INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 153-158

e-ISSN : 2583-1062

Impact Factor: 5.725

SHIELDING THE COMPUTING INFRASTRUCTURE WITH CYBER SECURITY EMBEDDING AUTOMATION

Julian Menezes Rathinam[1], Muhilarasi Arumugam[2], Krishna Prakash Rajakannu[3], Chandraleka Mathiyazhagan[4]

[1]Assistant Professor, Department of Computer Science and Engineering, Loyola Institute of Technology, Chennai, Tamil Nadu, India.

[2,3,4]Final Year Student, Department of Computer Science and Engineering, Loyola Institute of Technology, Chennai, Tamil Nadu, India.

ABSTRACT

The terminology which is defined as Artificial Intelligence pin points to the imitation of the intelligence of a Human Being on to a particular Machinery, which in turn are coded to contemplate as a normal individual and ditto the activities of the same persona. The afore mentioned terminology may get plastered on to any sort of a machinery that has the idiosyncrasy relevant to an Individual like that of the art of learning coupled with the solving of problems. The archetype trait of the terminology Artificial Intelligence lies in the competence of extenuating as well as undergoing rigorous game plan for accomplishing a particular objective. The terminology defined as Cyber Security relates to the technological advancement, procedures as well as the exercises and game plan blueprinted to cast a net of protection over the network of Computers, Routers, Switches, Hubs, Applications as well as the digital 0's and 1's from stealth activities, physical swap, or any sort of unwanted intrusion. The security which is associated with the Cyber Domain is also christened as Information Technology oriented Security. Security with relevance to the Defense, Governance, Finance, IT sector and last but not the least the Health Sector gather, work on the data as well as pile up remarkable digital 0's and 1's on the Metallic HDDs as well as other trivial contraptions. The yesteryears had laborers to perform any sort of a task. The invention of wheel to the present day machinery revolutionized the task put forth as a challenge to the Individuals. Stationing a guard 24/7 is quite a herculean task for safe guarding an entity from any sort of a mishap. The revolution in the Surveillance to the Monitoring Sector has brought forth the inclusion of Technology to make the safeguarding task much easier and efficient for Individuals to protect and preserve entities, which are deemed valuable. The Security systems which are based out of the entity Artificial Intelligence tend to use entities like Big Data and other competitive Computer Algorithms for the purpose of Automating the task of Managing the Security associated with an entity. Several Methodologies get utilized, but one among them termed Case Studies get employed for scrutinizing the appropriate clout of the security clubbed with Artificial Intelligence in a Cyber Environment. The denouement exposes the comparison between Systems based out of Signature and with the Systems rooted upon Artificial Intelligence. The aftermath of the comparison denotes that the latter technology possess three trivial qualities like competence, authenticity, as well as trustworthiness. The reason behind the above statement is that the systems associated with Security are sound enough to scrutinize as well as equate with voluminous digital 0s and 1s for expediting the disclosure as well as the acknowledgement to the fulminations.

Keywords: Cyber Security, Artificial Intelligence, Automation, Authentication, Security.

1. INTRODUCTION

With the rise of new Technology or a Product in the Industry, there is always a loophole to crack it and utilize the same without any sort of restrictions. The above gets applied to almost all the Applications as well as Operating Systems from different vendors, like Microsoft, Apple, Unix, and so on. Likewise, the menace associated with security in the Cyber domain has evolved from a tiny minuscule loophole to a huge cavity, breaching the wall of Security. The solution to an issue given out by a primitive entity based on signatures has been deemed quite feeble. The end of something marks the beginning of a new entity, and the same gets applied in the field of security governing the Information Technology Domain. The state-of-the-art Security Peripherals tend to utilize a combination of both Machine Learning as well as Artificial Intelligence. There is a need of the hour that the above-mentioned ought to automate the management of the Security in the Information Technology Sector. If we consider a rough estimation there are approximately 4328 IT-related organizations in Chennai, according to a source in Google. From the above statement, it is known that almost 3/4 of the organizations are dependent upon the resources which are associated with their Information, in order to prevail with pertinence coupled with the spirit of rivalry. A minor breach in the aspect of an organization's security means a catastrophic event is waiting to happen and would directly have an intense effect on the functioning of an organization. For the purpose of augmenting the security trait which is shielding the information related to data, the concerns and institutions may clout the technologies associated with Machine Learning as well as

