IJERMT
International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
Volume 11, Issue-1 January-February- 2024
Email: editor@ijermt.org
www.ijermt.org

# AN ANALYTICAL STUDY ON RECENT ADVANCES IN ARTIFICIAL INTELLIGENCE TO STRENGTHEN CYBER SECURITY

**Bhavika Chechani,**

Research Scholar,

University of Technology, Jaipur

***Abstract***

*In the computerized age, cyber security has become a major concern. Information breaks, fraud, manual human test cracking, and other comparative issues every now and again hurt large number of individuals as well as enterprises. Imagining the legitimate standards and cycles and trying them with demanding flawlessness to battle cyber attacks and wrongdoings has forever been a battle. Ongoing advances in artificial intelligence have fundamentally expanded the risk of cyber attacks and different wrongdoings. It has been utilized in essentially all parts of designing and exploration. AI in Cyber security Market allows organizations to screen, recognize, report, and battle cyber dangers to maintain data privacy. The utilization of reliable and improved cyber security arrangements has become vital across all organizations because of rising public mindfulness, advancements in data innovation, moves up to intelligence and policing, and an expansion in the volume of information accumulated from different sources. We require state of the art apparatuses and advancements to distinguish, examine, and take brief activity on new attacks and dangers as the cyber danger situation deteriorates. Artificial intelligence (AI) applications have the ability to dissect and consequently order huge volumes of Web traffic. AI-based arrangements that computerize attack recognition and address testing cyber security issues are drawing in increasingly more consideration.*

***Keywords:*** *Cyber Security, Artificial Intelligence (Ai), Cognitive Security, K Mean and Svm*

## 1. INTRODUCTION

Cyber security is characterized collectively of techniques that aid in safeguarding electronic data, human way of behaving, and frameworks. Like the Moore's Regulation, which expresses that coordinated circuit parts will twofold in size at regular intervals and that chip advancement will bring about falling chip costs; cybercriminals are definitely expanding the viability of their designated attacks while reducing the expense at regular intervals.

Somewhere in the range of 2016 and 2021, it is anticipated that speculation on cyber security would reach $1 trillion around the world. From 2013 to 2016, spending on cyber security has previously expanded by over 40%. Artificial intelligence, in some cases known as AI, is the making of refined PC frameworks that can carry on like customary people and utilize human mental cycles to fabricate discourse acknowledgment and language handling abilities, for example. The objective of AI is to make another clever framework that exhibits intelligence traits. AI is a complete logical framework containing different branches in way of thinking, software engineering, and math. The expression "artificial intelligence" is commonly used to allude to gadgets that recreate "discernment" works those people partner with their brains, for example, critical thinking and swotting

To safeguard PC networks, end frameworks, projects, and information against attacks, unapproved access, changes, and mischief, various advances and strategies have been created under the umbrella of cyber security. At the host, network, application, and information levels, there are cyber-guard measures. To forestall attacks and find security breaks, various instruments like firewalls, antivirus programming, interruption location frameworks (IDS), and interruption insurance frameworks (IPS), work secretively. Nonetheless, foes keep on having the high ground since they just have to find one weakness on the frameworks that are being safeguarded. Cyber attacks are filling in scale, refinement, and cost as additional gadgets are being associated with the Web. Because of the quicker digitization and developing dependence on the computerized foundation throughout the long term 2019 and 2020, the attack surface expanded (e.g., cloud-based administrations, remote work). In the second quarter of 2020, north of 60 million destructive endeavors were halted, a 74.6% increment over the earlier months, as per a Symantec report. One of the most impossible to miss and horrendous cyber attacks happened toward the beginning of 2021. To make the water ill suited for utilization, a cybercriminal endeavored to change explicit substance levels in the water treatment arrangement of the City of Oldsmar in Florida. Following this example, it is anticipated that a solid and dependable cyberspace will turn out to be considerably more essential in the new friendly and financial standard laid out after the Coronavirus pandemic and the resulting change of the computerized climate in the latest report of danger landscape gathered by the European Association Organization for Network and Data Security (ENISA).

