustive search.

In [23], Jakimoski and Subbalakshmi, have analyzed various encryption schemes for multimedia applications. Randomized arithmetic coding (RAC), Key-based multiple Huffman table (MHT) and arithmetic coding with key-based interval splitting (KSAC) are some of the method used.

According to Spillman, Janssen, Nelson and Kepner [24], directed random search algorithm (genetic algorithm) can be used for simple substitution cipher and new approach for cryptanalysis can be identified.

In [25], E-Zogghabi, Yassin and Hussien have reviewed on the use of artificial neural networks in cryptography and studied their performance on approximation problems related to cryptography.

In [26], Luis and Seoane have suggested general probabilistic attacks for neural cryptography. These have used mathematical tools (From the field of statistical mechanics) to calculate some underlying probability distributions like the secret keys generated by the cryptographic protocol take this or that shape.

Another survey by Zahir [27], based on key exchange of using two tree parity machines is also available. He introduced two new techniques with multi-bit communication, which decreases attacker's probability.

In [28], Wolfgang kinzel and Ido kinter have suggested that How mutual learning can be applied for public key exchange over the network.

According to Klein and team [29], the phenomenon of two neural networks that are trained on their mutual output synchronize to an identical time dependant weight vector is utilized for creating safe cryptographic keys. Some models were also proposed and tested for security under various attacking conditions for this cryptographic system.

In [30], A mathematical black-box model was proposed by Alallayah, AbdElwahed and Alhamami which led the foundation for the development of Neuro-Identifier for determining the key from any given plaintext-Ciphertext pair. Some system identification techniques were combined with adaptive system techniques were used for the creation of the model.

Generation of secret key using neural network is experimented by Jogdand and Bisalpur [31].In this neural cryptography work, the communicating networks are provided identical input vector. An output bit is generated for training the networks to encrypt and decrypt information over a public channel the generated secret key is used.

In [32], Michal Ido and Wolfgang have conducted analytic study on mutual learning process between two parity using feed-forward networks with discrete and continuous weights and found that the number of steps required to achieve full synchronization between the two networks in the case of discrete weights is finite.

In [33], Mislovaty, Klein, Kanter and Kinzel have presented a bridge between the theory of neural networks and cryptography. They proposed an encryption scheme based on neural networks, and discussed its security in detail. They analyzed the security of Neural Cryptography- a novel key-exchange protocol based on synchronization of Neural Networks.

Lawrence, Giles and Tsoi [34] used, neural networks (AI machine learning models) with back propagation algorithm, takes a controlled task with known optimal training error. They found that the optimal solution is typically not found, and observed that larger network with lower training will result in high generalization error.

According to A. S. Weigend [35] discussed connectionist networks with previously stored knowledge. The two main part of HKP address two very different problems. The focus was on before turning to learning, i.e. the automated extraction of rules from examples.

In [36], Alexander, Mityagin and Shamir have analyzed the security of a new key exchange protocol, which is based on mutually learning neural networks. According to them, this is a new potential source for public key cryptographic schemes, which are not based on number theoretic functions, and have small time and memory complexities.

The power of neural network in cryptography domain is mentioned by Alallayah, Amin, El-Wahed, and Alhamami in [37].According to them the cryptanalysis problems are unknown and use of neural networks is good for such problems. A black box (Mathematical) model has been conceptualized by them. On the basis of this model, Neuron-Identifier is constructed using the combination of system identification techniques and adaptive system techniques. They used LM algorithm is used to train the Neutron-Identifier, which increases the speed, approximation capabilities and accuracy of the system. As a result, the performances of the higher up till the required degree.

In [38], Hertz, Krogh and Palmer have done analysis and comparison of different cryptanalysis model by using uniform notation and symbols. Calculation for storage capacity of

random patterns is done in this study.

In [39], Ruttor, Kinzel, Shacham and Kanter, have conceptualized addition of feedback mechanism in neural cryptography. As a result of introduction of feedback mechanism the repulsive forces gets increased. Probability based successful attack is calculated using numerical simulations and analytic approach for different model parameters.

For confidentiality of Block ciphers Baigners, Thomas [40] performed quantitative analysis; here quantitative analysis of blocks ciphers is done to find the extent of the confidentiality. They also described the difference between the distinguishing attacks and key-recovery attacks against block ciphers.

