ISSN 2277-8616

International Journal of Scientific & Technology Research

IJSTR.ORG

Editorial Board - IJSTR

Effect Of Company Resources And Capabilities To Product Innovation Smes In East Java Batik

Andrias Dwimahendrawan, Mohammad Saleh, Djoko Poernomo, Edy Wahyudi

Abstract : This study aims to explain the influence of resources and capabilities of enterprises with product innovation. This study uses a quantitative approach with a sample of 92 micro-enterprises. Analysis of data using regression. The results showed that the company's resources a significant effect on product innovation, while capability is valuable, rare, and can not be duplicated nor significant effect on product innovation. Originality of this study to measure product innovation by combining resources and capabilities of micro enterprise in eastern Java batik.

Keywords: Product innovation, the company's resources, capabilities,

1. PRELIMINARY

Innovation in the enterprise is a measure of the success of a company in conducting business activities. Among the theories are many factors that affect innovation, but in general can be classified into internal and external factors [1]. Internal factors which focused on the research is based on the idea of resource-based view (RBV) based enterprise resources and considers innovation a company can be built through the management and optimize the appropriate placement of resources and capabilities of companies [2], [3], [4], [5]. Placement of resources and capabilities are right, then the potential of creating a strategic and competitive advantage is very large company, and indirectly have a positive impact for the company. The company's resources is a whole wealth of companies whose shape can be tangible (tangible resources) and intangible (intangible resources). Examples of intangible company resources are the raw materials, production machinery, office buildings, money, as well as finished goods whose value can be found in the company's balance sheet. Examples of intangible resources of the company is a business network, reputation, trademarks, knowledge, which is not to be found in the company's balance sheet value [6], [7], [8], [9], [10]. Capability of the company is actually an enterprise resource that is intangible, but because it is specifically the number of experts distinguish it from the company's resources in general [11], [12], [13], [14], [15]. Enterprise resource called also supplies a significant venture or strategic to the company [16] when it has the characteristics worth (valuable) and rare (rare), other than the inimitable (inimitable) and can not be replaced (non-substitutable) to be processed further. Resources are valuable and rare is necessary for the company, a blend of the two simultaneously would potentially create added value (added value) for the company. But the company's resources that are strategic will be futile if the individual in the company did not have a good capability in managing the company's resources.

- *Andrias Dwimahendrawan is a student of the Doctoral Program in Business Administration at University of Jember.*
- *Mohammad Saleh is lecturer at University of Jember.*
- *Djoko Poernomo is lecturer at University of Jember.*
- *Edy Wahyudi is lecturer at University of Jember.*

Resources still need treatment or need to be processed further by the capability to change or move so that it has a value. Capability of the company is the ability, skills, expertise, skill personnel of the company in putting its resources to be processed in attaining the expected [17]. Capability company puts effectively and efficiently all the resources that exist within the company. If it can not be achieved in a company, enterprise resource management has failed.

Here it can be said the capabilities of the company has a very strategic position for the company because it involves the process and how to treat existing resources in the company. Same with the company's resources, organizational strength is said to be worth (valuable) if the company has the skills or the ability to process and manage the company's resources effectively and efficiently. In addition, the capability of the company is said to be rare (rare) and can not be imitated (inimitable) when processing and managing the company's resources are specific and unique that can be seen from the peculiarities of the products compared with competitors' products.

2. LITERATURE REVIEW

2.1 Company Resources

In developing the principles of RBV should be described in detail in the company's resources that make it a source of competitive advantage. Resource company must have the characteristics of Vrin (valuable, rare, inimitable, and nonsubstituable) [18]

2.2 Company Capability

Define the organizational strength is the bond amount of expertise and accumulated knowledge that allows the company to coordinate activities and use of asset-its assets to create economic value and competitive advantage be continued [19]. Other Definitions of the capability of the company is the company's capacity to use the resources that are integrated with the aim of achieving the desired end goal [20]. Furthermore Hitt and his colleagues revealed, as the glue of the organization, capabilities whenever it appears through a complex interaction between resource tangible and intangible.

2.3 Product Innovation

OECD define the product innovation as the introduction of new products or services or significantly improve in terms of the characteristics of the product or service or expand the use of products or services [21]. Camison and colleagues define product innovation as manufacture of new products or new services or improved and introduced to the market. product innovation is closely related to the main activities of the company, therefore, product innovation can be seen as an important source of competitive advantage that can lead to the improvement of organizational performance.

3. RESEARCH HYPOTHESIS

3.1 Company Resources and Product Innovation

Strategic resources of the company have the characteristics of valuable, rare, inimitable and irreplaceable is the source of creation of products [22], [23]. There are four (type) type of innovation, one of which is a product innovation. This explanation indicates that there is a relationship of company resources (especially intangible resources) with product innovation [24]. Based on the description above can be hypothesized

H1: the company's resources are valuable and rare significant effect on product innovation

3.2 Company Capability and Product Innovation

According to Chang implies that the company has a dynamic adaptive capability, absorptive, and high innovative indirectly steer the strategy focuses on continuous product innovation [25]. Therefore, continuous product innovation an important requirement for the company. Based on the description above can be hypothesized

H2: Company Capability valuable, rare, and can not be imitated significant effect on product innovation

4. RESEARCH METHODS

Based on the problems and research objectives, this study used quantitative methods. Research using quantitative methods [26] Indriantoro and Supomo emphasis on testing theories through the measurement of research variables with numbers and perform statistical data analysis procedures.

4.1 Population and Sample

The study population numbered 120 micro enterprises batik in Banyuwangi, Bangkalan, Sumenep, and Tuban. According to Slovinto determine the number of samples proportional sampling method using the proportionate method, namely, Banyuwangi 19 units, 31 units Bangkalan, Sumenep 27, and Tuban 15 units. Research analysis unit at the level of the represented company owner.

4.2 Measurement

The company's resources are corporate assets tangible and intangible, measured by indicators of precious and rare. Capability of the company is the skill to manage resources to generate profits with valuable indicator, rare, and can not be imitated. Measurements on the questionnaire using Likert scale.

4.3 Method of Data Collection and Analysis

Collecting data using enclosed statement. Enclosed statement has five answer choices according to Likert scale. Analysis of data using regression.

5. DISCUSSION

Model Summaryb

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.399a	.159	.140	1.91736	1,749

Model table contains summary about the strength of the relationship between the dependent and independent variables. The regression model has:

a) The R value of 0.399 means that the relationship between independent variables and the dependent variable was a positive value. Rated R is the value of multiple correlation coefficient. R value ranging from -1 to 1. If the value closer to -1 or 1 indicates the relationship is getting stronger, if the value closer to 0 indicates weaker relationships. The relationship between independent variables and the dependent variable is positive it means increasing the value of the independent variable causes an increase in the value of the dependent variable.

b) For regression with more than two independent variables, in the use value of adjusted R ² (R ² adjusted) as the coefficient of determination of 0.14 means that the diversity of independent variables (enterprise resource and capability of the company) can explain 14% of the diversity of the dependent variable (the variable product innovation). Here means that only 14% of the variation of product innovation that can be explained by resource companies and company capabilities. While the rest (100% -14% = 86%) is explained by other causes.

ANOVAb

Model		Sum of Squares	df	mean Square	F	Sig.
1	Regression	61 888	2	30 944	8417	.000a
	residual	327 188	89	3676		
	Total	389 076	91			

The results of the above analysis obtained F value of 8417 and p (0.000) <α (0.05) means that H0 is rejected. It can be deduced that simultaneously (simultaneously) the independent variables affect the dependent variable or resource companies (X1) and Capability company (X2) together (simultaneously) affect product innovation (Y1)

Partial test shows that

- Resource companies have a p-value (0.008) <α (0.05) so H0 is rejected means that there is influence of corporate resources to product innovation
- Capability company has a p-value (0.029) <α (0.05) so H0 is rejected means that there is influence company's capability to product innovation

So that the partial test (effect of each independent variable on the dependent variable partially) produce that all independent variables affect the dependent variable

Model discovered is
y = B0 + β1 + β2 X2 X1
y = 11,705+ .103 X1 + 0,138 X2

6. CONCLUSION

Resources scarce and valuable company have significantly affect product innovation. This means that more resources are precious and rare owned by micro enterprises resulted in higher batik creation of the company's product innovation. Company capabilities are valuable, rare, and can not be imitated have positive values significantly affect product innovation, this means that the capability of a larger company that is valuable, rare, and can not be imitated owned by micro enterprises batik produce innovative products more good limitation of this study is homogeneous samples, therefore, for future research, the study sample must be heterogeneous.