Artificial Intelligence for the purpose of automating the management of security tasks as well as provision acumen on the menace affecting the security. The idea behind the terminology Artificial Intelligence is literally associated with the systems related to the Information, which in turn automates tasks which are highly convoluted as well as arduous in nature for the purpose of espial as well as the alleviation of menace. The systems which are associated with the Security mechanism have the caliber for figuring out humongous voluminous digital 0s and 1s as well as classifying the patterns which are utilized to take up the required decisions. The heart and console of Artificial Intelligence is Machine Learning, which provisions the system related to the Computers with a mechanism for enrolling and acclimate via actuality. The desideratum lies in scrutinizing the efficacy of the security solution provisioned out of Artificial Intelligence by means of bringing down the risk that may appear in terms of breaching the walls of Security while improvising the entity of competence as well as taking care of the commonly known issues in the Cyber Computing domain.

2. THEORY OF RESEARCH

An explication to the concerns arising on account of Security gets dually sorted under Signature or the entity termed as Artificial Intelligence. The explications which are rooted under Signatures utilize rules and regulations conceived by a team of experts who have inherent knowledge in the security domain for revealing the menace associated with the entity called Security. These variant explications which are associated with Security have transformed from being effective to less effective and capricious on account of the extremity rate in false positivity [4]. Moreover, there exists a delay factor which exists between dual entities, one being the distinguishing of a menace as well as the exertion of panacea. The updation of signatures ought to happen on a day to day basis, if the signatures need to be potent in the longer run.

The Computer Hacktivists, Black Hats, as well as Pentesters may take the systems for a ride when they realize there exists a delay when it comes to the release or an execution of an update, while jeopardizing the trivial entity defined as a Security associated with a system relevant to the digital 0s and 1s [3]. The individuals who utilize the Internet to wreak havoc tend to utilize, state of the art Network Adapters for conceiving a novel menace else bypass exposure when a scan gets done by security systems, which are rooted upon signatures. The diagram printed by the numeral 1 displays the blueprint of a solution based on Information security which is given out by Artificial Intelligence. From the blueprint the digital 0s and 1s from variant provenance like logs from the systems, proof of compromise, traffic from the network of computers, data from previous histories, and feed from intelligence get utilized for the abutment of learning in terms of supervised as well as unsupervised coupled with the mechanism leading to the learning based upon reinforcement. In the aftermath of the learning process, the systems involved in providing the security utilize an entity termed as a tracker associated with identity, in turn gets used for disclosing exceptional as well as ever unfolding patterns that paves a new pathway for novel attacks [5].

The entity termed as an identity tracker constitutes of dual entities termed as Systems based out of Fuzzy Logic as well as Behavior Analytics. The tracker based out of identity goes through several analysis like Future Impacts, Context, and last but not the least Reasoning [4].

The above mentioned analysis grants the systems to identify novel as well as unfolding menaces in order to etch protective means so that the required response can be given to the issue at hand. The system gets equipped with a dashboard to display the required information. The ranks which are getting identified and the relevant issue is showcased on to the dashboard. It is trivial to observe that the system associated with the security assimilates an in-built automatic response mechanism that which makes it possible to acknowledge and reply back to the issues or menace poking their heads in an automated manner sans the interference of an individual employed as an Admin.

3. PROPOSED METHODOLOGY

The methodology which is defined as Case study gets utilized for scrutinizing the caliber with respect to dual security explications based out of Artificial Intelligence. The approach embroils comprehensive scrutiny else an expedition of an anomaly. The approach which is defined as Case study was preferred on account of its ability for favoring the juxtaposition of variant facets associated with dual entities defined under the Security machineries which go hand in hand with Signature as well as Artificial Intelligence.

Apart from the above, the approach grants a green signal for an encyclopedic scrutiny relevant to the subject under study. There exists a possibility for zero downing a case which is deemed to possess deviation that can also expose novel data relative to the subject under study. The approach which is defined as Case study is defined to relevant to full-fledged peril filled with data being biased coupled with perception [9]. Dual entities are taken under for the purpose of case study, termed as Darktrace as well as Deep Instinct.