### 1.1 Applications of AI in Cyber security

The fields of artificial intelligence and cyber security every now and again cross. Cyber wrongdoing identification and avoidance have seen an expansion in the utilization of AI devices, including master frameworks, computational intelligence, brain networks, keen specialists, artificial resistant frameworks, AI, information mining, design acknowledgment, fluffy rationale, heuristics, and so on. They can be utilized to find how to make it feasible for security experts to appreciate the computerized climate to detect abnormalities.

Artificial intelligence usage can possibly expand the capacities of current cyber security arrangements. Organizations can involve AI in the four areas of computerized guard, cognitive security, ill-disposed training, equal handling, and dynamic observing to further develop current cyber security frameworks.

Mechanization of Guard Cyber security arrangements come in two flavors: programmed and master (expert driven) (machine driven). While mechanized frameworks make utilization of AI-upgraded devices, master frameworks are made and run by people. AI-based frameworks capability as free, self-further developing specialists. The Manual human test (Totally Computerized Public Turing Test to Distinguish PCs and People) framework is a pleasant outline of a robotized framework. Without robotization, individuals can't handle the speed and volume of information expected to safeguard the cyber domain. Artificial intelligence can be a huge assistance to an association's cyber safeguards as networks become greater and more confounded. A definitive objective of cyber protection is to shield clients while maintaining all usefulness totally. Computerized AI frameworks can be integrated into cyber security tasks currently set up. Coming up next are a couple of this task:

- Growing more exact biometric login strategies
- Utilizing prescient examination to track down risks and noxious action
- Regular language handling can further develop learning and investigation. It can likewise get contingent verification and access.
- Involving in the computerization of humble security exercises Working on human examination - from malevolent attack discovery to endpoint assurance Having no zero-day weaknesses
- Integrating artificial intelligence into cyber security has various benefits. AI-based cyber security solutions are made to operate continuously to keep you safe.

**Cognitive Security**: The upsides of both human and artificial intelligence are joined in cognitive security. A high level kind of artificial intelligence called cognitive registering (CC) makes utilization of various sorts of AI. It alludes to gadgets that utilization programming or equipment to recreate how the human brain capabilities. As far as aim, AI and CC are still practically the same, yet they vary from each other as far as how they naturally collaborate with individuals. Artificial intelligence (AI) is a term used to depict frameworks that can do tasks that would commonly require human intelligence. Bypassing the constraints of customary programmable (von Neumann) PCs is the objective of cognitive processing. In a mock Risk game, IBM's most memorable cognitive framework, Watson for cyber security, demonstrated that it could respond to testing questions similarly as well as the best human players. With each discussion, Watson picks up new data that assists him with recognizing dangers and deal commonsense guidance. Subsequently, an examiner can respond to dangers all the more quickly and with certainty.

**Adversarial training:** is a term that is habitually used to portray the creation and utilization of AI for evil. To test for AI weaknesses, cyber security engineers are creating proactive antagonistic attack models. An ill-disposed learning attack can make the calculations act inappropriately or reveal details of how they capability. AI frameworks can turn out to be more vigorous through ill-disposed training, which additionally makes it simpler to recognize the framework's weaknesses. The more secure AI applications become as we push toward a "ill-disposed" and "consistently on" technique.

**Parallel and dynamic**: observing is essential during arrangement because of the designated frameworks' inclination for learning. Checking is expected to make sure that inconsistencies between a framework's normal way of behaving and real way of behaving are recognized and successfully tended to. To do this, engineers of AI frameworks ought to keep a control framework that goes about as a standard against which the exhibition of the first framework is assessed.