REFERENCES

[1]. Sampurno, 2011, Strategic Management: Creating Sustainable Competitive Advantage, Gadjah Mada University Press.

[2]. Penrose, ET, 1959, The Theory of the Growth of the Firm. Oxford: Oxford University Press

[3]. Wenerfelt, Birger, 1984, A Resource-based View of the Firm, Strategic Management Journal 5: 171-180

[4]. Barney, Jay., 1991, Firms Resources and Sustained Competitive Advantage, Journal of Management, Vol 17, No. 1: 99-120

[5]. Teece, DJ, Pisano, G., & Shuen, A., 1997, Dynamic capabilities and strategic Management, Strategic Management Journal, 18 (7), pp. 509-534.

[6]. Barney, Jay B., Clark, Delwyn N., 2007, Resource-Based Theory: Creating and Sustaining Competitive Advantage, Oxford University Press.

[7]. Purnomo, Djoko et al. 2013, The Effect of the Resources and Capabilities to Competitive Advantage and Company's Performance of "Batik" Micro. European Journal of Business and Management, Vol 5, 23, pp 152-159.

[8]. Gruber, Marc., Heinemann, Florian., Brettel, Malte, Hungeling, Stephan., 2010, Configurations of Resources and Capabilities and Their Performance Implications: An Exploratory Study on Technology Ventures, Strategic Management Journal, 31: 1337-1356.

[9]. Kunc, Martin H., Morecroft, John DW 2010, Managerial Decision Making and Firm Performance Under a Resource-Based Paradigm, Strategic Management Journal, 31: 1164-1182.

[10]. Masakure, Oliver; Henson, Spencer; Cranfield, John, 2009, Performance of microenterprises in Ghana: a resource-based view, Journal of Small Business and Enterprise Development, Vol. 16, No. 3, pp. 466-484

[11]. Penrose, ET, 1959, The Theory of the Growth of the Firm. Oxford: Oxford University Press

[12]. Amit, Raphael, & Schoemaker, Paul JH, 1993, Strategic Assets and Organizational Rent, Strategic Management Journal, Vol. 14, pp. 33-46.

[13]. Barney, Jay., 1991, Firms Resources and Sustained Competitive Advantage, Journal of Management, Vol 17, No. 1: 99-120.

[14]. Ljungquist, Urban, 2007, Beyond the Core Competency Identification: Presentation of a Model, Management Decision 45 (3).

[15]. Barney, Jay B., Clark, Delwyn N., 2007, Resource-Based Theory: Creating and Sustaining Competitive Advantage, Oxford University Press.

[16]. Hsieh, Jasper J., 2008, Toward A Dynamic Resource Based View of Strategic Stakeholder Management, Paper presented at the Western Academy of Management International Conference on 'strategic alliances and networks' at the Asian Academy of Management.

[17]. Hitt, Michael A., R. Duane Ireland, Hoskisson, Robert, 2001, Strategic Management: Competitiveness and Globalization Concepts, Thomson Learning Asia 60 Albert Complex, Singapore.

[18]. Barney, Jay., 1991, Firms Resources and Sustained Competitive Advantage, Journal of Management, Vol 17, No. 1: 99-120.

[19]. DeSarbo, Wayne S .; Di Benedetto, C. Anthony; Song, Michael, 2007, A Heterogeneous Resource Based View For Exploring Relationships Between Firm Performance And Capabilities, Journal of Modeling in Management, Vol. 2 No. 2, pp. 103-130.

[20]. Hitt, Michael A .; Sirmon, David G., 2003, the Managing Resources: Unique Linking Resources, Management, and Wealth Creation in Family Firms, Baylor University, Download http // www.ssrn.com.

[21]. Camison, Cesar; Lopez, Ana Villar, 2010, An Examination Of The Relationship Between Manufacturing Flexibility And Firm Performance: The mediating Role Of Innovation, International Journal of Operations & Production Management, Vol. 30 No. 8, pp. 853-878.

[22]. Hitt, Michael A., Holmes Jr., R. Michael, Holcomb, Tim R. 2006, Diversification to Achieve Scale and Scope: The Strategic Implications of Resource Management For Value Creation, Ecology and Strategy: Advances in Strategic Management, Volume 23 , pp. 549-587.

[23]. Barney, Jay B., Clark, Delwyn N., 2007, Resource-Based Theory: Creating and Sustaining Competitive Advantage, Oxford University Press.

[24]. Pang Changwei, Qiong Wang, Yuan Li, Guang Duan, 2019. Integrative Capability, Business Model Innovation And Performance: Contingent Effect Of Business Strategy, European Journal of Innovation Management.

[25]. Coulthard, Max, 2007, The Role of Entrepreneurial Orientation on Firm Performance and The Potential Influence of Relational Dynamism, Monash University, Working Paper, Download http // www.ssrn.com.

[26]. Indriantoro, Nur and Supomo, Bambang. 2002 Business Research Methodology For Accounting and Management. Yogyakarta; BPFE

A Competitive Study Between Different Cryptographic Algorithms

Ohoud Al-Harthi, Mohammed A. AlZain, Jehad Al-Amri, Mohammed Baz, Mehedi Masud,

Abstract: Encryption is the strategy of blocking message therefore entirely the supposed receiver can browse it. Through the rapid development of digital Information swapping in automatic suggests that data Safety is turning into far additional necessary in information storage and transmission. It's a kind of substitution code throughout which individually and every message interval the plaintext is swapped by a message. Throughout this research, author improved the old Caesar cipher and stuck the key size collectively. Coding and scrambling of the letters at intervals the Cipher Text. Genetic algorithms (GAs) are a category of optimization algorithms. GAs commit to solving issues through modeling a simplified version of genetic processes. There are several issues that a GA approach is beneficial. It is, however, undetermined if cryptology is such a tangle.
General Terms Security, Encryption

Keywords : Decryption, Symmetric Encryption, Plaintext, Cipher Text. Cryptography, Genetic Algorithm, Encryption, Decryption, key, Mutation.

1. INTRODUCTION

1.1. Caesar algorithm

knowledge privacy and security actually frame one in all the foremost significant options of an individual's life [29-40]. One cannot communicate firmly any longer. Encryption means that data is translated into unreadable forms by electronic or digital codes or keys. Only then are the legitimized users the original data fully available again. Cryptography deals with serving to create knowledge safer. Cryptography alongside the protection of data from stealing or alteration is also used for user authentication. Cryptography is the real art of encryption, and there are two main methods used, transposition and substitution. Already the Greeks and Brahmins over 1500 years ago made use of these procedures. In transposition, the letters of a message are merely organized otherwise. The alternative to transposition is a substitution. This technique is most commonly used in today's encryption techniques. For the first time, this method was used for military purposes by Julius Caesar in the Gallic War. In literature, this is referred to as Caesar cipher or simply Caesar. In contrast to classical cryptography, modern cryptography means the methods that are usually used with the use of a computer or special electronic devices. In most cases, binary data on a computer is encrypted or decrypted with programs running on a computer.

Modern cryptography is divided into

1. symmetric encryption (one key)
2. asymmetric encryption (shared key)
3. Coding (no or fixed key)
4. Hashes (checksum method).

The encryption methods that work with a secret key used for coding and decoding are called symmetric methods or secret-key methods. The terms Secret-Key-Cryptography and Secret-Key-Encryption are also common. Almost all symmetric methods are optimized for resource-conserving environments.