The landmark article in the direction of contemporary cryptography in [41],by Diffie and Hellman, have presented the basic information, theoretic and computational properties of classical and modern cryptographic systems, followed by cryptanalytic examination of several important systems and an examination of the application of cryptography to the security of timesharing systems and computer networks. They have provided a guide to the cryptographic literature.

As the key length used by cryptosystem is increased the processing time and efforts needed to guess the actual key increases For example 8 bit long key contains 256 possibilities. A systematic attempt for exploring this key is feasible ,But the number of possible keys increases exponentially with the key size. For a 56-bit key containing 2^{56} possible keys. A cryptanalyst or hacker tries one million keys per second would take approx 2284 years to try. Similarly, for 64 bits with 2^{64} possibilities he would take 5.85x105 years. With the development of multi Another approach of advancement in cryptography is Automatic variable key approach, The cipher generated from this approach are through dynamic keys that keeps changing from session to session.

some variety of techniques(such as Fibonacci Q and Sparse Matrix) and it's analysis from hackers and cryptanalyst perspective is available in [43,44,45,46,47,48,49].In the light of Cryptic mining, The clustering and classification of ciphers is to be investigated from ANN and it's variants.

In [50,51] Some System design models and implementation of cryptosystem for analysis of cipher-text and extracting plain-text from it has been presented, the system was built with some AI and knowledge base components and works for substitution ciphers. The work will be extended for inclusion of other complicated ciphers in near future.

In [52] performance analysis of two or more then two cryptosystem has been compared that are for symmetric key and performance analysis can be compared w.r.t. various file size, key-size and enciphering algorithm types. The web interface for comparing some state of art algorithms has been compared and various plots has been demonstrated.3. Survey Statistics

So here approximately 50 research papers have been considered for the survey of last two decades, fig.3 shows the variation of the applied techniques.The survey is carried out on the basis of certain keywords and classification has been done on the basis of those keywords. The keywords set being considered are as follows:

Keywords = { ANN, KNN, SVM, AES, DES, Blowfish, Two fish Decision Tree(DT), Data mining(DM), Genetic Algorithm(GA), Public key (PKI), fuzzy classification, Mean square error method, symmetric key encryption, polynomial interpolation, vignere cipher, quantum cryptographic, key based multiple Huffman tables, tree parity machine }

On the basis of these keywords, these papers were classified to analyze the amount of work done using various techniques and algorithms in the field of cryptanalysis.