## 2. REVIEW OF LITREATURE

**Li. ct al. (2016)** arranged an insufficient cryptography gadget for SCADA frameworks' to ensure quick emergency response and inadequacy recovery under extraordinary circumstances. They got a handle on a philosophy of security approval part for achieve a two-way affirmation and surefire the strong correspondence between the master and the slave stations. This method used a vicariate symmetric polynomial to achieve the gathering key by permitting the master and the slave stations to character values considering the polynomial calculation. The dispensing key has widened and the information transmission close by encryption in SCADA frameworks has done by the usage of expanded allotting key. The normal check for master and slave stations was given by the lightweight security part. Unprecedented requirements old SCADA frameworks gave the quick response encountering exactly the same thing and consistent information correspondence.

**Quciroz Carlos. Abdun Mahmood. and Zahir 'T'ari (2011)** in their paper named "Twistedness A Framework for Building SCADA Recreations" have depicted about attacks on SCADA frameworks, highlighted the need to break down the security risks and made fitting securily deals with defend the frameworks. The makers have investigated in pain point where there is nonappearance of authentic showing gadgets to evaluate the security of SCADA frameworks. As for the most part acknowledged in researcher and current networks, it is nonsensical to lead security examines live frameworks. The makers in their paper have shut a construction which was a unique solution for make pragmatic entertainments of SCADA frameworks considering a blend of association establishment and veritable devices network. It abandons different reliable and execution issues in the propagation environment to allow certified devices (like splendid meters, RTUs, and so forward) to be added to the test framework. The entertainment structure, SCADA

**Amin Saurabh, Xavicr ILitrico. (2013)** in their paper named "Cyber security of water SCATDA frameworks part I: examination and preliminary and cruor of clandestine trickery attacks". Have planned to perform security risk appraisal old networked control frameworks with regulatory and authoritative control layers. They have broke down the introduction of a relating vital controller (managerial layer) and a model based expressive arrangement (regulatory layer) under a class of trickery attacks. They embraced a moderate system by tolerating that the assailant knows around: 1) 'The framework merciful: 2) The limits of the logical arrangement; and 3) The sensor-control Signs.

**James and Prabhakaran (2015)** arranged one more multiplication environment to perceive the attacks in a SCADA dissemination framework. The guideline reasoning of this environment was to permit the certifications of cyber weaknesses and mishandlings of coordinating ways. Then, il was significantly important for the cyber-security mitigations, since it researched the approach to acting of the framework during the location of anticipated attacks. Nevertheless. it needs. With the presentation of the framework execution, with no damage to an electrical stock. The expectation technique offered a high unflinching quality and genuineness during attack location in SCADA associations

**Mcquillan and L.loyd (2016)** proposed an association interface which was salcly organized close by the SCADA framework to speak with the collection of present day control contraptions by Modern Control Framework (ICS) network arrangement. The device information of current control contraption had memory and association interweave. The SCADA framework contained the interference identification part pardoned by one processor and facilitated with the arrangement information. Iu was used to create the SCADA game plan information. Supported correspondence information illustrative of something like one specific correspondence for ICS network transmission.

**Shamcli Sendi et al. (2012)** arranged one more plan for expecting a multi-step attack, in which the associations among aggressors and associations were liken out by using Stowed away Markov Model (1IMM). Cautions relationship expected a huge part in the conjecture and a reasonable reality through association thought by the solitary alerts and Earnestness'. Controlled reality crated the assumption alert strides of multi-step attacks for working on the precision. A unique prepared association was used to cut the false negatives in gauge. to research the interferences and to order off incredible response vital. Here, the discovery part was used to forks the spread repudiation of organization attacks and to recognize the multi-step attack.

## 3. METHODS

### *3.1 Experimental Setup*

The different apparatuses and programming dialects utilized while completing the investigation is as per the following:

- Splunk Enterprise version
- Jupyter Editor
- Splunk Programming Language
- Python

### *3.2 Design Modules*

The modules that make up the whole framework are portrayed in Figure 1.