- *College of Computers and Information Technology,*
- *Taif University, Saudi Arabia*

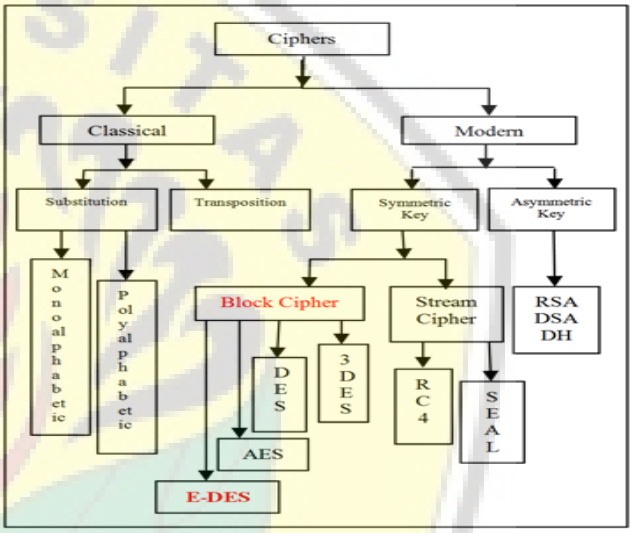

***Figure 1**. The classification of encryption algorithms [27]*

They are characterized by low hardware requirements, low power consumption and easy implementation in hardware. Asymmetrical encryption can be applied to systems in which many users need to encrypt and decrypt a message or record, especially when speed and processing power are not paramount. The necessity of having an algorithm for encryption and decryption has already been reported above, but what is still an essential component is a method of key exchange in connection with checking integrity and authenticity. Caesar encryption (also referred to as Caesar cipher, Caesar algorithm, Caesar shift, shift cipher or Simple Caesar) is a simple symmetric encryption technique based on monographic and monoalphabetic substitution [1] . As one of the simplest and most insecure methods, today it is mainly used to clearly illustrate basic principles of cryptology. For the sake of simplicity, often only the 26 letters of the Latin alphabet without distinction of upper- and lower-case letters are used as the alphabet for plain text and ciphertext, and special characters, punctuation, etc. are disregarded. The name of the Caesar encryption is derived from the Roman general Gaius Julius Caesar, who has used this type of secret communication for his military correspondence according to the tradition of the Roman author Suetonius. Caesar used a shift of the alphabet by 3 letters.

***Figure 2**. Cipher disk for reverse Caesar encryption [22]*

***Table 1.** A scheme of alphabet for encryption messages*

Plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

The subsequent is an example of however the Caesar cipher works. This can be through with a key with the value three. original text: This is a scientific research paper. Cipher: Wklv lv d vflhqwlilf uhvhdufk sdshu. It's simple to envision, however, every character within the plaintext is solely shifted up the alphabet. decoding is simply as simple, by selecting an offset of -3. Cipher: Aol lujyfwapvu thrlz tl ohwwf. Plaintext form: The encryption makes me happy. If another key is used, the encoding alphabet can clearly be shifted by a varied number. As are often seen, owing to its simplicity, the algorithm is susceptible to attacks owing to the repetition and straightforward decoding of the encrypted information. To cypher the plaintext message, we tend to use transformation: Where (x) is the numerical equivalent of a plaintext letter and (n) is the value of key. To decrypt we use the transformation

$$E_n(x) = (x+n) \bmod 26$$

In genetic algorithms, the chromosomes are preferably coded with the Gray code instead of the standard binary code. The
Gray code has a Hamming distance of 1, d. H. distinguish two consecutive code words each in only one binary place. The standard binary code, on the other hand, has different Hamming distances, as the following example illustrates:

***Table 2**. Hamming distance [25]*

decimal	Standard binary code	Gray-Code
0	000	000
1	001 (d=1)	001 (d=1)
2	010 (d=2)	010 (d=1)
3	011 (d=1)	011 (d=1)
4	100 (d=3)	100 (d=1)

In d = Hamming distance (k, k-1)
standard binary code, each binary represents a power of two. By a random mutation in a higher-order place can therefore cause great leaps occur in the phenotype. For example, the two genotypes 1000001 and 0000001 differ only by one binary, the corresponding ones Phenotypes 65 and 1, however, are quite far apart. On the other hand, the Hamming distance between the binary representations 01111 and 10000 five, although the associated types 15 and 16 differ only by one. By using the Gray code, a mutation in the higher-order bits does not affect the phenotypes so severely. However, there are also cases in which the standard binary code has a smaller change in the phenotype than the Gray code causes. Here is an example:

Decimal: 3
Standard binary code: 011
Gray code: 010
After the mutation of the 2nd bit, the following values result:
Standard Binary Code: 001 Gray Code: 000
Decimal: 1 Decimal: 0
Difference: 2 Difference: 3

The mutation-related changes of an allele when using the Gray Code are thus not always less subtle than with the standard binary code.

***Table 3**. A comparison between classic cryptography and modern cryptography techniques [23]*

Classic Cryptography	Modern Cryptography
Works on Characters directly	Works on binary bits (0,1)
The method of securing message is a secret	The algorithms for securing message are public
Entire system is required to be a secret	Only the key needs to be a secret
Less secure	Much more secure

***Table 4**. A comparison between substitution and transposition techniques [24]*

Basis for Comparison	Substitution technique	Transposition Technique
Basic	Replaces the plaintext characters with other characters numbers and symbols.	Rearranges the position of the characters of the plaintext.
Forms	Monoalphabetic and polyalphabetic substitution cipher	Keyless and keyed transposition cipher
Alterations	The identity of the character is changed while its position remains unchanged.	The position of the character is changed in spite of its identity.
Demerit	The letter with the low frequency can discern the plaintext.	Keys near to the correct key can disclose the plaintext.
Example	Caesar Cipher	Reil Fence Cipher

***Table 5**. A comparison between symmetric key and asymmetric key encryption*

Symmetric Key Encryption	Asymmetric Key Encryption
Uses one key for encryption and decryption	Uses two keys (public and private keys) for encryption and decryption
Low power consumption	Higher power consumption

Speed in performance	Slow in performance
Inexpensive to generate	Expensive to generate
Randomly generated k-bits strings	Have special structures E.g.: large prime numbers
E.g.: 1. Advanced Encryption Standard-AES 2. Triple Data Encryption Standard-3DES 3. Twofish 4. Rivest Shamir adleman-RSA	E.g.: 1. X25519 key exchange 2. Elliptic curve cryptography 3. Diffie-Hellman key exchange 4. Digital Signature Algorithm-DSA RSA
Symmetric Key Encryption	Asymmetric Key Encryption

***Table 6**. Comparative between Symmetric Encryption Algorithms [26]*

Factors	DES		3DES	AES	E-DES
Key length (bits)	56		112, 168	128, 192 or 256	1024
Cipher Type	Sym.		Sym.	Sym.	Sym.
Block (bits)	64		64	128	128
Rounds	16		48	10,12,14	16
Developed	1975		1978	1998	2013
Security	Not good		Passing	Secure	Secure
Possible Key	256		2112	2128	21024
Time for Brute Force key attack (1012 keys/sec)	<1 day		1.6x1014 years	1019 years	10152 years
Avalanche effect	Resists		Resists	Resists	Resists
Encryption Software	Fast		Slow	Medium	Very fast
Time to encrypt 48KB	7s		21s	13s	2s

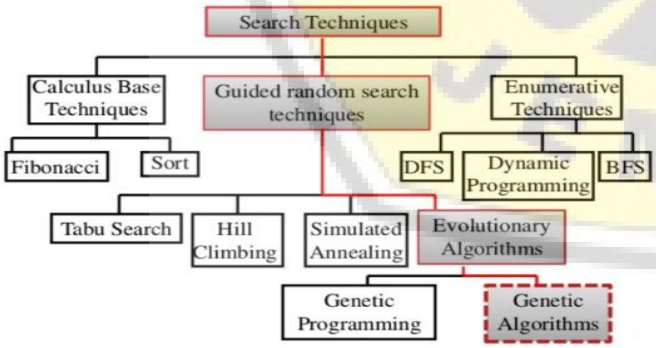

***Figure 3**. The classification of genetic algorithms [28]*

1.2. Genetic Algorithm

Evolutionary algorithms (EA) are optimization methods based on the model of biological evolution. They can be basically in four Divide subareas:

• Evolutionary Strategies (ES)
• Evolutionary Programming (EP)
•Genetic Algorithms (GA)
• Genetic Programming (GP)

Genetic algorithms were first introduced in the early 1960s by John Holland and his staff at the University of Michigan[2]. Approximately, at the same time, Ingo Rechenberg and Hans-Paul Schwefel founded the ¨TU Berlin the evolutionary strategies [3] [4]. The subdivision into the individual Subdivisions is thus mainly historically conditioned, since they have very high ancestors have properties. Nonetheless, there are some differences between the sub-areas in terms of content or center of gravity. For example, in the genetic algorithms, individuals are coded as bit strings, whereas in evolutionary strategies and evolutionary programming, real vectors are usually used. Another difference between the subfields is the selection of the Individuals. Take Genetic Algorithms and Evolutionary Programming a stochastic selection, d. H. also the individuals with a bad one. Fitness value has a, albeit small, chance of passing on their genes to the next generation. In evolutionary strategies, however, a deterministic selection is made; H. only the individuals with the best Fitness pass on their genes. let's look more closely at the biological background, mathematic fundamentals as well as properties and applications of genetic algorithms.