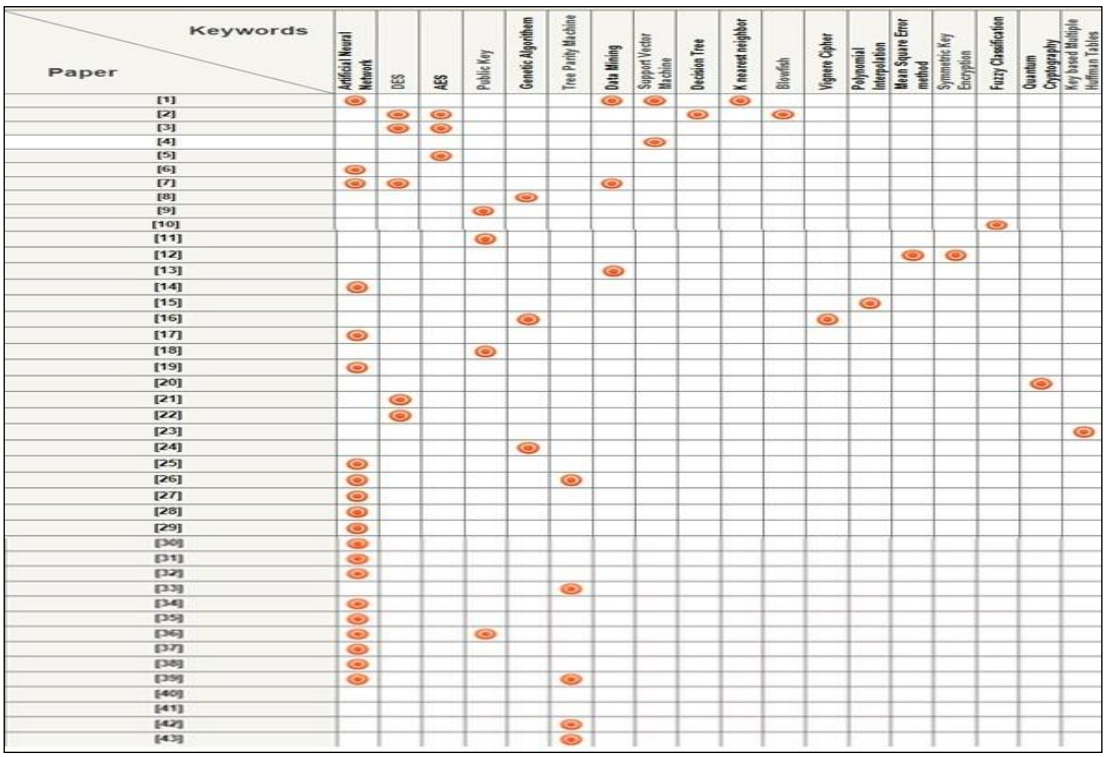

Fig 3 : Tools used for cryptanalysis and keywords in considered Publications

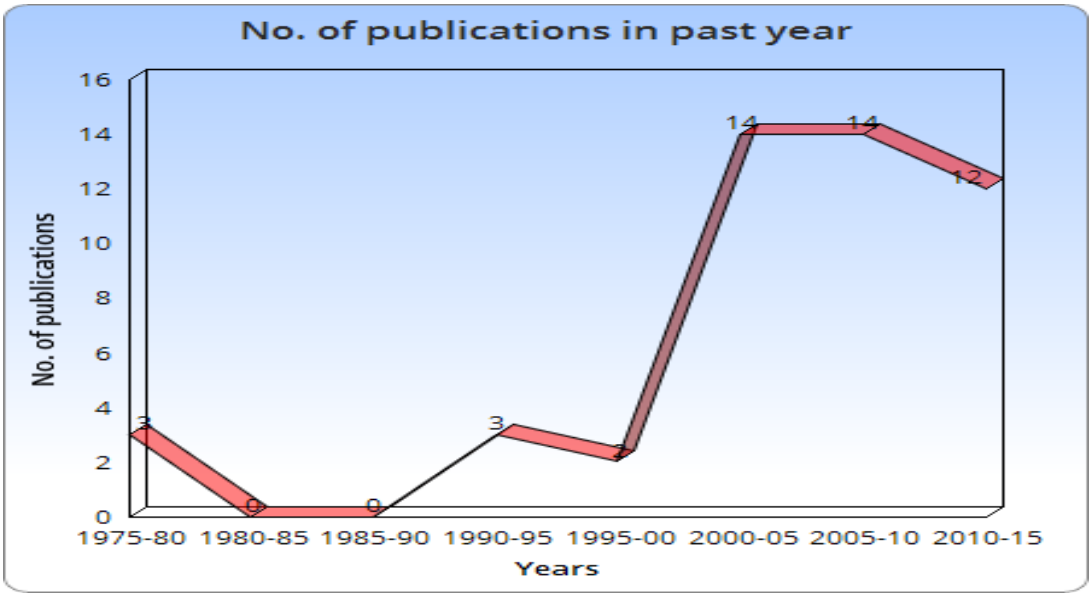

Fig 4: Year wise publications in past year with count

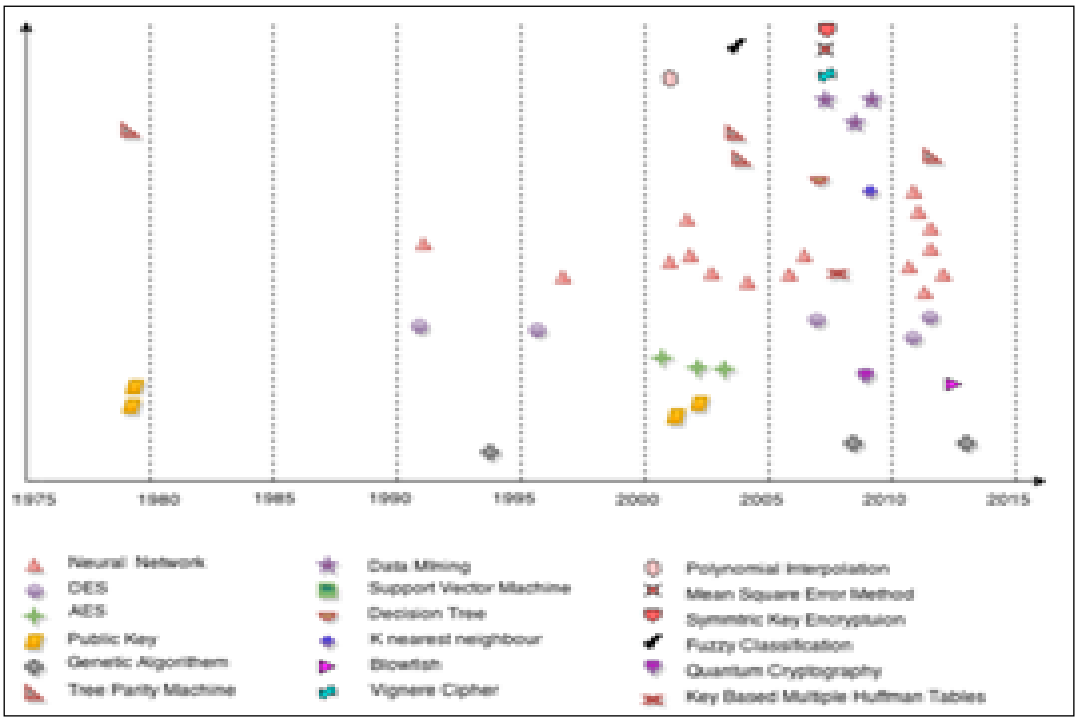

Fig 5: Publications v/s algorithms in past years

3. AVK PERSPECTIVES

The study reveals that before last two decades, the study in the field of cryptanalysis using neural network was diminishing. However, considering the survey being done the result shows a startled growth in the same field. There are many reasons for this but it certainly shows the presence of research gap and opportunities.

After the study of referenced paper, these papers shows a wide range of future scope that can be covered with further research. The study provide a basis for further research many referenced have been considered for survey in a chronological order. Following table shows the future scope of different paper being considered for the survey.

3.1 AVK based cryptosystem and IOT

Recently IOT is also gaining pace, here system and Internet is connected to the physical world via ubiquitous sensors". The concept of communication between one device with other is not a new concept. Recently, communications among Machines also have been demonstrated with talking machines. Deployment of IoT technologies is demanding more intelligence, more complexity – into the conversation. With the development of Computational Intelligence approach, Intelligent Agent Based System seems to be the backbone and Demand of Future Technology that are capable to provide intelligent Machine-to-Machine conversations and IoT connectivity solutions for wireless and wired networks for the benefits of society and Mankind. Since lightweight cryptography, algorithms are demand of current and future

devices. There are symmetric cryptography algorithms namely, AES, DES, RC4, Blowfish, TwoFish, for enhancing security. The Latest trend in symmetric cryptography is to increase the key length, which leads to higher power and computation time. Still we do not have good candidate in Hash and symmetric key encryption function. This paper highlights the efficient way of enhancing them to be ready for new dimensions of IOT. Our work of Fibonacci-Q, Sparse approach and cryptic-mining are aligned in the extension of AVK concepts, with hacker's and cryptanalyst perspectives.

Following research questions are yet to be answered:

(1). What are the scopes of AVK approaches of ensuring efficiency in IOT ? Especially when heterogeneity is high like for devices with connectivity at the "edge" of networks in remote and demanding environments, using Ethernet, serial, wireless and USB communication technologies.

(2). How system would maintain reliability on operating with WSN?

(3). How system will control and manage keys in g IoT environments?