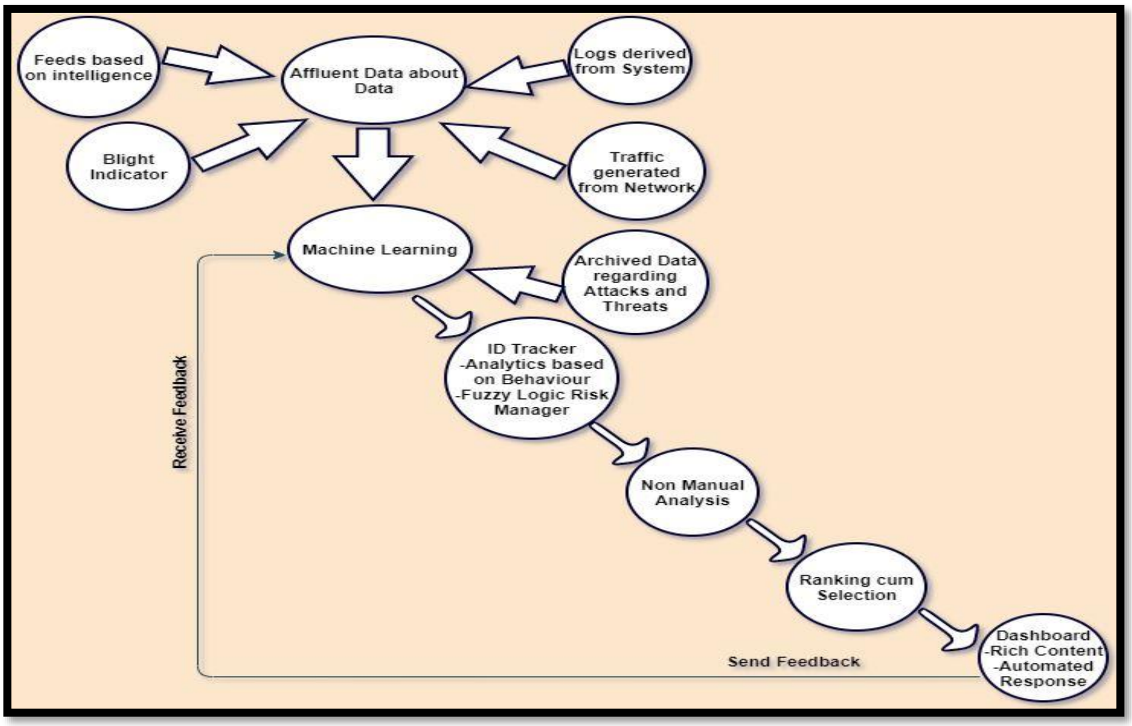

Feeds based on intelligence
Affluent Data about Data
Logs derived from System
Blight Indicator
Traffic generated from Network
Machine Learning
Archived Data regarding Attacks and Threats
Receive Feedback
ID Tracker -Analytics based on Behaviour -Fuzzy Logic Risk Manager
Non Manual Analysis
Ranking cum Selection
Send Feedback
Dashboard -Rich Content -Automated Response

Figure 2.1: Blueprint of Security Solution driven by Artificial Intelligence.