1.2.1. Basic terms from genetics

• Individual / chromosome

An individual in the biological sense is a living organism whose genetic information is stored in a lot of chromosomes. In the context of genetic algorithms, the terms individual and Chromosome but mostly equated. An individual is coded as a binary string of the fixed length n. that's mean we can it as an element of {0, 1} n interpret.

• Gene

A particular sequence of a chromosome is called a gene. Usually, it is clear from the context, whether one understands under a gene single point or a whole section.

• Allele

The specific expression of a gene is called an allele. Will the gene as a variable, the allele is the value of the variables. If the genes denote single digits of the binary string, then the alleles can accept only be the values 0 and 1.

• Length of a chromosome

By the length of a chromosome is meant the length of the binary vector, that's mean, the number of genes of an individual.

• genotype

The genotype is the coded vector of decision variables. By him generally depends on which coding method is chosen.

• phenotype

The phenotype, on the other hand, is the decoded vector of decision variables. Its expression depends on the genotype and the chosen decoding method.

• Population, generation

A set of structurally similar individuals of a particular genus is called a population. When new creatures of this genus are born or others die, so the size of the population is changed. Looking at the populations of one genus over several Times, one speaks of generations of living things.

1.2.2. Building a genetic algorithm

Genetic algorithms can usually be subdivided into the following subroutines:

The problem to be optimized is coded, i.e. it's going to be a binary coded chromosome shown. A population of individuals

is created and initialized randomly. you here speak of the starting population or generation 0. Each individual is evaluated with a fitness function which assigns a real-valued number to each individual chromosome. Two parents each are selected by means of a selected selection variant. From the genetic information of the parents the descendants are generated by means of a chosen crossover variant. The alleles of the offspring can mutate, i.e. their values become inverted. The population is supplemented by the newly produced offspring. Becomes If the size of the population is exceeded, a set of substitutes will be chosen according to a chosen substitution scheme be replaced.
From step 4, the subroutines are repeated until a termination criterion is met.
The GA [5] is also a randomized search and improvement procedure supported the principle of activity systems. 3 rudimentary operators employed in GAs include: selection, crossover, and mutation. The GA goes through the subsequent sequence: valuate, Select, Join and Mutate until some stop conditions are met. Reproduction and crossover along offer give genetic algorithms most of their search benefit.

A. Fitness and evaluation function

The evaluation function measures the goodness of an individual with respect to the task to be optimized, while the fitness function assesses his chances of reproduction. One can equate both functions if the best individuals measured at the optimum should also have the best chance of reproduction.

B. Selection

The selection can be divided into a choice step and a selection step. The selection algorithm assigns each chromosome one Probability value for its replication too.

C. Crossover

The most important genetic operator in genetic algorithms is the crossing operator (also known as the crossover operator). Offspring are produced from two individuals of the parent generation by copying genes of the parents and passing them on to the children. The selection of parents is stochastically successful through one of the already mentioned selection procedures. The crossover probability pc indicates the probability of a cross between the two parents at all. There are various crossroads, which will be discussed in more detail below.

- **N-point crossover**

In contrast to the one-point crossover, there are several intersections here. The first child receives the genes of the first parent to the first intersection, then the corresponding to the next intersection Genes of the second parent. Now, again, the chromosomes of the first the second child, by analogy, receives the chromosomes of the other parent.

- **Template crossover**

In this method, a template in the length of the chromosomes is created by chance at first. The template is made up like the two parents Ones and zeros. The first child will receive this for every 1 in the template speaking allele from the first parent and for each 0 that of the second. At the second child is the behavior at 0 and 1 reversed.

- **Uniform crossover**

In Uniform Crossover, each bit is tested for each bit individually, whether it is between the both parents are exchanged or not.

- **Shuffle Crossover**

In this cross-breeding process, the genes of the parents are first numbered consecutively and then mixed. On the mixed chromosomes is now done a one-point or N-point crossover. Last, the Genes again arranged according to their numbering. The basic GA Cycle has been showed in fig4.

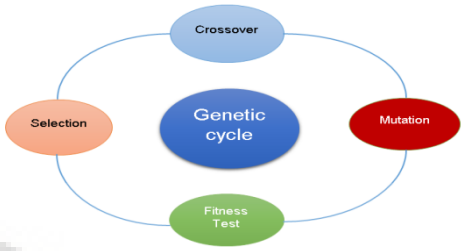

***Figure 4**. Basic Model of Genetic Algorithm [29]*

3. BACKGROUND

genetic algorithm

In [6], expresses that Cryptography is utilized to appreciate limited aims like Privacy, information integrity, Verification etc. of the direct information presently, thus on notice these goals varied cryptologic algorithms area unit developed by varied scientists. For Associate in Nursing awfully nominal quantity of information those procedures wouldn't be value operative subsequently those are not intended for little quantity of information. The purpose of this work was to style and perform a unused algorithmic rule to modify this problem thus we've a determined to don´t have to be compelled to smear those algorithms (which are not lucrative) to cipher very little quantity of information. With this in mind, the planned algorithmic rule has been designed during a fairly easy manner while not neglecting the safety problems. One is employed for each encoding and decipherment, i. e. it's placed beneath the key encoding algorithmic rule, however as a public key. Cryptography is healthier protected then secret key cryptography our subsequent task would be to change and style a public key cryptologic algorithmic rule in a very informal way because it's worked during this research. In [7], states that Cryptography is utilized to appreciate limited aims like Privacy, information integrity, Verification etc. of the send information presently, thus on notice these goals varied cryptologic algorithms area unit developed by varied people. For Associate during a Nursing awfully minimum total of data, those procedures wouldn't be worth current subsequently those aren't calculated for a tiny quantity of data. The aim here was to vogue and tool a spick-and-span rule to handle this issue, therefore, we've got an inclination to tend to don't need to apply those procedures (which aren't lucrative) to cipher a bit quantity of data. Possession this aim in mind the planned rule has been calculated in a fairly simple style however in any case not sacrificing the protection of issues. One is employed for each secret writing and writing i.e. it's fallen below secret key scientific discipline rule, however, because of the public key. In [8], it tosses light-weight that enciphering plays an important role within the excitable development of digital information storage and communication. It's shown the mains of safety goals like confidentiality, integrity, verification, non-repudiation. thus, on notice these goals,

varied cryptologic algorithms area
unit developed. inside this, variety of the algorithms have succeeded et al have failing attributable to lack of security. The algorithmic rule for secret writing is elite supported the kind of knowledge, being interconnected and sort of channel through that knowledge is being interconnected. the foremost persistence of this research is to publicize the essential data regarding science algorithms and comparison of accessible bilateral key cryptography techniques supported approximately strictures like susceptibility to attack, singularity regarding the procedure, etc. In [9] this research the appliance of the GA program for stream cipher is mentioned. The GA program offers the foremost effective resolution and it's about to be applied for generating a casual flow of numbers for ciphering. Irregular vary creating reproduces the generating of Key done by a duplication of genetic method. The key with the uppermost fitness grade is chosen and associated with the beginning price. This work arranges that once the key's generated through a GA it's atomically distinctive and has huge security. throughout my research, a paradigm has stood planned to urge flow cipher key of the stream cipher exploitation genetic formula. the foremost intention of this research is to output irregular and distinctive keys for cryptography and economic performance. Safety is else supplemented because of strictly random keys. In [10], The genetic formula is in short presented and its comprehensive procedure is providing utterly by MATLAB v7 to boot, applying in the improvement of functions and backbone of the compilation is shown concluded 3 examples then the technique of avoiding native improvement by rising the value of pm is else mentioned. The assumed occurrences throughout this text demonstrate that the genetic formula is exercised to hunt out the simplest resolution and to resolve equations and indicate that the genetic formula may even be a powerful world looking tool. therefore, to avoid native best resolution, we've got an inclination to be able to increase the separate amount of mutation and upsurge the inherited generations of a population. In [11], it's mentioned that GAs are supported by process concepts of survival and biology. GAs resolve the issues step by step and manufacture consequent obstetrics. All process algorithms in conjunction with the Genetic formula will notice preparing for to best resolution. a set of check functions in conjunction with unimodal and multimodal benchmark functions is utilized for improvement. In [12] [13] delineate a new approach to cruciate block cryptography noted as ICIGA`s, where the session secret is generated throughout a random methodology. ICIGA`s is associate degree associate extension of the system (GIC). Genetic Algorithms galvanized Cryptography [14].

