International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Data Mining and Machine Learning Techniques for Cyber Security Intrusion Detection

K. Sai Manoj, P. S. Aithal

Abstract: ***An interference discovery framework is customizing that screens a singular or an arrangement of PCs for toxic activities that are away for taking or blue-penciling information or spoiling framework shows. The most methodology used as a piece of the present interference recognition framework is not prepared to deal with the dynamic and complex nature of computerized attacks on PC frameworks. In spite of the way that compelling adaptable methodologies like various frameworks of AI can realize higher discovery rates, cut down bogus alert rates and reasonable estimation and correspondence cost. The use of data mining can realize ceaseless model mining, request, gathering and littler than ordinary data stream. This examination paper portrays a connected with composing audit of AI and data delving procedures for advanced examination in the assistance of interference discovery. In perspective on the number of references or the congruity of a rising methodology, papers addressing each procedure were recognized, examined, and compacted. Since data is so fundamental in AI and data mining draws near, some striking advanced educational records used as a piece of AI and data burrowing are depicted for computerized security is shown, and a couple of recommendations on when to use a given system are given.***

Keywords: Cloud Computing, Data mining, Block Chain, Machine Learning, Cyber Security, Attacks, ADS, SMV.

I. INTRODUCTION

All through the 1990's the ascent of business enthusiasm for the Internet has lead to the joining of the data foundation as a center part of the United States economy. Nonetheless, an expanding number of digital assaults and dangers of digital assaults on our national systems have indicated that our vitality, transportation, and fund frameworks are open to possibly desperate results. While a huge division of these assaults has been insufficient, the internet has become a field for fighting and demonstrations of fear-based oppression, since it controls different basic frameworks. Securing these foundations has become a basic and key territory of enthusiasm for a country barriers. Current digital security capacities have advanced to a great extent as patches and additional items to the Internet, which was structured on the standards of open correspondence and understood shared trust. It is currently perceived that it is never again adequate to pursue such developmental ways and that security must be a fundamental piece of the data foundation. Existing interruption location frameworks have advanced as discrete specially appointed abilities and are not adequate for reacting to complex and masked digital assaults anticipated from well-supported psychological militant associations. This made a chance to build up another bearing on enormous scale and coordinated interruption discovery and reaction frameworks, which is the fundamental inspiration for this paper [1].

Proposition The Machine learning, Data Mining strategies are depicted, and furthermore a couple of usages of each system to computerized interference identification issues. The diverse nature of different AI and data mining counts is discussed, and the paper gives a course of action of assessment criteria for AI and data mining methods and a game plan of recommendations on the best techniques to use depends upon the qualities of the computerized Issue to handle Cybersecurity is the game plan of advances and methodology planned to guarantee PCs, frameworks, ventures, and data from ambush, unapproved access, change, or pounding. Computerized security frameworks are made out of framework security frameworks and PC security frameworks. Each of these has, in any event, a firewall, antivirus programming, and an interference recognition framework. Intrusion discovery frameworks help find, choose, and perceive unapproved use, duplication, alteration, and pulverization of information frameworks.

The security breaks consolidate external interferences ambushes from outside the affiliation and inside interferences. There are three essential sorts of advanced assessment in the help of interference identification frameworks: misuse based, oddity based, and crossbreed. Misuse based methodologies are expected to recognize realized attacks by using characteristics of those ambushes. They are effective for perceiving known kinds of attacks without making a stunning number of bogus alerts. They require to visit manual updates of the database with rules and stamps. Misuse based methodology can't recognize novel attacks. Idiosyncrasy based techniques show the conventional framework and framework lead and recognize peculiarities as deviations from ordinary direct. [2]

They are drawing in an aftereffect of their ability to perceive zero-day ambushes. Another favored point of view is that the profiles of commonplace development are changed for every framework, application, or framework, thusly making it inconvenient for attackers to realize which practices they can finish undetected.

Revised Manuscript Received on February 05, 2020.

* Correspondence Author

Dr. K. Sai Manoj*, Member IEEE & Postdoctoral researcher, Department of CSE, Srinivas University, Karnataka, Mangalore, India.