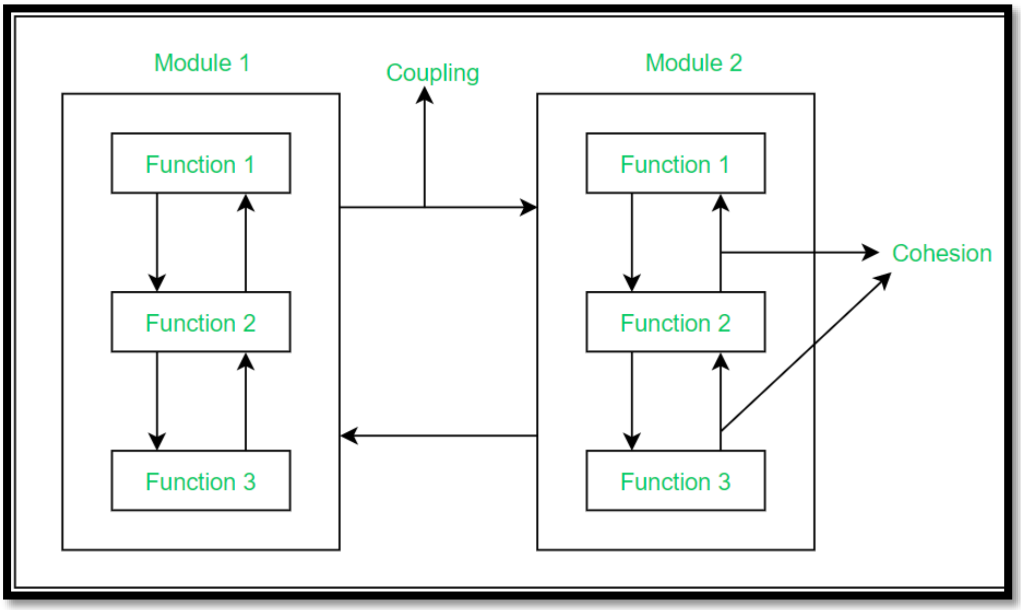

**Figure: 1** design modules

Splunk is a piece of programming that gathers continuous information, lists, connects, and presents it such that makes it simple to look for, envision, and use for cyber security.

K-means is a calculation that utilizes an unaided learning method to recognize examples and bunches in information. Information focuses are grouped by how comparative they are. The foreordained number of groups is K, and it is.

Factual models called artificial brain networks endeavor to mimic the workings of the human brain. There are hubs in the ANN that give the contribution to the accompanying neuron and so forward until the result hubs get it. Marks can then be applied to the result after this.

The SVM calculation is a directed sort of calculation that is basically utilized for characterization. The marked information focuses are separated into different classes by a hyper plane, which is a line.

### *3.3 Implementation*

The NSL-KDD dataset is utilized as the wellspring of the information, which is then taken care of into the Splunk Indexer for parsing and ordering. The created information is then taken care of into the Splunk Forwarder for information sending. Splunk was utilized over PCA for the essential highlights in light of the fact that such hurtful movement are fixed, meaning that the elements will remain something very similar and the proficiency would be higher.

The information is separated into training and testing parts in a proportion of 7:3 relying upon the qualities utilized. Information groups are made by the K-Means calculation utilizing the training information. The individual ANNs are taken care of these information bunches, and different results are created. The SVM gets the accumulated discoveries and decides if the attack was malevolent, not noxious, or harmless.

## 4. ANALYSIS

The information that these procedures are applied on. The calculations were all tried utilizing a test informational index of 50 examples and a training set of 100 examples, including 50 training tests. The precision results from every one of the four distinct kinds of calculations were looked at..

| Method | Accuracy | Precision | Recall | F1 score |
|---|---|---|---|---|
| K Means and SVM | 1.236 | 1.36 | 1.63 | 1.93 |
| PCA K Mean and SVM | 1.693 | 2.36 | 2.66 | 2.63 |
| Splunk k- Means and SVM | 2.153 | 4.42 | 3.82 | 3.89 |
| Splunk k- mean ANN and SVM | 2.963 | 4.69 | 4.36 | 4.22 |