***Table 7**. A comparison between genetic encryption and another algorithm [28]*

	DES	AES	Genetic Cipher
Encryption Time	068907mm	084440mm	27069mm
Key search space Size	$4.85*10^{28}$ keys	$2.31*10^{57}$	$1.11*10^{120}$
Attack Time(1000k/s)	15.41 thousand trillion days	7.34 hundred million trillion days	3.53 hundred billion billion trillion days

In [15] applied genetic algorithmic rule among the encoding rule using a secret key for the cryptography methodology. In [16] declared that if the standard of the irregular numbers created through the strategy is sweet then the key produced can endlessly robust. The writer used a threshold worth for selection. The constant association is employed to seem at the randomness of the sample. In [17] projected a model that makes the utilization of GA to urge Pseudo- irregular numbers. The cryptography methodology pursues the operation of the crossover operator and mutation operator. It uses the conception of MA (memetic algorithm) and pseud-irregular binary classification. inside the key generation method, 9 strictures of linear congruential generators are utilized. In [18] uses the conception of brain-GAs and a pseudo-irregular binary classification. this methodology of quick wind is very safe and reliable. the randomness of

4. METHODOLOGY

• Original text: typically, this can be often the data to be protected throughout the program.
• Encryption Algorithm: a disciplined sequence of achievement that provides ciphertext for notable original text and encoding key. it is a cryptographical algorithmic rule that takes original text and encoding key as effort and produces the ciphertext.
• Ciphertext: a text or a set of data that has been changed by encryption using the encryption process (hand or device) using a key is that it can no longer understand its content.
• Decryption Algorithm: usually, this may be usually a scientific monotonous that produces original text for ciphertext and cryptography key. it's a cryptanalytic formula that seizes ciphertext and cryptography key as input, and outputs original text. The cryptography formula primarily reverses the cryptography formula and so is closely associated with it.
• Encryption Key: it is a key that is notable to the sender. The despatcher supplements the encoding key hooked on the encoding algorithmic instruction combined with the plaintext in the core to effort out the ciphertext.
• Decryption Key: It's associate article that is noteworthy to the receiver what is more as despatcher. The cryptography key's related with the key of encryption; but it is not repetitively duplicating of it. The receiver delivers the cryptography key into the algorithmic instruction of cryptography in conjunction with the ciphertext accordingly on work out the plaintext.

5. FUTURE WORK

The aim of the analysis was, to style and show a variation of cryptographical algorithms. throughout this study, the discrepancy of the Inherited rule was beleaguered in such some means so as that it will uphold the protection of communication. It reflects that the protection side of the system is extraordinarily sensible. the foremost feature that produces the system a lot of reliable is, the user is in a position to make a decision the secret writing Key. this may increase the atomicity and secrecy of the structure. Meanwhile safekeeping is that the topic towards can rise therefore this study is as long as a compact path to effort towards a genetic algorithms-based undisclosed writing classification. during this

research, the analysis stayed limited up to manuscript messages solely. Consequently, in forthcoming a study for Image, Acoustic, and Audiovisual forms of info will be finished. This analysis totally censorships Still information and Energetic information (Streaming-data) therefore alternative facets of this mixture will stand increased. otherwise a cryptanalytic rule is taken into account economical adequate only if its adequate pledge given in rapports of sanctuary of some information. however, whereas sanctuary will its substance, the time of execution is additionally correspondingly required meanwhile it shouldn't income an excessive amount of time to execute a specific rule. The projected rule as will be gotten from the results affords far improved results than those that are most generally used. Also, it's associate advancing of the quality Caesar-code through on condition that a lot of sanctuary and additionally making certain character like area is additionally concealed. It upholds the crux of the Caesar-code rule within the logic that it confirms fast secret writing and affords larger safety that's an additional extra. Genetic algorithms are a category of improvement ways that use serving to operators of natural evolution manage plenty of answers associated do a quest for an optimum solution in them. She is especially compatible for issues whose actual structure is unknown ("Black Box improvement ") or not resolved in polynomial time will. However, since there are several variants of biological process algorithms, it's definitely a motivation for future analysis comes, alternative applications development areas and to develop new concepts for the answer of improvement issues.

6. REFERENCES

[1] M. Abdalla, J. H. An, M. Bellare, and C. Namprempre, "From Identification to Signatures Via the Fiat–Shamir Transform: Necessary and Sufficient Conditions for Security and Forward-Security," IEEE Transactions on Information Theory, vol. 54, no. 8, pp. 3631-3646, 2008.

[2] J. H. Holland, Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence. MIT press, 1992.

[3] J. Sanchez, R. Correa, H. Buenaño, S. Arias, and H. Gomez, "Encryption techniques: A theoretical overview and future proposals," in 2016 Third International Conference on eDemocracy & eGovernment (ICEDEG), 2016: IEEE, pp. 60-64.

[4] I. Rechenber, "Optimierung technischer Systeme nach Prinzipien der biologischen Evolution," Verlag nicht ermittelbar, 1970.

[5] H.-P. Schwefel, "Optimierung von Simulationsmodellen mit der Evolutionsstrategie," in Simulationsmethoden in der Medizin und Biologie: Springer, 1978, pp. 115-129.

[6] A. Kumar and M. K. Ghose, "Overview of information security using genetic algorithm and chaos," Information Security Journal: A Global Perspective, vol. 18, no. 6, pp. 306-315, 2009.

[7] A.-A. M. Aliyu and A. Olaniyan, "Vigenere Cipher: Trends, Review and Possible Modifications," International Journal of Computer Applications, vol. 135, no. 11, 2016.

[8] G. Matthews, "Elementary Cryptanalysis—A Mathematical Approach. By Abraham Sinkov. Pp. ix, 189. 1968.(Random House.)," The Mathematical Gazette, vol. 54, no. 389, pp. 307-308, 1970.

[9] S. Mewada, P. Sharma, and S. Gautam, "Exploration of efficient symmetric algorithms," in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016: IEEE, pp. 663-666.

[10] A. Sharma, R. Thakur, and S. Jaloree, "Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud," International Journal of Scientific Research in Computer Science and Engineering, vol. 4, no. 5, pp. 5-11, 2016.

[11] W. Stallings, L. Brown, M. D. Bauer, and A. K. Bhattacharjee, Computer security: principles and practice. Pearson Education Upper Saddle River, NJ, USA, 2012.

[12] A. Kumar and K. Chatterjee, "An efficient stream cipher using Genetic Algorithm," in 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016: IEEE, pp. 2322-2326.

[13] C. Guo and X. Yang, "A programming of genetic algorithm in matlab7. 0," Modern Applied Science, vol. 5, no. 1, p. 230, 2011.

[14] C. R. Gaidhani, V. M. Deshpande, and V. N. Bora, "Image Steganography for Message Hiding Using Genetic Algorithm," International Journal of Computer Sciences and Engineering, vol. 2, no. 3, pp. 67-70, 2014.

[15] A. Tragha, F. Omary, and A. Kriouile, "Genetic algorithms inspired cryptography," AMSE Association for the Advancement of Modeling & Simulation Techniques in Enterprises, Series D: Computer Science and Statistics, 2005.

[16] A. Tragha, F. Omary, and A. Mouloudi, "Improved cryptography inspired by genetic algorithms," in ICIGA, 2006 International Conference on Hybrid Information Technology (ICHIT'06).

[17] A. Agarwal, "Secret key encryption algorithm using genetic algorithm," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 4, pp. 216-218, 2012.

[18] S. Goyat, "Genetic key generation for public key cryptography," International Journal of Soft Computing and Engineering (IJSCE) ISSN, pp. 2231-2307, 2012.

[19] F. Ahmad, S. Khalid, and M. S. Hussain, "Encrypting data using the features of memetic algorithm and cryptography," International Journal of Engineering Research and Applications, ISSN, pp. 2248-9622, 2011.

[20] G. N. Rajendra and B. R. Kaur, "A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves," 2011.

[21] S. Prajapat and R. S. Thakur, "Various approaches towards cryptanalysis," International Journal of Computer Applications, vol. 127, no. 14, pp. 15-24, 2015.

[22] https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung, ed.

[23] https://studyflix.de/informatik/hamming-distanz-396, ed.

[24] https://www.youtube.com/watch?v=qaYVyXh4Zlo, ed.