CEO, Amrita Sai Institute of Science and Technology and Innogeecks Technologies, Vijayawada, AP, India.

Dr. P. S. Aithal, Member IEEE & Vice-Chancellor, Srinivas University, Karnataka, Mangalore, India.

Besides, the data on which variation from the norm-based frameworks alert can be used to portray the imprints for misuse discoverers. The key obstacle of irregularity based techniques is the potential for high bogus alarm rates in light of the fact that previously covered framework practices may be requested as peculiarities. This paper fixates basically on advanced interference location as it applies to wired frameworks. With a wired framework, an adversary must experience a couple of layers of shield at firewalls and working frameworks or increment physical access to the framework. In any case, a remote framework can be engaged at any center point, so it is regularly more helpless against vindictive ambushes than a wired framework. The Machine learning and data mining methodologies campaigned in this paper are totally material to the interference and misuse recognition issues in both wired and remote frameworks. The peruser who needs a point of view focused just on remote framework protection is suggested papers, for instance, Zhang et al, which focuses more on one of a kind changing framework topology, coordinating computations, decentralized organization, etc.

II. METHODOLOGY

Related Work The essayists SongnianLi, Suzana Dragicevic, et al. in made a study on various geospatial theories and procedures used to manage geospatial immense data. Given some phenomenal properties, makers thought about that standard data taking controlling ways of thinking and frameworks are missing and the going with spaces were seen as in need for advancing progress and assessment in the control. This wires the degrees of progress in tallies to supervise the steady examination and to advance flooding data, and furthermore improving new spatial requesting systems. The difference in speculative and methodological ways to deal with deal with the trading of enormous data from illustrative and parallel research and applications to ones that analyze pleasant and illustrative affiliations. In Yuehu Liu, Bin Chen et al. have proposed another strategy for controlling monstrous remote identifying picture data by utilizing HBase and MapReduce framework. From the start, they have divided the certified picture into various little pieces, and store the squares in HBase, which is dissipated in a social event of focuses [3].

They have used a MapReduce programming model on managing the set away pieces, which can be simultaneously executed in a social event of focuses. The middle focuses in the Hadoop bunch have no necessities for predominant and precision with the objective that they can be especially affordable. Likewise, in light of the high flexibility of Hadoop, it is unquestionably not difficult to add new focuses to the gathering, which was regularly staggeringly problematic with everything taken into account ways. Finally, they see that the paces of data exchange and taking care of addition in light of the fact that the pack of HBase creates. The outcomes show that HBase is to an incredible degree reasonable for considerable picture information gathering and managing. The makers Chaowei Yang, Michael Goodchild et al. in have foreseen a substitution paralleling limit and access strategy for huge scale NetCDF sensible information that is maintained liable to Hadoop.

The recovery framework is acknowledged ward on MapReduce. Argo data is utilized to show the proposed methodology. The execution is looked a spreading space considering PCs by utilizing indisputable data scale and varying task numbers. The assessments result shows that the parallel procedure can be utilized to store and recuperate the gigantic scale NetCDF gainfully. Huge data has changed into a noteworthy focal point of generally speaking interest that is coherently pulling in the assertion of the educated gathering, industry, government and other association [4].