4. ALGORITHMS

For the purpose of being adequate, the security explication based out of Artificial Intelligence utilize a few variants of Algorithms concerned with learning enumerated as reinforced, supervised and as well as unsupervised. The Algorithm which is associated with learning termed "Supervised" is quite trivial in the assessment of a situation. The Algorithms which are relevant to the Learning get utilized for performing scrutiny over the experience which had happened in the past, the current prevailing situation as well as the impact which happens in the future in terms of issues which are deemed unidentified [5]. The primary and the most important trivial dissection showcased by the Algorithms incorporate three entities named Analysis of a Risk, Context and the last being Reasoning. The first entity aids the machinery associated with security to comprehend the outcome, the final goal, as well as the reason for the execution of an action. The second entity gets utilized for the investigation of the primary events associated with security coupled with their background as well as the relationship in the foreground of a Computer [6]. Last but not the least; the first entity gets utilized for the scrutiny of the pros and cons of an action and their causes which are possible. The above well defined Analyses turn out to be the stronghold for the induction of actions which seem to be available in terms of Learning Algorithm depicted under the supervised term. In terms of Algorithms depicted under Unsupervised, the entity termed as Analyses are utilized to conceive novel actions which are quite pertinent in terms of uprising as well as upcoming new sort of menaces. When the discussion gets pointed towards the Algorithm christened under reinforced, the existing analyses get utilized for the purpose of finding out patterns which are quite identical. It is conspicuous that the options which are pre-existing are loaded by default on to Machinery responsible for provisioning security which in turn gets driven by Artificial Intelligence. Therefore the Algorithms termed under Supervised Learning have the ability to give out a good response depending on the attributes of a security event deemed unidentified. On the other hand, the Learning Algorithms defined under Unsupervised tend to gain a lot of knowledge as and when the digital Information gets insinuated by them. With the reference to the above statement, there exists a possibility for the modification of the responses based upon the information received on the go [7]. Therefore the Algorithms depicted under Unsupervised, gets utilized to conceive a novel choice in terms of the systems giving security which are driven by Artificial Intelligence. The Learning Algorithm depicted under Reinforcement gets utilized to choose the best choice which is suited, depending on the output of the analysis termed cost-benefit. 'N' number of solutions circling around security, in turn driven by Artificial Intelligence tends to utilize variant Algorithms associated with Learning. The Algorithms which are associated with Learning fall under dual categories, one being close-sourced and the other falls under open-sourced. For an instance the entity defined as Deep Instinct tends to employ two variant entities namely analysis of a static file as well as modeling based out of menace predictivity for the purpose of distinguishing as well as terminating the menace in an automated fashion. The combination of source codes mentioned here, utilizes algorithms which are associated with the entity called Deep Learning for the purpose of learning as well as forecast novel assaults [7]. The coders who are involved in conceiving novel Applications constructed a network associated with a neural entity in a suitable Lab like infrastructure and then gave training with reference to a humongous volumes of digital data embedded with malevolent coding [6]. Thence the entity defined as Deep Instinct utilizes algorithms defined as Predictive, for the purpose of actuating if a particular set of codings are threatful in nature or not. The explication associated with security has the caliber to gain knowledge in a continuous manner as and when, novel sets of data tends to appear. When an application deemed malevolent gets interacted by the entity defined as Deep Instinct, the algorithms associated with it chop down the Application into very small chunks for the purpose of scrutiny [11]. The System which is associated with security functions in a same way as an entity defined as sequencing by genome, wherein minuscule sequences get utilized to tutor the network which is closely associated with neural entities for the purpose of pin pointing certain patterns which are unique in nature. The entity defined as Deep Instinct utilizes clusters associated with a Graphical Processing Unit for the purpose of supporting computations which are complex in nature.