(4). How system will be designed to work robustly on deploying intelligence at the network edge? The paper also opens a new direction to think about efficient security mechanism for talking devices in IOT environment using AVK and prepares the basis for AVK based security architectures with the issues of key management scheme, including key provisioning, key updating policy or key agreement

Table 1: Cryptic Mining: Some Classification approaches

No.	Method	Concepts	Feature	Limitations
1.	Rule-Based classifier	If…then … like rules	Simple to Use	Complex situation are hard to define in Simple rules
2.	Bayesian Networks	Probability of patterns in ciphers or key	Efficient with causal relations	Cannot handle missing data well
3.	Artificial Neural Network	Mathematical model calculating output based on inputs	Can handle complex relations	Black box
4.	Support Vector Machines (SVM)	Classes of ciphers are separated by a hyper plane by calculating support vectors to the closest points from each class	Small chance at over fitting and possible to use dynamically	Slow on large sample sizes
5.	Decision Trees	Classification by If..then..like tree structure	Can handle numeric and text data types	Very hard to find optimal solution

Table 2: Cryptic Mining: Some Classification approaches

No.	Method	Concept	Feature	Limitation
1.	kNN	Distance/ density computation between objects and classes.	Simple to implement	Storage intensive and susceptible to noise
2.	HMM	The probability of a sequence of observed encrypted objects is used to calculate the probability of a sequence of non-visible events.	Can analyze sequences of events in which the events are not independent	Events must be independent. (The events may not provide a probability of a event.)
3.	k-Means	Clustering based on equality Clusters data into a Given number of k clusters by minimizing the mean	Insensitive to noise and cluster shape Pre-classification not necessary	Initial choice of parameter values Hard to find Optimal solution and sensitive to cluster shape
4.	Self-organizing maps(SOM)	Distance to a cluster center Neural network where output neurons are pixels of a density map and similar cases are mapped close to each other	Good reduction of data feature dimensionality while maintaining relationships between the features	Resulting model is a black box and creating a model is computational intensive.

Table 3: Future Scope and research directions for ANN perspective

No.	Paper Title	Method	Future Direction
1.	Pattern analysis of cipher text: a combined approach	Dictionary and decision tree based approach	effective cryptanalysis for the AES algorithm
2.	Cryptography and Cryptanalysis Through Computational	Artificial neural network	In order to find the effectiveness and efficiency of proposed cryptographic systems EC method can be

	Intelligence		used
3.	Cryptanalysis of a three rotor machine using a genetic algorithm	genetic algorithm	Cryptography could be into the cryptanalysis of substitution-permutation systems and possible variations of the rotor machine.
4.	Fuzzy classification based on Fuzzy association rule mining	Fuzzy association rule mining	The framework can deal with not only binary and category attributes but also continuous quantitative attribute.
5.	Multiuser cryptographic techniques	protective protocol, Public key cryptography, Public key authentication	If sender's keying information is made public then need for secure key distribution is completely eliminated.
6.	Neural Synchronization based Secret Key Exchange over Public Channels: A survey	Neural Network	the study of chaotic maps for transformation of synchronized states of the networks to chaotic encryption keys, with exceptionally low tolerance for decryption error
7.	Quantum Cryptography: A New Generation of Information Technology Security System	Cryptography, Information Security, Security of Data, optical polarization, Quantum Cryptography	Quantum cryptography is headed forwards
8.	Probabilistic attack on neural cryptography	Tree parity machine (a bi layered feed forward artificial neural network	Some experiments may be carried out so the results will be completed and safety of the cryptographic procedure.
9.	Synchronization of neural networks by mutual learning and its application to cryptography	Neural Network	Advanced algorithms for synchronization, which involve different types of chaotic synchronization, seem to be more secure. Such models are subjects of active research
10.	Applying Neural Networks for simplified data encryption standard (SDES) cipher system cryptanalysis	Neural Network	It possible to use this model with the most sophisticated cryptosystems such as public key. as well as to use search for any efficient algorithm to reduce the space search for the keys and use the results as inputs for the neural network to get the correct keys
11.	Design of an efficient neural key generation	Neural Network	The key distribution centre generated the secret key. The key distribution centre will distribute the generated key securely by some method.
12.	Security Of Neural Cryptography	Neural Network	Our understanding for the reason of the majority attack's success implies that we should be looking for algorithms where the Overlap between the attackers would develop much faster than their overlap with the parties. This might be achieved by using larger K values, or some other modifications. These models are still under consideration.
13.	Lessons in Neural Network Training : Over fitting may be harder than expected	Neural Network	Methods for creation of more parsimonious solutions, importance of the MOP/BP bias.
14.	Security of neural cryptography	Neural Network	Our understanding for the reason of the majority attack's success implies that we should be looking for algorithms where the overlap between the attackers would develop much faster than their overlap with the parties. This might be achieved by using larger K values, or some other modifications. These models are still under consideration.