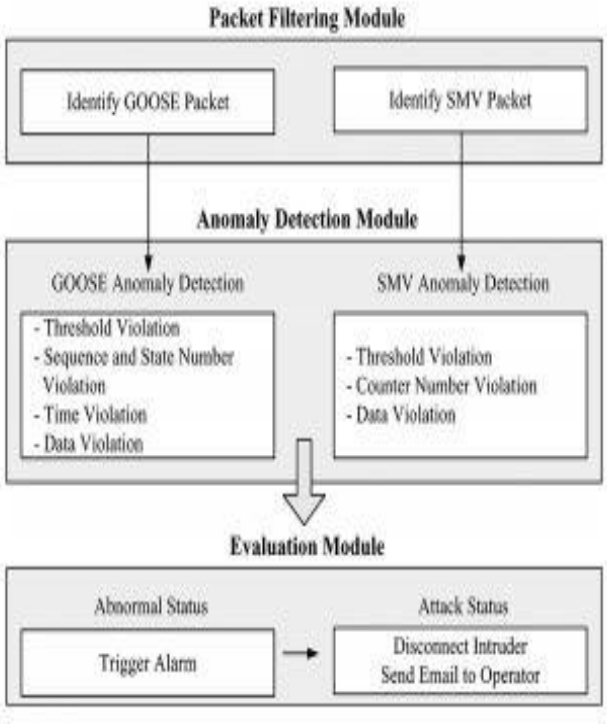

Figure.1: Packet filtering internal Process

This paper is worried about inconsistency recognition at a substation. An incorporated technique for have based and arrange based oddity location plans is proposed. The host-based irregularity location utilizes an efficient extraction procedure for interruption impressions that can be utilized to recognize believable interruption occasions inside a substation, e.g., firewall, UI, IEDs, and circuit breakers. The system put together irregularity discovery is engaged with respect to multicast messages in a substation arrange; it additionally identifies, in a continuous domain, oddities that exhibit anomalous practices. The fundamental commitment of this paper is another technique for

- an incorporated peculiarity discovery framework for the insurance of IEC 61850 based substation mechanization framework, e.g., IEDs, UI, and firewall, and
- a system based irregularity location calculation that can be utilized to recognize pernicious exercises of IEC 61850 based multicast conventions,

e.g., GOOSE and SMV, over the substation organize. Inconsistency location for multicast messages in substation mechanization arrange is another field of research for the power lattices. In this examination, a cybersecurity tested has been created and used to approve the proposed peculiarity identification calculations. Digital interruptions are reproduced utilizing the tried including defensive IEDs. The test outcomes exhibit that proposed abnormality recognition calculations are compelling for the identification of recreated assaults [3].

III. RELATED WORK

Technical Approach

We built up an incorporated cybersecurity system for recognizing and containing digital assaults at the degree of hierarchical system space. This structure comprises of three parts: interruption discovery, assault source restriction, and assault regulation. For the first and third segments, we used the current techniques just as built up a few new parts. Specifically, we created novel data combination strategies for having level peculiarity discovery and furthermore for organizing level determination and assault source distinguishing proof.

Our coordinated system for interruption location and regulation accommodates versatility by enabling different sensor motors to work in parallel. Single system sensors can just deal with little traffic stacks and are regularly constrained in their usefulness. Just by working in a conveyed manner can a largescale approach be effective. This new approach works in a self-governing way that permits close to an ongoing reaction to occasions and to guarantee that the most recent mark refreshes are accessible to the sensors when they exist. Current interruption location frameworks are not self-sufficient and depend on human mediation as a key piece of their activity, which makes them requests of size slower than required. An immediate human-on the up and up activity can't generally viably counter the more up to date digital assaults, especially, at high system speeds. By utilizing a self-governing and dispersed structure that appeared in Figure 1 the sensor yields from different pieces of the authoritative system space can be quickly connected [4].

Our structure is fit for tending to the switches to set parcel channels and the firewalls to square explicit ports. Together they structure a functioning reaction that is actuated by the source detachment segment. For any presumed assault, its mark is acquired by the identification module together with the physical ways prompting the districts of the assault source. This part enacts the channels along with the physical ways from the assault source to deny entry rights to the assault bundles. Therefore the degree of the assault's scope is contained. We researched two classes of assault control strategies. The primary strategy is appropriate for assaults that produce low degrees of traffic, for example, unapproved logins. Here the fusers can promptly trade information with sensors and actuate the firewalls nearest to the source to sift through the bundles from the assault machine. This strategy, be that as it may, doesn't work on account of assaults that create high traffic, for example, a forswearing of administration assaults. To deal with these cases, in this system the fuser grows the rate controls step by step from the close by channels to more remote ones [6].