**Table: 1** Comparison of different models

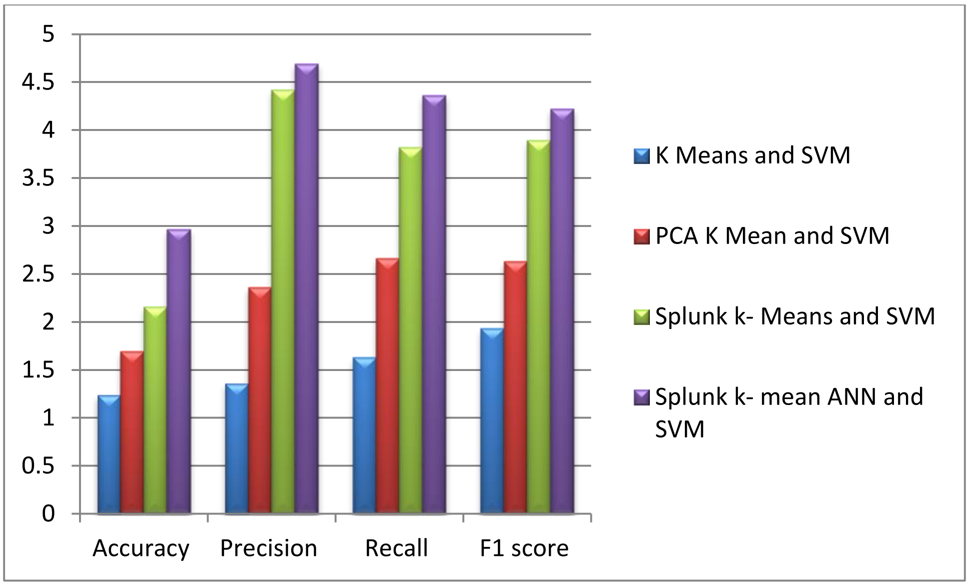

**Figure: 2** Comparison of different models

Subsequently, we can see that utilizing a mix of calculations at first could be tedious, yet as training goes on, this is obviously the best way.

## 5. RESULT

7 models are inspected utilizing the KDD'99 informational index. These incorporate KNN, SGD, CNN, Choice Tree, LSTM, MLP, and GRU. The ordinary progression of information and the attack identification rate are found in three unique parts. Precision starts things out, trailed by responsiveness and FPR. All of the dataset's 41 elements is utilized in this part of the review. The models are more compelling and effective when the precision and awareness are higher and the FPR is lower. Except for CNN, SGD, and to some degree GRU, every one of the models in this occurrence have precision paces of over 90%, awareness paces of over 85%, and FPRs of under 10%. The models are accordingly very great at distinguishing attacks and the ordinary progression of information. In the initial step, the typical precision and responsiveness results of AI models utilizing 41 highlights are more than 90%, which is an excellent outcome. Moreover, the typical FPR result is practically under 10%, which makes AI models successful.

At the point when the trained ML models are thought about in contrast to the new dataset NSL-KDD, they keep on creating great outcomes (almost 85%) with a FPR under 15%. Thus, AI models perform really in the abnormality identification process.

| Class Name | Average Accuracy % | Average Sensitivity% | Average FPR% |
|---|---|---|---|
| AI Model using 41 Features of KDD'99 | 52.3 | 93.6 | 11.23 |
| AI Model using 41 Features of NSL-KDD | 61.3 | 99.2 | 15.36 |