[25] C. Riman and P. E. Abi-Char, "Comparative Analysis

of Block Cipher-Based Encryption Algorithms: A Survey," Information Security and Computer Fraud, vol. 3, no. 1, pp. 1-7, 2015.
[26] https://www.slideshare.net/AMedOs/introduction-to-genetic-algorithms-26956618, ed.
[27] T. Abut, "Dynamic Model And Optimal Control Of A Snake Robot: TAROBOT–," International Journal of Scientific & Technology Research, vol. 4, no. 11, p. 4, 2015.
[28] M. I. Nazeer, G. A. Mallah, N. A. Shaikh, R. Bhatra, R. A. Memon, and M. I. Mangrio, "Implication of Genetic Algorithm in Cryptography to Enhance Security," INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, vol. 9, no. 6, pp. 375-379, 2018.
[29] M. A. AlZain, A. S. Li, B. Soh and M. Masud, Byzantine Fault- Tolerant Architecture in Cloud Data Management, International Journal of Knowledge Society Research (IJKSR), 7 (2016), pp. 86-98.
[30] M. A. AlZain, A. S. Li, B. Soh and M. Masud, Managing Multi- Cloud Data Dependability Faults, Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth, IGI Global, 2019, pp. 207-221.
[31] M. A. Alzain and E. Pardede, Using multi shares for ensuring privacy in database-as-a-service, 2011 44th Hawaii International Conference on System Sciences, IEEE, 2011, pp. 1-9.
[32] M. A. AlZain, E. Pardede, B. Soh and J. A. Thom, Cloud computing security: from single to multi-clouds, 2012 45th Hawaii International Conference on System Sciences, IEEE, 2012, pp. 5490-5499.
[33] M. A. AlZain, B. Soh and E. Pardede, A byzantine fault tolerance model for a multi-cloud computing, 2013 IEEE 16Th International Conference On Computational Science And Engineering, IEEE, 2013, pp. 130-137.
[34] M. A. AlZain, B. Soh and E. Pardede, Mcdb: using multi-clouds to ensure security in cloud computing, 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, IEEE, 2011, pp. 784-791.
[35] M. A. AlZain, B. Soh and E. Pardede, A new approach using redundancy technique to improve security in cloud computing, Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), IEEE, 2012, pp. 230-235.
[36] M. A. AlZain, B. Soh and E. Pardede, A new model to ensure security in cloud computing services, Journal of Service Science Research, 4 (2012), pp. 49-70.
[37] M. A. AlZain, B. Soh and E. Pardede, A survey on data security issues in cloud computing: From single to multi-clouds, Journal of Software, 8 (2013), pp. 1068-1078.
[38] M. A. AlZain, Data security, data management and performance evaluation in a multi-cloud computing model, (2014).
[39] M. A. AlZain, Utilization of Double Random Phase Encoding for Securing Color Images, International Journal of Computer Applications, 975 (2018), pp. 8887.
[40] M. A. AlZain and J. F. Al-Amri, Application of Data Steganographic Method in Video Sequences Using Histogram Shifting in the Discrete Wavelet Transform, International Journal of Applied Engineering Research, 13 (2018), pp. 6380-6387.

Financial Fraud Prediction Models: A Review Of Research Evidence

V.K.Wadhwa, A.K.Saini, S.Sanjay Kumar

Abstract: Despite reports about significant advances in techniques for prediction of financial frauds research findings till now do not provide specific evidence or tools for predicting frauds that could be averted. Researchers have explored different methods with varied degree of success relying on financial data as well as non-financial factors for their purpose. This paper reviews reported models/evidence including adaptations/improvements in the models used during investigation. Fraud triangle theory specified by Cressey in 1953 is at the foundation applied in empirical predictive modelling postulated by a number of researchers. Prominent contributors are Beasley, M.S. (1996)., Dechow, et al. (1996).,Beneish M. D. (1997)., Nieschwietz et al. (2000), Skousen and Wright (2008). Convergence of fraud triangle theory to fraud diamond theory was suggested by Wolf and Hermanson in 2004. This paper additionally reviews specific computational models known as Z-Score (Altman,1968), M-Score (Beneish, 1999, 2012), and computer software based models from Green B.P. & Choi J.H.(1997) Zaki & Theodoulidis (2013) and Arta & Seyrek, (2009). There is a noticeable changing trend in research going towards numerous investigations now using computer supported machine learning and artificial intelligence tools for prediction of financial frauds. At the end an assessment is made about degree of success achieved in prediction of financial frauds till date. Empirical fraud prediction, Fraud Triangle/Diamond, M-Score, Z-Score, Machine Learning & Artificial Intelligence for fraud prediction.

Index Terms: Empirical fraud prediction, Fraud Triangle/Diamond, M-Score, Z-Score, Machine Learning & Artificial Intelligence for fraud prediction.

1. INTRODUCTION

THIS review finds out the extent and effectiveness of models used for detection/prediction of financial frauds. An attempt is made to compile available literature connected with prediction of financial frauds. It is assumed that forecast of any phenomenon is dependent on a number of inputs which also interact inter-se in a complex manner. Hence visible outcome may conceal underlying causes. The challenge is to discover well in advance the possibility of occurrence of a financial fraud. To predict occurrence of financial fraud from time to time number of factors, evident, non evident, hidden have been explored by researchers with varying degree of success. Most common and classical method relies on empirical analysis to trace the possibility of fraudulent behaviour. The following part of this paper contains individual sections separately devoted to each model found in the research. Firstly proponents of empirical prediction of financial frauds through a set of observable fraud cues are reviewed. Secondly computational models based on financial information are reviewed. These are primarily two models i.e. M-Score and Z-Score. Lastly, machine learning/artificial intelligence as a tool to predict financial frauds is reviewed.

1.1 Empirical Research on prediction of financial frauds:-

A set of predetermined standard steps/procedure cannot be applied to predict financial frauds. Auditors generally are trained to routinely follow certain standard procedure to improve effectiveness of auditing. Nieschwietz et al. (2000) reported that check lists used by auditors provide an insight into the likelihood of financial fraud. The authors further discuss that the environment in which auditors operate is assessed through the checklist and research on the predictors of fraud centres around empirical tests of validity of fraud indicators. Evidence is also presented by the authors about the detailed fraud risk assessment undertaken by the auditors at the planning stage of auditing process. Nieschwietz et al. (2000) observed in this context of auditing that the professional requirements of an auditor ensures to put in place a fraud risk management program consisting of written policies of fraud risk measurement. The scale of such measurement may include objective computation of fraud risk score or some kind of fraud risk index which is essentially in quantitative terms. The research aims to examine and get empirical evidence with respect to internal control and internal auditing. Core structure of internal auditing alongwith design of management control system plays a crucial role in measurement of likelihood of financial fraud is pointed out by the authors in the research paper. Consistent with the aforesaid finding Albrecht and Romney (1986) published their first empirical study establishing major role of red flags to predict financial frauds. Authors in their research paper entitled “Red-flagging management frauds: A validation” documented the evidentiary value of red flags for prediction of financial frauds. Surveys conducted by authors demonstrated effectiveness of red flagging to predict financial frauds. Finding of the researchers prove relevance of formation of Ex-ante warning signs of a possible financial fraud. Contribution of the authors provides attributes to red flags in predicting financial frauds. Inference of researchers support relevant professional knowledge is the key to development of mechanism of prediction of financial frauds. The study of Albrecht and Romney (1986) further argues that frauds are inherent in the organisations and skilful people can at the most reduce the likelihood of financial frauds. Financial frauds cannot be completely eliminated. Association of Certified Fraud Examiners (ACFE) is an anti-fraud organisation situated in USA providing training and education. ACFE has conducted detailed studies of fraudulent occurrences of financial statement frauds to recognize such financial statement which are manipulated. ACFE has also enlisted some of the most frequently used tactics to perpetuate frauds in financial statements. Financial statements can be manipulated in various ways. ACFE has declared one of top most cause of fraudulent manipulation is greed and secondly it is the work pressure. Causes identified by ACFE include two prime circumstantial factors which are firstly ‘when it is easy to do it’ and secondly ‘when it is unlikely that perpetrator will get caught’. ACFE enlisted five basic types of financial statement frauds as under:

***Table-1**: Types of financial frauds*

S.No	Type of fraudulent activity
1.	Fictitious sales
2.	Improper expense recognition

3.	Incorrect asset valuation
4.	Hidden Liabilities
5.	Unsuitable disclosures

These kinds of activities are planned in such a way that they are difficult to trace in the normal course of audit. Only comprehensive forensic audit may bring such activities to light. ACFE enlisted the following red flags for fraud risk examiners

***Table-2**: Red Flags*

S.No.	Basis of Fraud Red Flag
1.	Growth in revenues without matching rise in cash flows
2.	Steady sales growth although well-known competitors are facing though time.
3.	Baffling rise in sale along with growing inventories. Useless stock of goods may be shown as future sale.
4.	Rising profit margin whereas the industry is in downtrend.
5.	Overstated life of fixed assets. Change in accounting policies without genuine reasons.
6.	Weak internal audit and control.
7.	Frequent violation of terms and conditions of loan or at the verge of default.
8.	Replacement of auditors without genuine reasons.
9.	Related party transaction not disclosed to auditors.
10.	Different ratios of financial statement over a period of time.