Preparative assaults establish a developing subclass of digital interruptions, which depend on relentlessly trading off hosts and utilizing them as platforms to assault different hosts. Specific sorts of worms (e.g., Code Red II) that sustain by spreading from host to have a place with this subclass. Facilitated disavowal of-administration assaults that gather zombies into a stockpile of traded off hosts to enact them at a later point, and spam generators that use a suite of bargained hosts to send email floods, have a place with this subclass. It is critical to detach the inception of assaults, which can possibly recognize insider and outer assaults. The capacity and speed with which such determination can be performed relying upon the exact idea of the assault and sensors that recognize different assault side effects. In this paper, we present a dynamic system that uses the propagative idea of these assaults to acquire effective issue source separation calculations by using the information (when accessible) of the sensor initiation times and assault proliferation times.

The basic attribute of this subclass of digital assaults important to us is that the assault proliferates over the system by "tainting 'one host or hub after another. The other assault qualities could fluctuate altogether in the sort of host bargain, the procedure for picking and assaulting has, and the produced time and traffic scales could differ broadly. In some worm assaults, the objective is to engender quickly, regularly arbitrarily, so as to taint whatever number has as would be prudent [Weaver et al 2003, Shankar et al 2003].

This conduct normally brings about the old style S-bend of the number of contaminated hosts: the pace of disease begins gradually during the underlying stage, rapidly turns out to be exceptionally high as the worm develops in quality, and afterward decreases when a large portion of the powerless targets are undermined. Zombies that are made for disavowal of-administration or spam assaults use an increasingly conscious methodology of trading off hosts without creating high traffic levels and ordinarily spread all the more gradually. Increasingly insightful worms like Nimda and Code Red II check the nearby systems more every now and again than they examine remote systems. The absence of information on the endeavor's inner system addresses proposes that such worms would choose a technique of filtering and spread deliberately and not haphazardly inside the undertaking intranet [7].

We explored expository and algorithmic parts of diagnosing a conventional class of preparative assaults that spread crosswise over big business organizes by relentlessly bargaining hosts and afterward utilizing them to assault different hosts. Particular kinds of worms and preliminary periods of facilitated forswearing of-administration and spam assaults have a place with this class. Side effects of such assaults are identified at the system sensors by bundle marks and traffic attributes, and at the hosts by execution corruptions and peculiar framework conduct. We indicated that data about worm spread occasions and dynamic sensor initiation times can be intertwined with the system basic data to:

a) Seclude the districts of the system that contain the first assault starting point, and
b) Anticipate the following arrangement of target has.

We built up the assault spread charts that catch the over three kinds of data and tackled the source disconnection and admonishing issues utilizing diagram calculations. As the assault spreads, its side effects are distinguished by the sensors situated at the hubs, which could themselves fluctuate in their abilities and execution. In light of the areas and enactment times of the sensors that recognize an assault, we indicated that the source can be confined inside specific districts of the system. We considered two sorts of sensors sent to recognize the side effects of cyber attacks, in particular host and system sensors. Host sensors commonly recognize assaults by using bundle marks, framework trouble making and execution debasements, and strange traffic levels to and from the host.

System sensors work on the traffic streams inside the region of switches, switches, and firewalls; they recognize assaults by examining bundle marks just as by watching oddity examples of individual and total traffic streams. These two sorts of sensors could give subjectively extraordinary data, which is commonly limited in either case.

A venture arranges sends a blend of host sensors and deliberately found system sensors. We created calculations to consolidate the data from different sensors together with the basic network data to seclude the districts that contain the assault starting point. Specifically, these strategies choose if the assault began outside or inside the venture; in the previous case, firewalls at entryway switches can be actuated to drop the assault parcels, and in the last case, fitting neighborhood firewalls can be enacted to isolate the sources. We additionally created calculations to anticipate the following arrangement of potential objective hubs dependent on the present sensor data with the goal that nearby firewalls can be enacted early to counteract the further spread of assault [8].

The areas of traded off hosts together with the condition of sensor enactments give the auxiliary direction data about the assault to aid finding. The sensor initiation times together with the evaluated assault spread occasions give us the directional data about the assault proliferation. We combined the auxiliary and directional data to seclude districts of the system that contain the first assault source. Our techniques are viable for assaults that spread purposely and structure the class of topological worms that normally work in the intranet setting just as for worms that target has haphazardly over the Internet however start inside the intranet. As is not out of the ordinary, the accuracy of seclusion and cautioning relies upon:

a) Areas of host and system sensors,
b) Arrange availability, and
c) System, engendering times, and sensor enactment properties of the assault.

