May-June 2020
ISSN: 0193-4120 Page No. 3866-3872

A Study on Cyber Security by Means of Machine Learning and Deep Learning Techniques

[1]Soundharya.M, [2]Vijaya Kumar H, [3]Thirunavukkarasu.V
[1]Student of MCA, REVA UNIVERSITY, Bengaluru, Karnataka, India
[2]Assistant Professor, School of CSA, REVA UNIVERSITY
[3]Assistant Professor, School of CSA, REVA UNIVERSITY
[1]soundharya.m897@gmail.com, [2]vijayakumarh@reva.edu.in, [3]arasu_mca3@yahoo.com

Article Info
Volume 83
Page Number: 3866-3872
Publication Issue:
May-June 2020

Article History
Article Received:*19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *12 May 2020*

Abstract
In past decade computer-based intelligence (ML) and significant learning (DL), has delivered overpowering assessment premium and pulled in momentous open thought. With the extending compromise of the Internet and open movement, there is change in how people learn and work, anyway it furthermore opens them to real security perils. It is an inciting task to guarantee delicate information, data, framework and PCs related structures from the unapproved cyberattacks. Hence, convincing advanced security is required. Continuous progressions, for instance, machine learning and significant learning are composed with cyberattacks to offer response for this issue. The paper contemplates machine learning and significant learning in computerized security in like manner it analyses the troubles and odds of using ML/DL and offers proposition to look at orientation

Keywords: *Cyber security, Machine learning, Deep learning, Intrusion detection.*

.

1. Introduction

Before long structure related by web, for instance, the hardware, programming and data can be protected from cyberattacks by techniques for advanced security. Cybersecurity is a ton of advances and methodology planned to guarantee PCs, frameworks, ventures and data from attacks and unapproved access, change, or pummelling. As perils become more propelled the most recent advances, for instance, Machine learning (ML) and significant learning (DL) are used in the cybersecurity system to utilize security limits. Nowadays, advanced security is a fortifying issue in the computerized space, and it has been endless supply of different application spaces, for instance, reserves, industry, remedial, and various other huge districts [11]. To perceive distinctive frame work ambushes, particularly not as of late watched attacks, is a key issue to be settled critically [1]. This paper oversees past work in simulated intelligence (ML) besides, significant learning (DL) systems for cybersecurity applications besides, a couple of uses of each system in advanced security assignments are depicted. The ML and DL procedures covered in this paper are material to recognize advanced security risks, for instance, software engineers and predators, spyware, phishing and orchestrate interference revelation in ML/DL. Appropriately, remarkable perceptible quality is put on a escalated depiction of the ML/DL methods, and references to essential works for each ML and DL procedure are given [1]. In addition, talk about the challenges and odds of using ML/DL for cybersecurity. The rest of the audit is sifted through as follows: Zone II tells about computerized security, Section III is shaped of man-made intelligence, Fragment IV contains outline on Significant
learning and Zone V gave to similarities and differentiates among man-made intelligence and Significant learning.

2. Cyber Security

Security of frameworks, PC related devices, activities, and data from pernicious attacks or unapproved find a good pace of advances is known as computerized security. Computerized security can be typically

May-June 2020
ISSN: 0193-4120 Page No. 3866-3872

insinuated as information advancement security. Information can be fragile
information, or various types of data for which unapproved find a workable pace. During the time went through synchronizing with new prospective advances, security examples and threat
Information computerized security are at high peril. Regardless, it is essential to shield information and data from cyberattacks, to keep up advanced security.
A. Challenges of cybersecurity
There are various challenges in the field of computerized security. One of the most testing parts of cybersecurity is the changing nature of security perils. Generally verifying the best known threats and not verifying structures against less unsafe perils was approach against caring for advanced
security.

Figure 1: Areas covered in cyber Security

Application security: To shield applications from perils begin from blemishes in the application structure, improvement, course of action, redesign or upkeep through moves that are made during the improvement life-cycle is known as application security. Some essential methods used for application security are:
1. Information parameter endorsement.
2. Customer/Employment Approval and Endorsement.
3. Session the officials, parameter control and
unique case the administrators.

Information security: It shields information from unapproved access to save security. Methods used are:
1. Conspicuous evidence, confirmation and endorsement of customer.
2. Cryptography.
Disaster recovery masterminding: It is a method that contains performing risk assessment, making needs, progressing recovery approaches in case of a cataclysm.
Framework security: Framework security joins exercises that are used to guarantee the convenience, resolute quality, dependability besides, prosperity of the framework. Security parts include:
1. Threatening to contamination and against spyware.
2. Firewall, to square unapproved access to your sort out.
3. To perceive fast spreading risks, and Virtual Private Frameworks (VPNs) and to give secure remote access interference evasion structures (IPS) is required.