1.2 Fraud Triangle as predictor of financial frauds:-

Empirical research on frauds goes back to 1953 when Cressey presented with the idea of fraud triangle (Cressey, D 1953). The three aspects of fraud triangle are (i) Opportunity, (ii) Pressure and (iii) Rationalisation. Empirical research suggests that the three components of triangle can be broken down to specific measurable items and then possibility of financial frauds can be deduced from the items. These items can be called proxies of the three corners of the fraud triangle. Skousen et al. (2008) evaluated influence of fraud triangle through proxies of one part of triangle called Pressure by subdividing the concept of pressure by way of computation of (i) Gross profit margin (ii) change in sales of the company in comparison to the average change in the industry and (iii) percentage change in the assets for the two years prior to fraud. The authors say that the company face pressure to commit fraud when financial stability or profitability is under threat. The threat may be due to external factors. Albrecht (2002) suggested that sales to accounts receivable ratio along with sales to total assets ratio and inventory to total sales represent pressure. Proxies of external pressure refer to demand for financing vis-a-vis internal cash generation (Dechow et al. 1996) adjusted by cash dividend and capital expenditure. Thus it can be stated that the pressure in terms of financial performance is whether the company is in a position to meet its financial targets or not. Opportunity is the next factor of fraud triangle. Proxies of 'Opportunity' refer to ineffective internal control system. Variable to measure opportunity include firstly the percentage of board members who are outside member. Oversight of audit committee by an independent member of board is known to have reduced incidence of fraudulent behaviour (Beasley et al. 2000). Proxies of 'Rationalization' proxies include the excessive use of discretionary accruals and the resultant qualified audit reports. Fraud diamond theory was first presented by Wolfe and Hermanson (2004) who added one more dimension to fraud triangle theory by adding capability as fourth aspect of motivation for incidence of frauds. It means that the perpetuator of financial fraud must have the necessary skill and ability to commit fraud.

2 COMPUTATIONAL MODELS:-

2.1 Altman Z-Score Model as predictor of financial failure:-

Altman published Z-Score formula in 1968. It is a computational method of predicting if the firm is likely to be bankrupt within next two years. The formula given by Altman is :-

$$Z=1.2(T1)+1.4(T2)+3.3(T3)+0.6(T4)+0.999(T5)$$

Where:

T1 = Working Capital/Total Assets
T2= Retained Earnings/Total Assets
T3=Earnings Before Interest and Taxes/Total Assets
T4=Market Value of Equity/Total Liability
T5=Sales/Total Assets

If Z is greater than 2.99 it is considered safe zone and if Z is between 1.81 to 2.99 it is considered grey zone and if Z is less than 1.81 it is considered distress zone.

If the firms happens to be unlisted not having a market value than the market value gets substituted with book value of the firm. Similarly there will be small modification in the formula for non-manufacturing companies and financial sector companies. Altman Z-score would have predicted in advance fraudulent behaviour of Enron as per the published financial statements of Enron. In this it was established that financial failure could have been predicted with the publically available published financial statements.

2.2 Beneish M-Score Model for prediction of financial frauds relating to earnings manipulation:-

Professor M Danial Beneish from Kelley School of Business published a path breaking research paper in 1999. He found out that a set of financial ratio and eight variables can identify financial frauds relating to earning manipulation. Since all the required input is obtainable from the published financial statements of the company the whole process of prediction becomes very practical and convenient. The variables used in computation of M-score are as under:-

S.No.	Variable	Meaning of Variable
1.	DSRI	Days' sales in receivable index
2.	GMI	Gross margin index
3.	AQI	Asset quality index
4.	SGI	Sales growth index
5.	DEPI	Depreciation index
6.	SGAI	Sales and general administrative. Expenses
7.	LVGI	Leverage index
8.	TATA	Total accruals to total assets

If M-Score is less than -2.22 it shall mean company has not manipulated earnings and M-Score greater than 2.22 shall mean there is a good chance of manipulation of earnings. This model has been applied all over the world by a large number of other researchers confirming reasonable accuracy of the model. Results obtained in India are not much at variation.

3 COMPUTER BASED ADVANCED SOFTWARES:-

3.1 MACHINE LEARNING/ARTIFICAL INTELLIGENCE/DATA MINING (HEREIN AFTER ML/AI/DM) FOR PREDICTION OF FINANCIAL FRAUDS:-

Sharma A and P.K.Panigrahi (2012) has observed that advancement of computer technology has brought about major change in methods of prediction of financial frauds. They have noted that ML/AI/DM have occupied a centre stage now in devising procedures for prediction of financial frauds. ML/AI/DM methods are divided into two categories of models called supervised methods and unsupervised methods. Green and Choi (1997) presented in their research article entitled "Detecting management fraud through neural network technology" a technique to find out fraudulent activity from the published financial statements. Green and Choi (1997) initially from the data of fraud firms fed input values to the machine learning software in order to train the software subsequently the trained software were applied on raw data to filter possibility of incidence of financial frauds. The process involves feeding of data to the machine for the machine to learn and subsequently apply the learnt algorithm to test the unknown situation to show generalised rules being applied for prediction of financial frauds. Consistent with Green and Choi (1997), Juszezak et al.(2008) concluded the problem of prediction of financial frauds can be considered as a problem of classification. By classifying unknown firms in two parts as fraudulent firms and non fraudulent firms we can predict that a firm is likely to engage in fraudulent activity or not. Authors pointed out that the machine learning models improve their performance with experience. In some cases the coefficient are computed at the time of feeding of data and in some other cases the processing is lazy because the updating is done while the data is being processed.

3 CONCLUSION:

Varied models examined in this paper provide inclusive evidence about the most accurate method of prediction of financial fraud. Most of the models lack generalisation potential because of over dependency on small size of data. All the models are highly data bias and therefore low in generalisation. It is a serious limitation which can be overcome only if large data size is available for dispensation. Finally it can be concluded that none of model could provide perfect solution for prediction of financial frauds and there is a lot yet to be done. However future is quite promising in view of available latest tools particularly machine learning and artificial intelligence is titivating all along.

REFERENCES

[1] A. Sharma and P. Kumar Panigrahi, (2012) review of financial accounting fraud detection based on data mining techniques, International Journal of Computer Applications, vol. 39, no. 1, pp. 37–47.

[2] Abbott, L.J., S. Parker, and G.F. Peters. 2004. Audit Committee Characteristics and Restatements. Auditing: A Journal of Practice & Theory 23: 69-88.

[3] Aghghaleh, S.F., Z.M. Mohamed, and M.M. Rahmat. 2016. Detecting Financial Statement Frauds in Malaysia: Comparing the Abilities of Beneish and Dechow Models. Asian Journal of Accounting and Governance 7: 57-65.

[4] Albrecht, W. S. and M. B. Romney (1986) Red-flagging management fraud: A validation. Advances in Accounting 3: 323-334

[5] Altamuro, J., A. L. Beatty, and J. Weber. 2005. The Effects of Accelerated Revenue Recognition on Earnings Management and Earnings Informativeness: Evidence from SEC Staff Accounting Bulletin No. 101. The Accounting Review 80: 373-401.

[6] Altman, E.I. 1968. Financial Ratios, Discriminant Analysis and the Prediction of Corporate Bankruptcy. The Journal of Finance 23 (4): 589-609.

[7] American Institute of Certified Public Accountants (AICPA). 1997. Considerations of Fraud in a Financial Statement Audit Statement on Auditing Standards No. 82. New York, NY: AICPA.

[8] American Institute of Certified Public Accountants (AICPA). 2002. Considerations of Fraud in a Financial Statement Audit Statement on Auditing Standards No. 99. New York, NY: AICPA.

[9] Baucus, M.S. & Near, J.P. 1991. Can illegal corporate behaviour be predicted? An event history analysis. Academy of Management Journal. 34(1):9-36.