Moreover, the degree of information about every one of these things can likewise have a critical effect both on the calculations and their exactness for separation and cautioning.

We created engendering diagram models that catch the properties (i) and (ii). Utilizing the data about the properties in (iii), we infer a reasonable sub graph that will be utilized both for segregation and cautioning. Such a methodology, to be specific using a preparative diagram for finding, has been used in process plants [Ira et al 1985], dynamical frameworks [Rao and Viswanadha 1987] and optical systems [Mas and Thiran 2000].

While these frameworks are very unique in relation to PC systems, they all offer certain basic properties that make it conceivable to take care of starting point detachment and admonishing issues. We expanded and adjusted the techniques created for chart based frameworks [Rao 1993a, 1993b] to propagative digital assaults. These augmentations included recognizing and characterizing the significant properties of PC systems and digital assaults as an engendering chart, and afterward using the fitting diagram calculations.

An enormous number of interruptions, for example, port sweeps, login endeavors, and support flood assaults can be recognized at the hosts by coordinating the headers and substance of system parcels with known marks. These systems are genuinely experienced and are accessible as freeware, for example, grunt, and framed a few segments of our design. While these techniques identify known assaults, another key issue in interruption recognition today is the capacity to recognize new assaults. The foremost approach to achieve this is the recognizable proof of oddities, in particular distorted deviations from typical conduct, that are covered up inside a foundation of ordinary action. Abnormality recognition is pivotal against new systems, for which no realized mark exists.

We built up a strategy for distinguishing the projects running on the hosts with bizarre framework calls; specifically, we use histograms of framework calls of a program as a mark. An identifier is prepared on-line on the host utilizing known projects and few assault programs [7].

Such a methodology has been utilized recently dependent on the Basic System Module (BSM) information that contains the framework calls made by a program. The strategies dependent on k-closest neighbor and bolster vector machines have been utilized with great achievement, however both these techniques left leftover forecast blunders.

We built up a data combination based way to deal with preparing a few neural system locators, wherein these different indicators are intertwined with the closest neighbor rule to produce the last answer. Such techniques are promising in that they can be appeared to perform in any event comparable to the best among the finders intertwined. Truth be told, a crucial outcome in locator hypothesis expresses that there is no single best indicator however each performs well under various conditions.

Our combination approach accomplishes the best execution among the accessible locators. By and by, be that as it may, the client must be suitably picked to accomplish such execution. We recently built up the closest neighbor projective fusers that have been appeared to beat the individual identifier. For the abnormality location part of our framework, we built up a client design on BSM information, which performed superior to the previous techniques on the DARPA benchmark test set [7]. This arrangement utilized a straight fuser to initially consolidate 10 sigmoid neural systems and the closest neighbor rule. At that point a meta-fuser dependent on the closest neighbor projective combination strategy [Rao 2002] is conveyed the join the first locators and the straight fuser. The resultant melded identifier can be scientifically appeared to perform at any rate just as the best blend of the indicators. This framework accomplished zero mistakes on the DARPA benchmark dataset, which is the best execution for this dataset [9].

IV. RESULTS AND DISCUSSION

The usage results can be appeared as a figure beneath Imagining and checking the possibility of data. There are wide blends of procedures open and changed as per imagining, dissect, control and composite immense data to make this sort of data volume reasonable. A portion of these systems are data blend, pack assessment, organize examination, swarm sourcing, Association oversees learning, AI, etc. In this portion, we have verified a portion of these systems and their challenges rapidly.

A. **Data Fusion:** Traditional data dealing with every so often considers data from one territory. In this enormous data time, everyone needs to settle on a wide decision of datasets from completely startling sources in a couple of regions. Each of these datasets contains various methods; for instance, exchange depiction, estimations, scale, dispersal, and consistency. Removing the intensity of information from different unique (anyway perhaps related) instructive files is a remarkable course of action in tremendous data investigate, which joins basically isolating colossal data from standard data mining tries. Which itself prompts pushed systems that can brush data blend and common data mix pondered in the database pack.