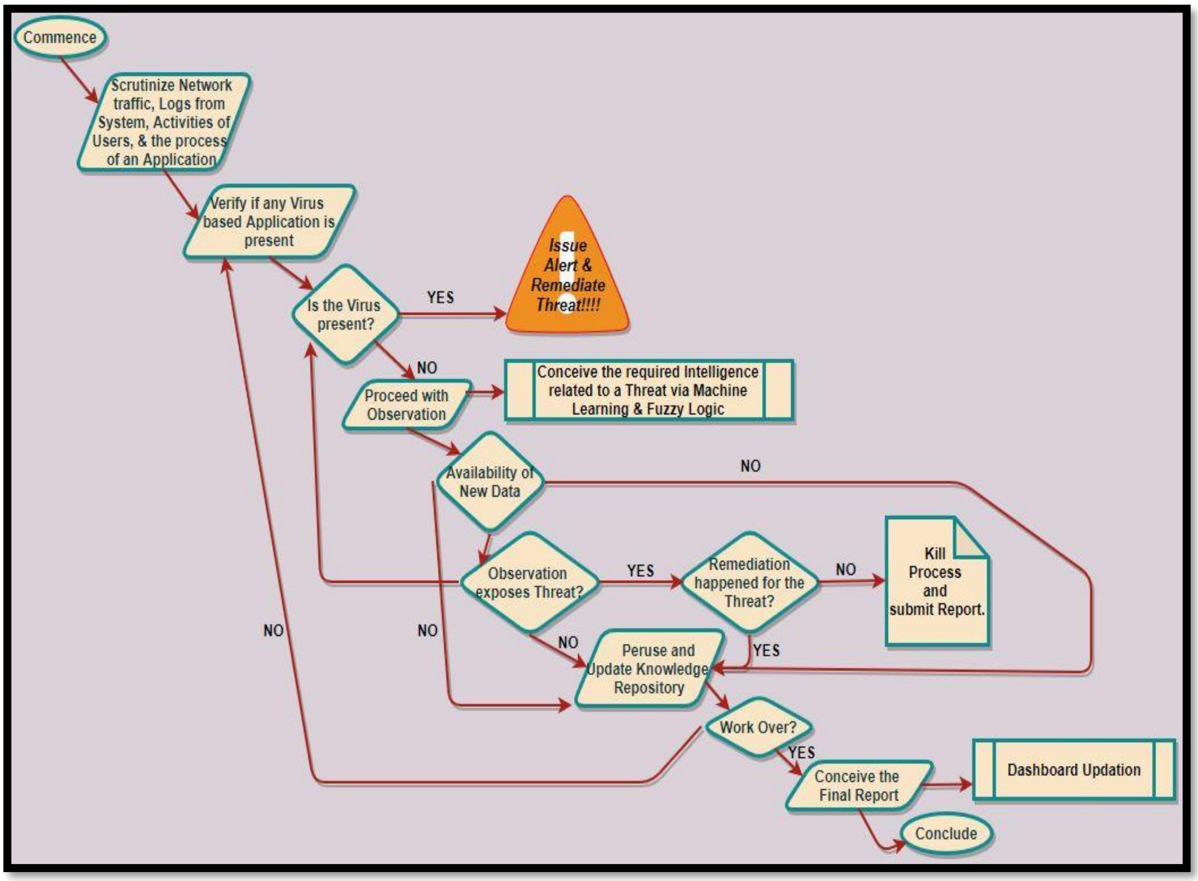

Commence
Scrutinize Network traffic, Logs from System, Activities of Users, & the process of an Application
Verify if any Virus based Application is present
Is the Virus present?
YES
Issue Alert & Remediate Threat!!!!
NO
Proceed with Observation
Conceive the required Intelligence related to a Threat via Machine Learning & Fuzzy Logic
Availability of New Data
NO
Observation exposes Threat?
YES
Remediation happened for the Threat?
NO
Kill Process and submit Report.
NO
NO
NO
Peruse and Update Knowledge Repository
YES
Work Over?
YES
Conceive the Final Report
Dashboard Updation
Conclude

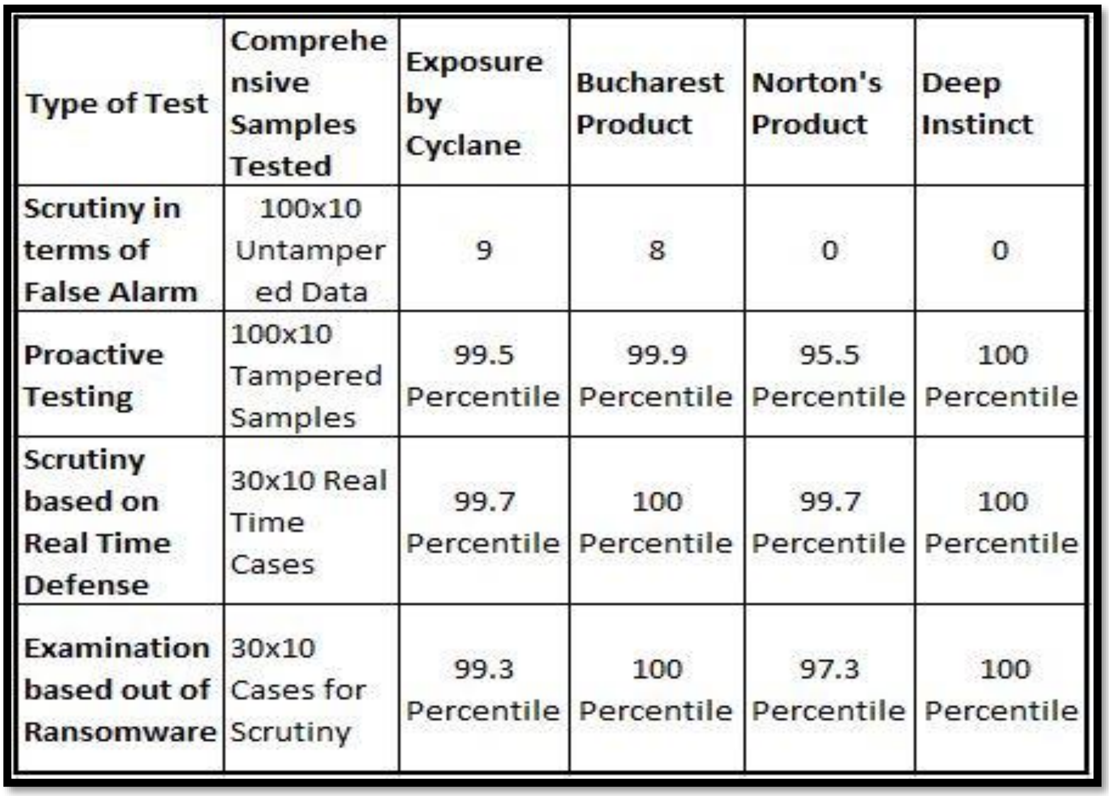
Figure 4.1: A Security System process driven by Artificial Intelligence.