**Table: 2.** Comparison among the Steps of Efficiency Test

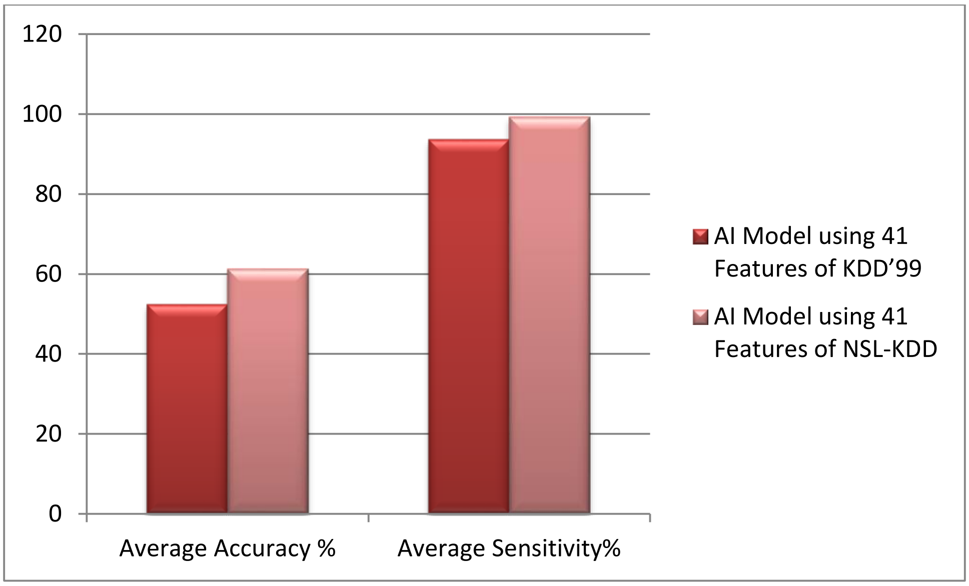

**Figure: 3** Comparison among the Steps of Efficiency Test

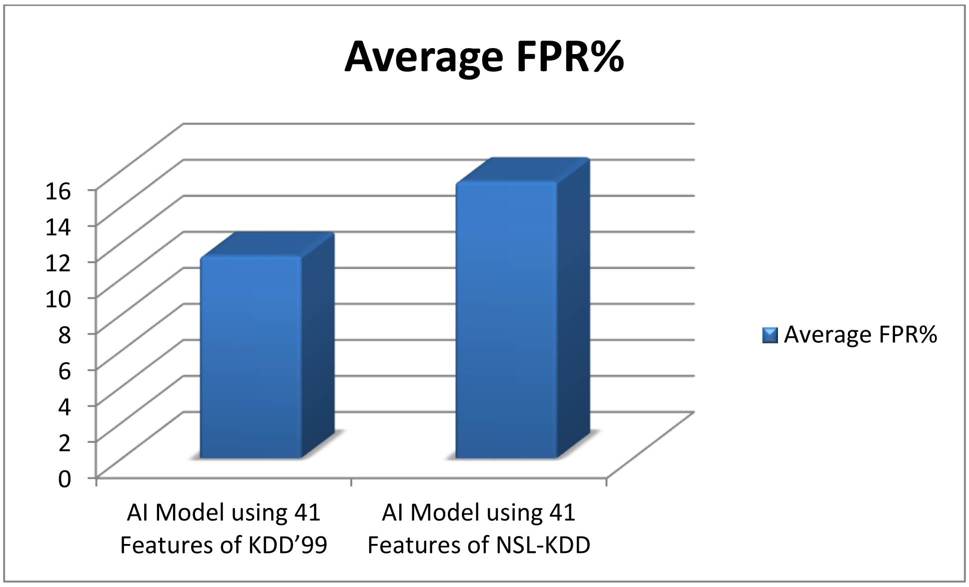

**Figure: 4** Comparison among the Steps of Efficiency Test

## 6. ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

### 6.1 Artificial Intelligence

A strategy for instructing a PC, a robot that is constrained by a PC, or a piece of programming to think basically, similar as a wise individual may, is called artificial intelligence. To make keen programming and frameworks, one must initially lead research on how the human brain capabilities, as well as how people learn, make choices, and team up while endeavoring to tackle an issue.

The capacity to learn and apply knowledge to take care of issues is the way the vast majority portray intelligence. Numerous human tasks will before long be supplanted by shrewd machines soon. Artificial intelligence is the review and improvement of insightful machines and programming that can think, learn, accumulate knowledge, convey, use, and sense objects. The word was first begat by John McCarthy in 1956 to portray a part of software engineering that was worried about training machines to act like individuals. View of reason and conduct are made conceivable by an understanding of registering. Artificial intelligence varies from brain research in that calculation is given more weight, and from software engineering in that discernment, thinking, and activity are given more weight. It builds the machine's utility and intelligence.