Digital substations of a power matrix are a wellspring of helplessness since most substations are unmanned and with a constrained assurance of physical security. In the most pessimistic scenario, concurrent interruptions into numerous substations can prompt extreme falling occasions, causing cataclysmic power blackouts. In this paper, a coordinated Anomaly Detection System (ADS) is proposed which contains host-and system based inconsistency location frameworks for the substations, and synchronous peculiarity identification for various substations.

Potential situations of concurrent interruptions into the substations have been reproduced utilizing a substation robotization tested. The host-based peculiarity location thinks about transient oddities in the substation offices, e.g., UIs, Intelligent Electronic Devices (IEDs) and circuit breakers. The malignant practices of substation computerization dependent on multicast messages, e.g., Generic Object Oriented Substation Event (GOOSE) and Sampled Measured Value (SMV), are consolidated in the proposed system based oddity recognition. The proposed synchronous interruption discovery technique can distinguish a similar kind of assault at numerous substations and their areas. The outcome is another incorporated device for the discovery and alleviation of digital interruptions at a solitary substation or numerous substations.

B. Publicly supporting: The term publicly supporting means to data acquiring by colossal and diverse social events of individuals, who a critical piece of the time are not prepared measurer and who don't have unprecedented PC getting the hang of, utilizing web headway. Thusly, this information is exchanged to and verified in a regular PC building, for example, a focal or a joined database, or in a scattered enrolling condition. The subsequent endeavor of altered data joining and dealing with is crucial to convey additional data. An assortment of data mining strategies can be associated with find affiliations and regularities in data remove learning in the kinds of fundamentals and envision the estimation of the dependent elements [9].

System Based Anomaly Detection The proposed technique additionally gives a system based peculiarity location calculation for multicast messages in the substation computerization arrange. The multicast messages depend on the IEC 61850 standard, e.g., GOOSE and SMV. The proposed Substation Multicast Message Anomaly Detection (SMMAD) model in Fig. 3 is partitioned into 3 procedure modules, i.e., parcel separating, peculiarity recognition, and assessment. The parcel sifting module comprises of capacities to recognize GOOSE and SMV messages. The channel will just permit going for GOOSE and SMV messages so the weight of preparing can be decreased and the framework execution will increment. The abnormality recognition module is utilized to discover infringement dependent on predefined rules. The assessment module will choose if the identified inconsistency status is "anomalous" or "assault." Details will be clarified in the following area.

Note that the proposed ADS can catch the GOOSE and SMV without the port reflecting capacity as it is centered on multicast messages and not different parcels.

We built up a disseminated and self-ruling structure able to do rapidly distinguishing existing and new assaults. It comprises of individual parts for the system and host-level interruption identification, assault source limitation, and assault control. The recognition part is a blend of system and host-based sensors that use the sensor information together with the system data to distinguish the assaults. We built up a data combination technique for distinguishing the host programs with irregular framework calls.

We are the first to create assault source seclusion techniques for propagative system assaults. The source confinement part is enacted by a speculated assault and finds the assault source(s) by following or reproducing the physical ways of assault parcels. The assault control segment uses firewalls and bundle channels on different host and system areas to manage or contain the parcel stream from the assault source inside the hierarchical system space. The execution of these regulation modules will be sought after as a pursue on action to this LDRD venture. These modules together with the ones created under this undertaking will establish a complete digital system for association level security [8,9].