Sorts of cybersecurity risks

Figure 3: Types of Cyber Threats

A cyberattack is a purposeful corruption of PCs besides, servers, electronic structures, frameworks and data. Cyberattacks uses fake code to change exceptional PC code, justification or data, achieving troublemaking results that lead to cybercrimes. Extreme target of computerized security is to prevent cyberattacks.
Following are some customary sorts of advanced risks:

- Kind of development that incorporates an aggressor hacking system records through encryption and mentioning a portion to unscramble is known as Ransomware.
- Malware is any record or program used to hurt a PC customer, for instance, worms, PC diseases,
- Trojan horses and spyware.
- Worms look like diseases in that they are self-copying
- An ambush that relies upon human relationship to hoodwink customers for breaking security to increment sensitive is Social building.
- A disease is a touch of pernicious code that is stacked onto a machine without the customer's data. It spread to other PCs by joining itself to another PC report.
- Spyware/adware can be presented on PC without data on customer when associations is opened or clicked or downloaded it sullies the item and assembles singular information.
- Trojan contamination is performing noxious development when executed.
- Phishing is a sort of coercion where phishing attacks are sent by methods for email and solicitation that customers click on an association

May-June 2020
ISSN: 0193-4120 Page No. 3866-3872

and enter their singular data. Nevertheless, the point of these messages is to take unstable data, for instance, charge card or login information. There is a concerning factor about phishing that phishing messages have gotten perplexing and every now and again look basically like authentic requesting for information.

3. Machine Learning

AI (ML) permits programming applications to foresee results without being expressly customized by utilization of a calculation or gathering of calculations. The machine learning assembles calculations for accepting info information and employments factual examination to foresee a yield while refreshing yields as new information gets accessible. Earlier work in digital security dependent on AI and computerized reasoning I s displayed underneath. Liu et al., distributed a precise report on security concerns with an assortment of AI procedures. The current security assaults investigated towards AI from two perspectives, the preparation stage and the testing/inducing stage [2]. Moreover, classification dependent on current guarded procedures of AI into security appraisal instruments, countermeasures in the preparation stage, those in the testing or gathering stage, information security what's more, security is finished. Paper exhibited by Fraley and Dr.Cannady gives better comprehension of how AI could be utilized to order different security occasions and cautions. They created model to respond to security occasions by alarming SMEs, alarming examiners or creating reports depending upon the seriousness of the security occasion. Extra help for digital resistance was examined to additionally diminish the time interest for reacting to basic security occasions [3]. Merat et al. introduced various kinds of PC forms that can be mapped inperforming various tasks condition for the improvement of AI. SHOWAN model created by them was utilized to become familiar with the digital mindfulness conduct of a PC procedure against different simultaneous strings [4]. The analysed procedure begins to beat, and would in general deal with various undertakings inadequately, however it steadily figured out how to gain and control assignments, with regards to abnormality recognition. At long last, SHOWAN plots the unusual exercises of physically anticipated errand and contrast and stacking patterns of different undertakings inside the gathering. In the article, a diagram of applying AI to address difficulties in developing vehicular systems was displayed by Ye et al. This paper presented nuts and bolts of

AI, including significant classifications and delegate calculations in a word. Some primer instances of applying AI in vehicular systems to ease information driven dynamic utilizing fortification learning was distributed [5]. Some open issues for additional examination likewise featured right now. A precise of the difficulties related with machine learning with regards to large information and order dependent on the V measurements of large information was distributed by L'Heureux also, Grolinger [7]. A diagram of ML approaches and how these methods beat the different difficulties were talked about right now. The utilization of the huge information to arrange the difficulties of AI empowers the making of cause-impact associations for every one of the issues. Further, the formation of unequivocal relations among approaches and challenges empowers a progressively exhaustive comprehension of ML with digital security.