4. CONCLUSION

The paper provides useful survey to all beginners and researchers who are interested to work in the directions of cryptic mining, implementing some honey pot, honey net for developing offensive mechanism, using pattern discovery and behavior analysis of cipher text being propagated in the communication channel. The work also provides highlights of various works going in this direction by considering the paper with survey and statistics. So, one can have clear glimpses of the work done in cryptanalysis using various techniques and algorithms. Further, the researchers can identify the scope about area for studies that can be carried out to enhance computational efficiency of algorithm and extension of work in that particular field. This paper is not merely listing the contribution by researchers and their published work since decades, but it also depicts the summary of those research papers to act as supplement to boost the research work in cryptanalysis. The representation of statistics is self-explanatory to draw the conclusions regarding the work done

in various fields of cryptanalysis.

5. REFERENCES

[1] Khadivi P, Momtazpour M. "Cipher text classification using data mining", International Symposium on Advanced Networks and Telecommunication Systems IEEE- ANTS, pp.64-66, 2010.

[2] Shivendra Mishra, Dr. Aniruddha Bhattacharya , "Pattern analysis of cipher text : a combined approach", proceeding of Recent Trends in Information Technology (ICRTIT), 2013 International Conference on ,25-27 July 2013,393-398, DOI:10.1109/ICRTIT.2013.6844236.

[3] Sushila Omer Sharif, saad P. Mansoor , "Performance evaluation of classifiers of encryption algorithm", ACEEE International Journal on Network Security , Vol. 02, No. 04, Oct 2011

[4] S. Swapna, A. D. Dileep, C. Chandra Sekhar, and Sri Kant, "Block cipher identification using support vector classification and regression", Journal of Discrete Mathematical Sciences and Cryptography, vol. 13, no. 4, pp. 305-318, August 2010.

[5] Malte Nuhn, Kevin Knight , "Cipher type detection", http://www-i6.informatik.rwth-aachen.de/~nuhn/2014-classification-poster.pdf, pp.1769–1773,2014

[6] Sambasiva Rao Baragad, P. Satyanarayana Redd "Studies on the advancements of Nerual Networks and Neural Network based cryptanalytic works", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Volume 2, Issue 5, September – October 2013 ISSN 2278-6856

[7] E.C. Laskari, G.C. Meletio, Y.C. Stamatiou, M.N. Vrahatis ,"Cryptography and Cryptanalysis through Computational Intelligence", proceeding of Computational Intelligence in Information Assurance and Security, Studies in Computational Intelligence Volume 57, 2007, pp 1-49

[8] A.J. Bagnall, G.P. Mckeown, V.J. Rayward Smith , "Cryptanalysis of a three rotor machine using a genetic algorithm", In proceedings of 7th International Conference on genetic algorithms,ICGA97,1997

[9] Whitefield Diffe, Martin E. Hellman , "New Directions in cryptography", IEEE Transactions on Information theory, VOL. IT-22, NO. 6, NOVEMBER 1976, pp.644-654,1976

[10] Weiqing Jin , "Fuzzy Classification Based on Fuzzy Association Rule Mining", http://repository.lib.ncsu.edu/ir/bitstream/1840.16/5924/1/etd.pdf, 2004

[11] W. Diffie, M.E. Hellman , "Multiuser cryptographic techniques", IEEE transaction,1976

[12] T.C. Aysal, K.E. Barner , "Sensor Data Cryptography in Wireless Sensor Networks", Vol. 3 Issue: 2, pp.273-289,2008

[13] P. Khadivi, M. Momtazpour , "Application of Data Mining in Cryptanalysis" , pp.358-363,2009

[14] Tai-Wen Yui, Suchen Chian , "The General Neural Network Paradigm for Visual Cryptography", Vol. 2084 , pp.196-206,2001

[15] Arne Winterhof , "Polynomial Interpolation of the Discrete Logarithm", Vol. 25 Iss: 1, pp.63-72,2001

[16] Ragheb Toemeh, Subanagounder Arumuga "Applying genetic algorithm for searching key-space for polyalphabetic substitution cipher", Vol. 5 Iss: 1, pp.87,2008

[17] Sandip Chakraborty, Jiban Dalal, Bikramjit Sarkar, Debaprasad Mukherjee , "Neural Synchronization based secret key exchange over public channels: A Survey", Journal of Engineering Science and Technology Review 8 (2) (2015) 152 – 156.