The diagram under the numeral number two exposes a flow chart detailing processes which are commonly utilized by systems which are driven by Artificial Intelligence. The Flow diagram commences with the scrutiny of data taken from variant sources. The data which is gathered is then probed for any sort of Applications or any Activity which possesses any sort of malevolent behavior. In the event of any abnormality, the system at hand gives out a red flag as well as redresses the concern at hand. Post which, the same goes on to observe novel data for the detection of newer menaces as well as gain knowledge. When a specific operation gets over, the system at hand commences the creation of a report and puts it to be available to the user via a neat dashboard.

5. RESULT ANALYSIS

The Tabular Diagram depicted by the numeral One exposes the outcome of the variant test iterations which was implemented by an organization associated with Security who have marked their presence with their URL as https://www.av-comparatives.org/, and they have iterated the required tests upon the solutions given in terms of security which in turn gets driven by Artificial Intelligence. The ultimate objective of the mentioned tests is to benchmark the caliber of the explication given in terms of security referencing the automated disclosure as well as avoidance pinpointing the fact that the explications are dependent on Artificial Intelligence [11]. When initiating the test on top of 250 to 300 cases referring the entity of Website Addresses coupled with vectors involving mails, the dual unique entities named Bitdefender as well as Deep Instinct put on quite a show by casting a net of protection with a rate of one hundred percentile, while the Applications derived from Cylance as well as Symantec came out with a percentile of 98 to 99.7. The entity defined as Framework of Testing based on proactiveness got utilized for the purpose of benchmarking the caliber of security explications on account of exposing foreign as well as ever unfolding menaces. The definitions associated with each and every product was initially made stagnant before the commencement of a particular test. Tens of hundreds of novel as well as positively tested malevolent source codes got scanned by the defined set of source codes. The aftermath of the procedure came out with One Hundred percentile positive for the entity termed Deep Instinct, whilst 98 to 99 percentile for Bitdefender, then again 99.2 to 99.5 percentile for the duo entities Cylance as well as Symantec appropriately. The caliber of the systems involved in provisioning security got benchmarked with the exposure and anchoring the ransome ware menace. For the purpose of scrutinizing the competence of the quadruple entities novel clear cut samples of ransom ware got utilized and the results came out as expected with one hundred percentile clear view protectivity given out by Deep Instinct as well as Bit Defender, whilst the other duo came out with a percentile of 99 to 97 plus a few numbers. The scrutiny defined by the name "falsified alarm" showed an output of zero percent for Symantec as well as Deep Instinct while a few percentiles for the other two.