Golam et al., consider an information driven cutting edge remote arrange model, where the MNOs utilizes propelled information investigation, ML and computer-based intelligence are utilized for proficient activity, control, and streamlining. How ML, computer-based intelligence and computational knowledge assume their significant jobs in information examination for cutting edge remote systems are talked about right now paper. A lot of system structures and improvement plans concerning information investigation are exhibited [8]. Feng and Wu displayed a client driven AI framework which use enormous information of different security logs, alert data, and investigator bits of knowledge to the distinguishing proof of unsafe client. Framework gives a total system and answer for dangerous client recognition for big business security activity focus

[12]. Creates marks from SOC examination notes, to relate IP, host, and clients to create client driven highlights, to choose AI calculations and assess exhibitions, just as an AI framework in SOC creation condition was quickly presented. The entirety AI framework is actualized underway condition and completely robotized from information procurement, day by day model invigorating, to ongoing scoring, which enormously improve and upgrade undertaking hazard recognition and the executives. With regards to the future work, learning calculations was proposed for additional improvement of the location precision. Innovative patterns in irregularity recognition and distinguishing proof what's more, open issues and difficulties in irregularity identification frameworks and half-breed interruption recognition frameworks was talked about by Patcha et al. In any case, the overview just covers papers distributed from 2002 to 2006. Not at all like Modi C et al., this survey covers the use of ML/DL in different regions of interruption recognition and isn't restricted to cloud security. [1]. Buczak et al. proposed AI strategies and their applications to distinguish interruption [1]. Calculations like Neural Systems, Bolster Vector Machine, Hereditary Calculations, Fluffy Rationales, Bayesian Systems and Choice Tree are likewise portrayed in paper.

AI strategies are coarsely isolated into three significant classes as regulated, unaided, and fortification learning. There are two stages in machine

May-June 2020
ISSN: 0193-4120 Page No. 3866-3872

learning for example preparing and testing. In the preparation organize, a model is scholarly founded on preparing information, while in the testing stage, the prepared model is applied to create the expectation.

Supervised Learning

Regulated learning gets a named informational index and further isolate into arrangement and relapse types. Each preparation test accompanies a discrete (arrangement) or persistent (relapse) esteem called a name or ground truth. The objective of directed learning is to pick up the mapping from the info include space to the mark or choice space. Grouping calculations appoint a straight out mark to every approaching example. Calculations right now Bayesian classifiers, knearestneighbors, choice trees, bolster vector machines, and neural systems [5]. Exemplary calculations incorporate calculated relapse, bolster vector relapse, and the Gaussian procedure for relapse [3].

Unsupervised Learning

For directed learning, with enough data, the screw up rate can be diminished close to the base error rate bound. Regardless, a gigantic proportion of named data is normally hard to obtain essentially.
Right now, with unlabeled data, known as solo learning, has pulled in more thought. This system for learning hopes to find gainful depiction of the data tests, which might be explained by disguised structures or covered components, which can be addressed and learned by Bayesian learning strategies. Gathering is an operator issue of independent getting the hang of, assortment tests into different gatherings dependent upon their similarities. Data features could be either the incomparable portrayal of every model or the relative comparable qualities between tests. Incredible gathering estimations consolidate k infers, different leveled packing, extend gathering, in addition, the Dirichlet methodology. Another huge class of independent learning is estimation decline, which adventures tests from a high-dimensional space onto a lower one without losing a great deal of information. In various circumstances, the unrefined data go with high estimation, andmight need to diminish the input estimation for various reasons. In progress, gathering, likewise, request, the model flightiness and the amount of required getting ready tests radically create with the component estimation. Another clarification is that the commitments of every estimation are regularly related, and a couple of estimations may be degraded with disturbance and impediment, which will corrupt the learning execution basically if not dealt with fittingly[5]. Some great measurement decrease calculations incorporate direct projection techniques, for example, head part investigation, and nonlinear projection techniques, for example, complex learning, neighborhood direct installing, and isometric mapping [5].

Reinforcement Learning

Support learning interprets how to outline to activities, through collaborating with the earth in a trialand- blunder search to expand a prize, and it comes without express supervision. A Markov choice procedure (MDP) is for the most part expected in fortification realizing, which presents activities and (postponed) prizes to the Markov process. The learning Q work is an exemplary sans model learning way to deal with tackle the MDP issue, without the requirement for any data about the earth. This Q work appraises the desire for whole prize when making a move in a given state, and the ideal Q work is the most extreme expected whole prize reachable by picking activities. Fortification learning can be applied in vehicular systems to deal with the transient variety of remote conditions [5].