[18] Elad Barkan, Eli Biham, Nathan Keller , "Instant Ciphertext-only cryptanalysis of GSM Encrypted Communication", Advances in Cryptology - CRYPTO 2003,Lecture Notes in Computer Science Volume 2729, 2003, pp 600-616, 2003.

[19] Dileep, A.D, Sekhar, C.C. , "Identification of Block Cipher using Support Vector Machines", 2006 International Joint Conference on Neural Networks Sheraton Vancouver Wall Centre Hotel, Vancouver, BC, Canada July 16-21, 2696 - 2701,2006.

[20] M.S. Sharaf ,"Quantum Cryptography: A New Generation of Information Technology Security System", In proceedings of Information Technology New Generations, 2009. Sixth International Conference,27-29 April 2009, 978-0-7695-3596-8, pp.1644 - 1648 ,2009.

[21] M. Matsui , "The First Experimental Cryptanalysis of the Data Encryption", Advances in Cryptology - CRYPT0 '94, LNCS 839, pp. 1-1 1, 1994Vol. 839 ,1994

[22] E. Biham, A. Shamir , "Differential Cryptanalysis of DES like Cryptosystems", Vol. 537, pp.2-21,1991

[23] G. Jakimoski, K.P. Subbalakshmi , "Cryptanalysis of Some Multimedia Encryption Schemes", Vol. 10 Iss: 3, pp.330-338,2008

[24] Richard Spillman, Mark Janssen, Bob Nelson, Martin Kepner , "Use of a Genetic Algorithm, The cryptanalysis of Simple Substitution Ciphers", Vol. 17 Iss: 1, pp.31-44,1993

[25] Adel A. El-Zogghabi, Amr H. Yassin, Hany H. Hussien ,"Survey Report on Cryptography Based on Neural Network", Vol. 3 Iss: 12, pp.456-462,2013

[26] Luis Francisco, Seone Iglesias , "Probabilistic attacks on Neural Cryptography", master thesis, Berlin, Granada, Barcelona 2009/12, may 2012.

[27] Zahir Texan , "Public Key exchange by neural network", LNCS, http://www.cs.bilkent.edu.tr/~guvenir/courses/CS550/Workshop/Zahir_Tezcan.pdf

[28] Wolfgang Kinzel, Ido Kenter , "Neural Cryptography", http://arxiv.org/pdf/cond-mat/0208453.pdf ,Aug 2002.

[29] Einat Kein, Rachel Mislovaty, Ido Kanter, Andreas Ruttor, Wolfgag Kinzel , "Synchronization of Neural Networks by mutual learning and its application to cryptography", pp.689-696,2014

[30] Khalid Alallayah, Moamed Amin, Wail AbdElwahed, Alaa Ahamami , "Applying Neural Networks for simplified data encryption standard (SDES) cipher system cryptanalysis", Vol. 9, pp.163-169,2012.

[31] R.M. Jogdand, Sahana S. Bisalpur ,"Design of an

efficient neural key generation", Vol. 2 Iss: ?, pp.60-69,2011

[32] Michal Rosen-Zvi, Ido Kanter, Wolfgang Kinzel , "Cryptography based on Neural Networks-analytical results" , 10.1088/0305-4470/35/47/104, Feb2002

[33] R. Mislovaty, E. Kein, I. Kanter, W. Kinzel ,"Security of Neural Cryptography", http://idokanter.ph.biu.ac.il/papers/2004/Security.pdf, 2004

[34] Steve Lawrence, C. Lee Giles, Ah Chung Tsoi ,"Lessons in Neural Network Training: Over fitting may be harder than expected", In Proceedings of the Fourteenth National Conference on Artificial Intelligence, AAAI-97 pp.540-545,1997

[35] Andreas S. Weigend (NA) "Introduction to Theory of Neural Computation", To appear in Artificial intelligence, Elsevier Science Publisher,1993.