### 6.2 The development of AI in cyber security

AI and Artificial Intelligence (AI) are being associated more profoundly than any other time in recent memory across organizations and applications as enrolling power, data gathering, and limits get to the next level. This colossal informational collection is a valuable wellspring of data for AI, which can figure out and assess everything obtained to track down surprising examples and fragile traits. This suggests that new drives and weaknesses in cyber security can be promptly found and explored to assist with halting extra attacks. It could decrease a portion of the strain on "accomplices" in human security. They are cautioned when a work is required, however they likewise have the decision to give their opportunity to additional creative and useful pursuits. A gainful relationship is taking into account the top security expert in your association. The artificial intelligence (AI) will be similarly pretty much as wise as your star worker on the off chance that your AI and artificial intelligence calculations are arranged utilizing this star delegate.

At this moment, in the event that you burn through the energy to foster your AI and artificial intelligence programs with your main ten workers, the outcome will be an answer that is similarly essentially as splendid as your main ten people set up. AI likewise doesn't take get-away days.

### 6.3 What uses does artificial intelligence have in terms of online safety?

Artificial intelligence (AI) is now being utilized or is effectively being concentrated on in a portion of the accompanying areas of cyber security arrangements, for example, Gmail, which uses AI to distinguish and block unwanted spam and false emails.

Whether or not an email message is spam or not, each time a client clicks on it, they aid in training Gmail's artificial intelligence to distinguish spam from now on. Worldwide, Gmail is utilized by a great many individuals. This improvement has made it feasible for artificial intelligence to now perceive even the subtlest spam emails that endeavor to imitate "ordinary" emails.

• **Fraud detection:** To recognize fake exchanges, MasterCard has presented Choice Intelligence, an artificial intelligence-based extortion location framework that utilizes calculations in light of expected client ways of behaving. The framework inspects the client's normal buying designs, the merchant, the exchange's area, and a lot more perplexing calculations to decide if a buy is uncommon.

• **Botnet Identification:** Especially troublesome regions, intermediary server timing examination and example acknowledgment are every now and again utilized in botnet discovery. A botnet attack frequently includes countless "clients" playing out similar questions on a site since botnets are regularly overseen by an expert content of directions. This could incorporate animal power secret word attacks utilizing botnets, network weakness look, and different breaks. The very confounded capability that artificial intelligence plays in botnet recognizable proof is hard to summarize in a couple of passages.

These are only a couple of instances of how artificial intelligence is utilized in cyber security. Various exploration articles that present persuading information right now exhibit the worth of artificial intelligence in the field of cyber security.

Most examinations show that endeavours to recognize cyber attacks are effective somewhere in the range of 85 and 99 percent of the time. An organization called Dark Follow that creates artificial intelligence declares to have a triumph record of close to 100% and as of now has thousands of clients around the world.

### 6.4. Network attack detection using AI

Early location of network cyber attacks is conceivable with the utilization of AI models. Three classifiers for network attack discovery have been proposed utilizing choice trees, support vector machines, and a mix of the two. Many models have been made for something similar since there are recommendations. Due to the huge datasets delivered by networking observing devices, AI models can be consistently trained in both the attributes and marks of hurtful network movement.

### 6.5 AI's Contributions to Cyber security

Exploring artificial intelligence's benefits with regards to cyber security uncovers that organizations that carry out it benefit incredibly. Two out of each and every three organizations saw an improvement in return for capital invested on cyber security frameworks, which makes this self-evident.

For example, Siemens AG, an innovator in overall charge, computerization, and digitalization, utilized Amazon Web Administrations (AWS) to make a stage for Siemens Cyber Safeguard Centre is AI-based, quick, independent, and extremely flexible (CDC). The AI being used could predict 60,000 potential attacks each unit of time. This limit might be overseen by a staff of less than 12 individuals without adversely affecting framework execution on the grounds that to the AI that was conveyed. Associations can study and reapply verifiable peril examples to recognize new dangers thanks to AI in cyber security. While finding events, exploring them, and eliminating risks, this saves time and exertion. Around 64% of directors claimed that AI had diminished the cost of recognizing and answering breaks. Quick activity is fundamental for forestalling cyber attacks. For organizations, the typical expense decrease is around 12%. AI offers potential open doors for cyber security in light of the fact that the climate is quickly changing from recognizable proof, manual reaction, and moderation to robotized relief. AI is equipped for recognizing intricate and innovative enhancements to battle extensibility.