4. Deep Learning

Profound Learning is a sub zone of AI look into. It is an assortment of calculations in AI, used to model elevated level deliberations in information. It Uses model models made out of various nonlinear changes. As of late, it has made huge advances on different AI errands. Profound learning means to comprehend the information portrayals, which can be implicit administered, unaided, and support learning. The input layer is at the furthest left, where every hub in the figure represents an element of info information. The yield layer is at the furthest right, comparing to the ideal yields, while the layers in the center are called concealed layers. Commonly, the number of concealed layers and the quantity of hubs in each layer are. A profound engineering implies it has various shrouded layers in the system as appeared in figure 3. Be that as it may, further systems bring new difficulties, for example, requiring significantly more preparing information what's more, angles of systems effectively detonating or evaporating. With the assistance of quicker calculation assets, new preparing techniques (new initiation capacities, pre-training), and new structures (bunch standard, leftover systems), preparing such profound design gets conceivable. Profound learning has been broadly utilized in such regions as PC vision, discourse acknowledgment, and common language handling and enormously improved best in class execution in these regions. Contingent upon applications, various structures can be added to the profound systems, for example convolutional systems share loads among spatial measurements, while intermittent neural systems (RNNs) and long momentary memory (LSTM) share loads among the worldly measurements [5].

Profound learning plans to take in a chain of command of highlights from input information. It can naturally learn highlights at numerous levels, which causes the framework to have the option to learn complex mapping work straightforwardly from information. The most describing highlight of

profound learning is that models have profound structures. Profound engineering has different shrouded layers in the system. In differentiate a shallow engineering has just a couple of concealed layers (1 to 2 layers). Profound learning calculations have been widely examined as of late. Calculations are gathered into two c ategories dependent on their models:

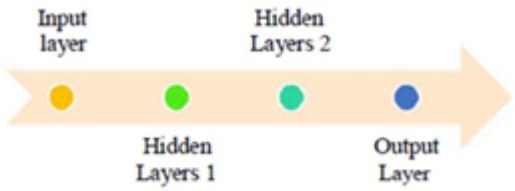

Figure 3: Deep Learning

Convolutional neural networks(CNN)

Convolutional neural systems (CNNs) has increase astounding acknowledgment in the field of PC vision. It has been persistently propelling the picture grouping precision. Likewise assumes a significant job for nonexclusive element extraction for example, scene characterization, object recognition, semantic division, picture recovery, and picture inscription. Convolutional neural system (CNNs) is generally significant part of profound neural systems in picture handling. It is profoundly powerful and regularly utilized in PC vision applications. The convolution neural system made out of three sorts of layers: convolution layers, subsampling layers, and full association layers.

Restricted Boltzmann Machines (RBMs)

RBM is a vitality based probabilistic generative model. It is made out of one layer of noticeable units and one layer of covered up units. The noticeable units speak to the info vector of an information test and the shrouded units speak to highlights that are preoccupied from the unmistakable units. Each noticeable unit is associated to concealed unit, though no association exists inside the unmistakable layer or shrouded layer. During past years, the nature of picture grouping and item discovery has been significantly improved because of the profound learning technique.

Repetitive neural System

RNNs are utilized to utilize consecutive data. In a conventional neural system all information sources (and yields) are autonomous of one another. To foresee the following word in a sentence, need to realize which words preceded it. RNNs are called intermittent as they play out a similar assignment for each component of a succession, with the yield being relied upon the past calculations. RNNs can utilize data in subjectively long groupings, yet by and by they are constrained to just a couple of steps. An online unaided profound learning framework is utilized to channel framework log information for examiner. In which variations of Profound Neural Systems (DNNs) what's more, Repetitive Neural Systems (RNNs) are prepared to perceive movement of every client on a system and simultaneously evaluate whether client conduct is typical or strange, all continuously [10]. Created model confronted a few key troubles in applying AI to the digital security area. Model was prepared constantly in an online design, yet location of vindictive occasions was testing task. Similar investigation was displayed by Gavai et al. (2015) of a regulated methodology and a solo methodology utilizing the segregation woods strategy for recognizing insider risk from arrange logs. Ryan et al. (1998) applied neural networkbasedways to deal with train coordinate with one shrouded layer to anticipate the probabilities-based system interruption [10]. A organize interruption was recognized for the likelihood not exactly 0.5. However, input highlights were not organized and didn't prepare the system in an online manner.

Displaying ordinary client action on a system utilizing RNNs was performed by Suspend et al. (1992). The RNN was prepared on a delegate succession of Unix order line contentions (from login to logout). System interruption recognized when the prepared system inadequately predicts the login to logout arrangement. While this work mostly addresses internet preparing, it doesn't persistently prepare the system to consider changing client propensities after some time. Intermittent neural systems have been effectively applied to oddity location in different elective areas, for example, signals from mechanical sensors for apparatus, for example, motors, and vehicles [10].