[10] Bayley, L., & S.L. Taylor. 2007. Identifying Earnings Overstatements: A Practical Test. Working paper.

[11] Beasley, M. S., Carcello, J. V., Hermanson, D. R., & Lapides, P. D. (2000). Fraudulent financial reporting: Consideration of industry traits and corporate governance mechanisms. Accounting Horizons, 14(4), 441-454.

[12] Beasley, M.S. 1996. An Empirical Analysis of the Relation Between the Board of Director Composition and Financial Statement Fraud. The Accounting Review 71: 443-465.

[13] Beasley, M.S. 1996. An empirical analysis of the relation between the board of director composition and financial statement fraud. The Accounting Review 71 (October): 443-464

[14] Beasley, M.S., J.V. Carcello, and D.R. Hermanson. 1999. Fraudulent Financial Reporting: 1987-1997. An Analysis of US Public Companies. Committee of Sponsoring Organizations of the Treadway Commission (COSO)

[15] Beasley, M.S., J.V. Carcello, D.R. Hermanson, and T.L. Neal. 2010. Fraudulent Financial Reporting: 1998-2007. An Analysis of US Public Companies. Committee of Sponsoring Organizations of the Treadway Commission (COSO)

[16] Bell, T.B., and J.V. Carcello. 2000. A Decision Aid for Assessing the Likelihood of Fraudulent Financial Reporting. Auditing: A Journal of Practice & Theory 19 (1): 169-184.

[17] Beneish, M.D. 1999. The Detection of Earnings Manipulation. Financial Analysts Journal 55 (5): 24-36.

[18] Bhasin M. L. (2012). Corporate Accounting Frauds: A Case Study of Satyam

[19] Bonner, S.E., Z-V. Palmrose, and S.M. Young. 1998. Fraud Type and Auditor Litigation: An Analysis of SEC Accounting and Auditing Enforcement Releases. The Accounting Review 73 (4): 503-532. 89

[20] Brazel, J.F., K.L. Jones, and M.F. Zimbelman. 2009. Using Nonfinancial Measures to Assess Fraud Risk. Journal of Accounting Research 47 (5): 1135-1166.

[21] Brazel, J.F., K.L. Jones, J. Thayer, and R.C. Warne. 2015. Understanding Investor Perceptions of Financial Statement Fraud and their Use of Red Flags: Evidence from the Field. Review of Accounting Studies 20: 1373-1406.

[22] Callen, J.L., S.W. Robb, and D. Segal. 2008. Revenue Manipulation and Restatements by Loss Firms. Auditing: A Journal of Practice & Theory 27: 1-29.

[23] Cohen, J.R., L.L. Holder-Webb, L. Nath, and D. Wood. 2012. Corporate Reporting of Nonfinancial Leading Indicators of Economic Performance and Sustainability. Accounting Horizons

26 (1): 65-90.
[24] Cressey, D. R. (1953). Other People's Money. Montclair, NJ: Patterson Smith, pp.1-300.
[25] Dechow, P.M, R.G. Sloan, and A.P. Sweeney. 1996. Causes and consequences of earnings manipulation: An analysis of firms subject to enforcement actions by the SEC. Contemporary Accounting Research, Vol 13, no. 1, pp. 1-36.
[26] Dechow, P.M. and A. Sweeney. 1995. Detecting Earnings Management. The Accounting Review 70: 193-225.
[27] Dechow, P.M., W. Ge, C.R. Larson, and R.G. Sloan. 2011. Predicting Material Accounting Misstatements. Contemporary Accounting Research 28: 17-82.
[28] Elda du Toit (2208) Characteristics of companies with a higher risk of financial statement fraud: A survey of the literature. South African Journal of Accounting Research, Volume 22, 2008-issue 1,pages 19-44
[29] Farber, D. 2005. Restoring Trust After Fraud: Does Corporate Governance Matter? The Accounting Review 80: 539-561.
[30] Feroz, E.H., K. Park, and V.S. Pastena. 1991. The Financial and Market Effects of the SEC's Accounting and Auditing Enforcement Releases. Journal of Accounting Research 29: 107-142.
[31] Francis, J., D. Philbrick, and K. Schipper. 1994. Shareholder Litigation and corporate Disclosures. Journal of Accounting Research 32 (Autumn): 137-164.
[32] Green B.P. and Choi J.H.,(1997). Assessing the risk of management fraud through neural network technology, Auditing: A journal of Practice and Theory, Vol. 16(1), 14-28
[33] Gul F.A., Lynn S.G., Tsui J.S.L. (2002), Audit quality management ownership and the informativeness of accounting earnings, Journal of Accounting, Auditing and Finance, Vol. 17, No.1, pp. 25-49.
[34] Gupta P.K.,Gupta Sanjeev, (2015),'Corporate frauds in India – perceptions and emerging issues', Journal of Financial Crime, Vol 22, Iss 1.pp. 79-133.
[35] Hogan, C.E., Z. Rezaee, R.A. Riley, Jr., and U.K. Velury. 2008. Financial Statement Fraud: Insights from the Academic Literature. Auditing: A Journal of Practice & Theory 27 (2): 231-252.
[36] ICSI (2007), The Institute of Company Secretaries of India, Guidance Note on Corporate Governance Certificate, ICSI, New Delhi.
[37] Jones, J. 1991. Earnings Management during Import Relief Investigations. Journal of Accounting Research 29: 193-228.
[38] Juszczak, P., Adams, N.M., Hand, D.J., Whitrow, C., & Weston, D.J. (2008). Off-the-peg and bespoke classifiers for fraud detectionll, Computational Statistics and Data Analysis, vol. 52 (9): 4521-4532
[39] Kaminski, K.A., and T.S. Wetzel. 2004. Financial Ratios and Fraud: An Exploratory Study using Chaos Theory. Journal of Forensic Accounting V: 147-172.
[40] Kaminski, K.A., T.S. Wetzel, and L. Guan. 2004. Can Financial Ratios Detect Fraudulent Financial Reporting? Managerial Auditing Journal 19 (1): 15-28.
[41] Marquardt, C.A., and C.I. Wiedman. 2004. How Are Earnings Managed? An Examination of Specific Accruals. Contemporary Accounting Research 21: 461-491.
[42] Nieschwietz, Robert J., Joseph J. Schultz, Jr. and Mark F. Zimbelman, Empirical Research on External Auditors' Detection of Financial Statement Fraud. Journal of Accounting Literature Vol. 19, 2000: pp 190-246.
[43] OECD (1999) Principles of corporate governance 1999, OECD
[44] OECD (2004) Principles of corporate governance 2004, OECD
[45] Palmrose, Z-V. 1988. An Analysis of Auditor Litigation and Audit Service Quality. The Accounting Review 63 (January): 55-73.
[46] Public Company Accounting Oversight Board (PCAOB). 2010. Identifying and Assessing Risks of Material Misstatement Accounting Standard No. 2110. Washington, DC: PCAOB
[47] PWC's 2018 Global Economic Crime and Fraud Survey.
[48] Rathinaraj D. (2010). Financial fraud, cyber scams and India – A small survey of popular recent cases, Anna University of Technology, Chennai.
[49] Rezaee, Z. 2005. Causes, Consequences, and Deterrence of Financial Statement Fraud. Critical Perspectives on Accounting 16: 277-298.
[50] Securities and Exchange Commission (SEC). 1999. Revenue Recognition. Staff Accounting Bulletin No. 101. Washington D.C.: Government Printing Office.
[51] Skousen, Christopher J., Charlotte J Wright,(2008) Contemporaneous Risk Factors and The prediction of Financial Statement Fraud, Journal of Forensic Accoutning IX:37-62
[52] Skousen, Christopher J., Kevin R. Sminth, and Charlotte J. Wright (2009). "Detecting and Predicting Financial Staement Fraud: The Effectiveness of the Fraud Triangle and SAS No. 99". SSRN Working Paper Series Feb
[53] Trompeter, G., T. Carpenter, N. Desai, K. Jones, and R. Riley. 2013. A Synthesis of Fraud Related Research. Auditing: A Journal of Practice and Theory 32: 287-321.
[54] Verma Gakhar, D. (2013). Earnings management practices in India: A study of auditor's perception. Journal of Financial Crime, 21(1), 100-110.
[55] Wells, J.T. 1990. Six common myths about fraud. Journal of Accountancy. 169(2):82-88.
[56] Zmijewski, M.E. 1984. Methodological Issues Related to the Estimation of Financial Distress Prediction Models. Journal of Accounting Research 22: 59-82