[36] Alexander Klimoy, Anton Mityagin, Adi Shamir, "Analysis of Neural Cryptography", Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings, pp.288-298,2002, 10.1007/3-540-36178-2-18

[37] Khaled Alallayah, Mohamed Amin, Waiel Abd El-Wahed, Alaa Allhamam ,"Attack and Construction of Simulator for some of Cipher System using Neuro-Identifier", Vol. 7, pp.365-372,2010.

[38] John A. Hertz, Ander S. Krogh, Richard G. Palmer , "Introduction to the Theory of Neural Computation", IAJIT 1992

[39] Andreas Ruttor, W. Kinzel, Lanir Shacham, I. Kater ,"Neural cryptography with feedback", Vol. 69 Iss: 4, ,2004

[40] R. Mislovaty, E. Klein, I Kanter, W. Kinzel "Security of Neural Cryptography", http://www.iasj.net/iasj?func=fulltext&aId=91984,2004

[41] Baigners Thomas ,"Quantum Security of block ciphers: Design and Cryptanalysis tools", Doctoral Thesis,2008

[42] Diffe W. Hellman, M.E. , "privacy and Authentication: An Introduction to cryptography", Vol. 67 Iss: 3, pp.397-427,1979.

[43] Shaligram Prajapat, A. jain, R.S.Thakur, "A Novel Approach For Information Security with Automatic Variable Key Using Fibonacci Q-Matrix", International Journal of Computer & Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 – 7449 Vol-3, Iss-3, 2012, p.p. No. 54-57.

[44] Shaligram Prajapat, R.S. Thakur et al."Sparse approach for realizing AVK for Symmetric Key Encryption", presented in 2 days International Research Conference on Engineering, Science and Management 2014 (IRCESM 2014), Dubai, UAE –ISBN 978-93-83303-51-9.

[45] Shaligram Prajapat, D. Rajput, R. S. Thakur, "Time variant approach towards Symmetric Key " ,IEEE Science and Information Conference 2013,October 7-9, 2013, London, UK p.p.398-405.

[46] Shaligram Prajapat, R.S.Thakur," Association Rule Extraction in AVK based cryptosystem",ICICS-2014,GOA,India,OCt. 2014.

[47] Shaligram Prajapat, R.S. Thakur, "Towards Optimum size of key for AVK based cryptosystem", Communicated and CJICT, Nigeria in June-Dec. 2015.ISSN (Online): 2354 - 3507; ISSN (Print): 2354 – 3566

[48] Shaligram Prajapat, R.S.Thakur, "Markov Analysis of AVK Approach of Symmetric Key Based Cryptosystem ",Computational Science and Its Applications, ICCSA 2015,Springer LNCS: Volume 9159, 2015, pp 164-176,Jun 2015,doi:10.1007/978-3-319-21413-9_12,ISBN:9783319214139 and 9783319214122.

[49] Shaligram Prajapat, R. S.Thakur, "Cryptic-Mining: Association Rules Extractions Using Session Log ", Computational Science and Its Applications, ICCSA 2015,Springer LNCS: Volume 9158, 2015, pp 699-711,Jun 2015,doi:10.1007/978-3-319-21413-9_12.

[50] Shaligram Prajapat, A. Thakur, K. Maheshwari and Ramjeevan Singh Thakur, "Cryptic Mining in Light of Artificial Intelligence",In second International Conference On Advances In Computing, Control And Networking - ACCN 2015 Digital Object Identifier: 10.15224/978-1-63248-073-6-77 Publication Year: 2015, Page(s):131 – 135.

[51] Shaligram Prajapat, A.Thakur, K.Maheshwari, R.S.Thakur, " Cryptic Minining in the light of Artificial Intelligence",(Extended version), Published in International Journal of Advanced Computer Science and Applications(IJACSA), 6(8), 2015. (DOI):10.14569/IJACSA.2015.060808

[52] Shaligram Prajapat, G. Parmar,R.S. Thakur," Towards investigation of efficient Cryptosystem using SGcrypter", ICCP-2015 and (extended paper) is in press IJAER.

[53] Shaligram Prajapat, R.S. Thakur, "Stochastic and Markov Analysis of AVK based cryptosystem", IEEE-ICCCC-2015 at MITM Indore.