A comprehensive examination of content Captchas, to assess security, a basic, successful and quick assault on content Captchas proposed by Tang et al. Utilizing profound learning strategies, which

effectively can assault all Roman character-based content Captchas conveyed by the best 50 most well known sites in the world and accomplished best in class results. Achievement rates go from 10.1% to 90.0% [9]. A tale picture based Captcha named SACaptcha utilizing neural style move systems likewise exhibited. This is a positive endeavorto improve the security of Captchas by using profound learning systems. Right now, learning systems play two jobs: as a character acknowledgment motor to perceive singular characters and as an incredible way to upgrade the security of the picture based Captcha This demonstrated profound learning is a twofold edged sword. It very well may be either utilized to assault Captchas or improve the security of Captchas [9]. In future, they anticipated existing content Captchas are never again secure. Other Captcha options are powerful, and the structures of new Captchas can be all the while secure and usable are as

May-June 2020
ISSN: 0193-4120 Page No. 3866-3872

yet provoking troubles to be chip away at [9]. Another methodology for discovery of system interruption utilizing solo profound learning with iterative K-implies bunching proposed by Alom and Taha. Furthermore, solo ELM, what's more, just K-implies bunching approaches were tried. From exact assessment on KDD-Cup 99 benchmark, it is watched that the profound learning approach of RBM and AE with k-implies grouping appear around 92.12% and 91.86% precision for arrange interruption location individually. RBM with K-implies bunching gives around 4.4% and 2.95% better identification exactness contrast with K-means and USELM methods separately [11].

Nichols and Robinson present an online unaided profound learning way to deal with distinguish atypical system action from framework signs progressively. Models decay irregularity scores into the commitments of individual client conduct highlights for expanded interpretability to help investigators investigating potential instances of insider danger. Utilizing the CERT Insider Danger Dataset v6.2 and risk location review, their novel profound and repetitive neural system models outflank Head Part Examination, Bolster Vector Machine and Seclusion [10].

5. Similarities and Differences Between machine Learning & Deep Learning

There are numerous riddles about the relationship among ML, DL, and computerized reasoning (artificial intelligence). AI is a part of man-made intelligence and is firmly identified with computational insights, which additionally centres around expectation making utilizing PCs [1]. though DL is a sub-field in machine learning explore. Its inspiration lies in the foundation of a neural system that mimics the human cerebrum for investigative learning. It impersonates the human cerebrum component to decipher information, for example, pictures, sounds and messages [14].

A. Likenesses

• Steps engaged with ML and DL ML and DL strategy fundamentally utilizes comparable four stages in but include extraction in DL is computerized instead of manual [12].

• Techniques utilized in ML and DL ML/DL are comparative in these three methodologies: regulated, solo and semi-directed. In administered learning, each occurrence comprises of an info test and a name. The managed learning calculation examines the preparation information and utilizes the aftereffects of the investigation to outline examples. Unaided discovering that finds the portrayal of concealed structures from unlabelled information. Since the example isunlabelled, the exactness of the calculation's yield can't be assessed, and just the key highlights of the information can be abridged and clarified. Semi-directed learning is a method for joining directed learning with solo learning. Semi-regulated learning utilizes a lot of unlabeled information when utilizing marked information for design acknowledgment. Utilizing semi-directed learning can diminish mark endeavors while accomplishing high exactness [1]. Highlight Building Picking fitting calculation Prepare and assess model execution Utilize the prepared model to order or on the other hand foresee the obscure information.

Figure 4: Steps engaged with ML and DL

Contrasts ML and DL strategies diverse in following manners:

Information conditions

The primary contrast between profound learning and machine learning is its presentation as the measure of information increments. Profound learning calculations don't perform well when the information volumes are little, since profound learning calculations require a lot of information to comprehend the information flawlessly. Then again, AI calculation utilizes the built-up rules, in this way execution is better.

Equipment conditions

The DL calculation requires numerous lattice tasks. The GPU is generally used to enhance lattice activities effectively. Subsequently, the GPU is the equipment vital for the DL to work appropriately. DL depends more on superior machines with GPUs than AI calculations.