Table 1. The outcome of the selected systems driven by Artificial Intelligence



Type of Test	Comprehensive Samples Tested	Exposure by Cyclane	Bucharest Product	Norton's Product	Deep Instinct
Scrutiny in terms of False Alarm	100x10 Untampered Data	9	8	0	0
Proactive Testing	100x10 Tampered Samples	99.5 Percentile	99.9 Percentile	95.5 Percentile	100 Percentile
Scrutiny based on Real Time Defense	30x10 Real Time Cases	99.7 Percentile	100 Percentile	99.7 Percentile	100 Percentile
Examination based out of Ransomware	30x10 Cases for Scrutiny	99.3 Percentile	100 Percentile	97.3 Percentile	100 Percentile

The outcome of the observation proves that the quadruple products driven by means of Artificial Intelligence function up to their worth in terms of exposing, anchoring menaces inclusive of malevolent codings, lines of codes as well as ransom wares subsequently. The Systems which are associated with Security have the competence for exposing as well as taking evasive actions even in the event of a foreign and ever unfolding menace with utmost perfection. The reason for the above leads to the disclosure of the fact on how is it, even possible to achieve such entities; leads to the answer; Artificial Intelligence. This sort of a novel idea which utilizes the technique of Algorithms associated with Machine Learning is far superior when compared with the primitive technique of signatures, abnormal behavior of tasks as well as full-fledged beforehand wisdom of tracking malevolent Applications. The explications rooted from Artificial Intelligence have the ability to expose the unfolding menaces that deceive the primitive techniques associated with Security. Consequently the devices with the Applications based from Artificial Intelligence will be the cornerstone in setting up the concept of Automation in the aspect of Security. The moment the above mentioned entities gets thrown in the production arena the required updates can get downloaded in a centralized server and they get shot to all the devices in a network by RJ45 cables at the click of a button. The above mentioned applications will get executed sans any issues whatsoever, and will keep a watch 24/7 to plug in any loops associated with Security.

6. CONCLUSION

When it comes to compare and contrastivity the explications which are rooted upon Artificial Intelligence seems to expose extreme competence than that of tool sets which are based out of signatures. The systems which are based out of Artificial Intelligence tend to distinguish momentous aberrations which are then equated for the purpose of classifying full-fledged original menaces with minimal triggering of falsified alarms. The systems associated with security have the competence to perform actions associated with reporting, distinguishing as well as find remedy for the menace in an automated manner. The scrutinies done over explications which are based out of Artificial intelligence expose the fact that they influence the technologies of AI for self improvisation. Furthermore, the explications utilize a blend of propositions inclusive of dual methods like scrutiny of behavior coupled with distinguishing of menace based on signatures. Whilst the scrutiny of behavior get utilized for fighting off the malicious codes present in the present era, training the system as well as providing automation depends on AI. The tools based out of security, that completely depend upon the scrutiny of behavior raises a huge alarm with reference to the entity of falsified positives. This is the sole reason why the tools based out of Artificial Intelligence never are dependent on the primitive menace distinguishing technologies. With the ever-unfolding progression made to avail in the field of Computing, the tools which are based out of Artificial Intelligence would turn out to be much more adequate in terms of ensuring the trait of security, when it comes to a particular organization sans the backing of any Individual employed as a Networking Administrator.

7. REFERENCES

[1] End Point Test, Website https://tinyurl.com/endpointtesting.

[2] International Business Machines, Website https://tinyurl.com/ibmsecurities.

[3] Forbe Security Website, https://tinyurl.com/forbesecurity.

[4] Integrating Cyber-Intelligence Analysis and Active Cyber-Defense Operations, Website https://tinyurl.com/infowarfares.

[5] SIEM-Platform for Research and Educational Tasks on Processing of Security Information Events, Website https://tinyurl.com/publonssecurity.

[6] Improvising Cyber Security via AI, Website https://tinyurl.com/cybersecviaAI.

[7] Artificial intelligence techniques for cyber security Website https://tinyurl.com/cybersecAI.

[8] Application of Artificial Intelligence in fight against cyber crimes Website https://tinyurl.com/AIApply.

[9] The case study as a type of qualitative research, Website https://tinyurl.com/Qualityresearches.

[10] Training a big data machine to Defend, Website https://tinyurl.com/bigdataintel.

[11] University of Jyväskylä, Artificial Intelligence in the Cyber Security Environment, Website https://tinyurl.com/AIinCS.