### 6.6 AI and Cyber Security Issues

i. Online risks: Hackers currently have far and away an excessive amount of admittance to your own data. They can basically track your whereabouts and hack your own data in the event that security steps are not taken.

ii. Artificial intelligence is viewed as a danger since certain investigations propose that a sizeable part of the workforce will be supplanted by AI programming and machines.

iii. Job misfortune The last worry about AI is that machines will start to rule over people. Various books and movies have recently tended to this point. To keep this from occurring, move should be made.

iv. Cost-adequacy: Not every person can utilize AI administrations since they can be unreasonably costly.

v. Since not every person is anxious to work with and find out about state of the art innovation, AI isn't generally perceived. Worldwide Diary of PC

## 7. CONCLUSION

By using the current security advances, cybercrimes can't be completely forestalled. A successful system for deciding whether an attack is malevolent, non-malignant, or harmless is proposed in this review. Utilizing Splunk to remove the key highlights, then, at that point, taking care of the information to K Means to get a group of subsets. Subsequent to gaining the bunches, training will be regulated to each artificial brain network freely, and the joined outcomes will then be taken care of into the SVM, which will arrange the attacks as pernicious, harmless, or non-noxious. The two arising advancements of AI and cyber security have been converged in this review. Attackers generally decide to trap the guard prior to making contact. In this way, the best strategy for pulling off a shock is to utilize current innovation. Subsequently, it is projected that this cyber security procedure would be very powerful.

## REFERENCES

1. *Abraham and J. Thomas, "Distributed intrusion detection systems: a computational intelligence approach," in Applications of information systems to homeland security and defense, ed: IGI Global, 2006, pp. 107-137.*
2. *Chio and D. Freeman, Machine learning and security: Protecting systems with data and algorithms: " O'Reilly Media, Inc.", 2018.*
3. *Gerhards-padilla and F. Fkie, "Intrusion Detection in Tactical Multi-Hop Networks," 2009.*
4. *F.-h. Hsu, "IBM's deep blue chess grandmaster chips," IEEE micro, vol. 19, pp. 70-81, 1999.*
5. *A. Mohammed, "Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature," International Journal of Innovations In Engineering Research and Technology [IJIERT], vol. 7, 2020.*
6. *J. Podishetti and K. Anjaiah, "Role of Artificial Intelligence in Cyber Security," International Journal of Research in Advanced Computer Science Engineering, Volume.*
7. *K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons, 2007.*
8. *L. F. Sikos, AI in Cybersecurity vol. 151: Springer, 2018.*
9. *R. Christopher, "Port scanning techniques and the defense against them," SANS Institute, 2001.*
10. *R. Kumar, "Artificial Intelligence: A Path to Innovation," International Journal of Scientific Research in Science and Technology (IJSRST), 2017.*
11. *S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," Journal of Computational Science, vol. 25, pp. 152–160, 2018.*
12. *S. Peddabachigari, A. Abraham, C. Grosan, and J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems," Journal of network and computer applications, vol. 30, pp. 114-132, 2007.*
13. *S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance detection in high bandwidth environments," in DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 1. IEEE, 2003, pp. 130–138.*
14. *S. Staniford, J. A. Hoagland, and J. M. McAlerney, "Practical automated detection of stealthy portscans," Journal of Computer Security, vol. 10, no. 1-2, pp. 105– 136, 2002.*

***15.*** *V. Kanimozhi and T. P. Jacob, "Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," in 2019 international conference on communication and signal processing (ICCSP), 2019, pp. 0033-003*