Highlight handling

The way toward placing area information into a component extractor to decrease the unpredictability of the information and create designs that make learning calculations work better is known as highlight handling. In ML, the greater part of the qualities of an application must be dictated by a specialist and afterward encoded as an information type. The presentation of most ML calculations relies on the precision of the highlights removed. Attempting to get elevated level highlights straightforwardly from information is a significant contrast among DL and customary

May-June 2020
ISSN: 0193-4120 Page No. 3866-3872

AI calculations. Consequently, DL lessens the exertion of planning a component extractor for every issue.

Critical thinking technique

In Critical thinking strategy on applying conventional machine learning calculations to take care of issues, conventional machine adapting for the most part separates the issue into various sub-problems what's more, takes care of the sub-issues, at last getting the outcome. Dissimilar to profound realizing which unravels start to finish issue.

Execution time

DL calculation sets aside long effort to prepare because there are numerous parameters in the DL calculation. Though ML preparing takes generally less time, just seconds to hours. The test time is inverse for ML and DL. Profound learning calculations require next to no opportunity to run during testing stage contrasted with ML calculations. This isn't material to
all ML calculations, some necessary short test times [1]

6. Conclusion

This paper gives experts a strong foundation for choosing less difficult and better instructed choices about machine learning and significant learning for advanced security. It was kept an eye on that AI has a couple of troubles in managing Big Data while significant learning execution is better in setting of tremendous data. To improve the security, an inventive picture based captcha named SACaptcha using significant learning strategies can be used. Solo significant learning of RBM and AE with iterative k-infers gathering show up around 92.12% and 91.86% precision for sort out interference distinguishing proof. In future, plan of framework interference distinguishing proof for computerized security with online learning approach can be sent. Computer based intelligence is used to develop a model which perceive and include advanced malware, by disturbing SMEs, advised inspectors or conveying reports dependent upon the reality of the security event. The model plays out these limits with astoundingly high exactness (90%). To recognize odd framework activity from structure signs consistently, an online independent significant learning approach can be used that produces interpretable examinations of insider chance in spilling structure customer logs. This work has along these lines accomplished its objective by giving potential headings for future work and will in a perfect world fill in as groundwork for phenomenal upgrades of Computer based intelligence and significant learning procedures for computerized security assignments.

References

[1] Yang Xin Et Al., “Machine Learning And Deep Learning Methods For Cybersecurity” In IEEE Journals & Magazine, May 2018.

[2] Qiang Liu Et Al., “A Survey On Security Threats And Defensive Techniques Of Machine Learning: A Data Driven View”,In IEEE Journals & Magazine, Vol 6, February 2018.

[3] James B. Fraley And Dr. James Cannady, “The Promise Of Machine Learning In Cybersecurity”, In Southeast conference, May 2017.

[4] SoorenaMerat, P.Eng, Dr.WahabAlmuhtadi, P.Eng., “Artificial Intelligence Application For Improving Cyber-Security Acquirement” In 28th IEEE Canadian Conference On Electrical And Computer Engineering, Halifax, Canada, May 2015.

[5] Hao Ye, Le Liang et al., “Machine Learning for Vehicular Networks” In IEEE Vehicular Technology Magazine, April 2018.

[6] Ge Wang, Jong Chu Ye et al., “Image Reconstruction Is A New Frontier Of Machine Learning”, In IEEE Transactions On Medical Imaging, Vol. 37, pp 1289 – 1296, June 2018.

[7] Alexandra L’heureux et al., “Machine Learning With Big Data: Challenges And Approaches”, In IEEE Journal &Magazine ,Vol 5, pp 7776 – 7797, April 2017.

[8] Mirza Golam Kibria Et Al., “Big Data Analytics, Machine Learning And Artificial Intelligence In Next-Generation Wireless Networks”, In IEEE Journal & Magazine, May 2018, pp 2169-3536.

[9] Mengyun Tang Et Al., “Research On Deep Learning Techniques In Breaking Text-Based Captchas And Designing Image-Based Captcha”, In IEEE Transactions On Information Forensics And Security,Vol13, Issue: 10,pp 2522 – 2537,Oct. 2018.

[10] Aaron Tuor ,Samuel Kaplan And Brian Hutchinson, “Deep Learning For Unsupervised Insider Threat Detection In Structured Cybersecurity Data Streams”, In Proceedings Of Ai For Cyber Security Workshop At AAAI ,Dec 2017.

[11] MdZahangirAlom And Tarek M. Taha, “Network Intrusion Detection For Cyber Security Using Unsupervised Deep Learning Approaches”, In IEEE National Aerospace And Electronics Conference (NAECON), Dayton, Oh, USA, June 2017.