V. CONCLUSION

In proposed work, the conjecture and evasion of various restorative illnesses is done using PCA, Canny edge manager nearby some handling and post-getting ready advances. Directly off the bat edge acknowledgment is done by then incorporate extraction is done to get the upgraded no. of feature to gather among tainted and nontainted afflictions. The following advances will be taken after to get the proposed sickness conjecture to illustrate. The proposed structure has been totally realized attempted with real CT analyze pictures. The objective is to help successful picture data taking care of and feature extraction. Obviously, to oversee certifiable picture data, the image planning gadget must have basic characteristics, for instance, being uproar tolerant, capable, reasonable, and accommodating to use. The purpose of this assessment was to perceive features for exact pictures. A gathering of data mining procedures can be associated with find affiliations and regularities in data, separate learning in the sorts of standards and predict the estimation of the poor variables. Fundamental data mining techniques which are used as a piece of the extensive number of divisions are recorded as: Naive Bayes, Decision Tree, Artificial neural framework (ANN), Bagging figuring,

K-nearest neighborhood (KNN), Support vector machine (SVM, etc. Data mining is a basic development of learning disclosure in databases (KDD) which is an iterative technique of data cleaning, compromise of data, data assurance, structure affirmation, and data mining learning affirmation. KDD and data mining are in like manner used correspondingly.

Data mining fuses association, gathering, packing, quantifiable examination, and desire.

A progressively outrageous Sub threshold Slope (SS) is gotten diverged from standard CMOS, considering the better electrostatic control and nonappearance of doping. Other than the diminishment of the spillage current, the multigate topology of the FinFET moreover grows the drain-source drenching current of the contraption with a factor two at a comparative inclination condition. In meager (or limit) mitigate devices, for instance, a FinFET, volume inversion takes place. In volume inversion charge bearers are not held near the (SiSiO2) interface, but instead all through the entire body of the device. Thusly the charge transporters experience less interface scrambling. Hence an extension of the adaptability and transconductance is ordinary in multigate devices. The different entryway structure of the FinFET diminishes the short channel impacts. To also improve the power over the channel.

This paper gives an incorporated peculiarity location framework which contains host-and system based inconsistency identification for a solitary substation, and concurrent oddity discovery for different substations. The host-based ADS utilizes logs that are extricated from vindictive impressions of interruption-based strides crosswise over substation offices. The system based ADS can identify vindictive practices that are identified with multicast messages in the substation arrange. The proposed concurrent interruption recognition strategy can locate a similar kind of assaults on different substations and their areas.

REFERENCES

1. Factom Partners With Honduras Government on Blockchain Tech Trial,http://www.coindesk.com/factom-land-registry-deal-hondurangovernment/
2. Blockchain Adoption Moving Rapidly in Banking and Financial Markets: Some 65 Percent of Surveyed Banks Expect to be in Production in Three Years, https://www-03.ibm.com/press/us/en/pressrelease/50617.wss
3. Bitcoin Developer Guide, https://bitcoin.org/en/developer-guide#blockchain-overview
4. Chapter 7. The Blockchain, http://chimera.labs.oreilly.com/books/1234000001802/ch07.html/
5. Cyber Crime Costs Projected To Reach $2 Trillion by 2019, http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crimecosts - projected-to-reach-2-trillion-by-2019/#768e4f293bb0
6. Tendermint: Consensus without Mining, http://tendermint.com/docs/tendermint.pdf
7. What is Ethereum, https://cryptocrawl.in/what-is-ethereum/
8. Will Knight, “Anti-Snooping Operating System Close to Launch,” NewScientist, (May 28, 2002).
9. Riptech Internet Security Threat Report (January 2002). www.riptech.com.

AUTHORS PROFILE

Dr. K. Sai Manoj, CEO of Amrita Sai Institute of Science and Technology / Innogeecks Technologies has extensive experience in financial services, IT Services and education domain. He is doing active research pointing to the industry related problems on Cloud Computing, Cloud Security, Cyber security, Ethical Hacking, Blockchain (DLT) and also on the Penetration testing. He obtained PhD Degree in Cloud Computing. He was completed M.Tech., in Information technology from IIIT Bangalore. He published research articles in various scientific journals and also in various UGC approved journals with Thomson Reuter id. Also He was presented innovative articles at High Standard IEEE and Springer Based Conferences. He has various professional certifications like Microsoft Certified Technology Specialist (MCTS), CEHv9, ECSA, CHFI, Chem., and “Paul Harris Fellow” recognition by Rotary International. He is currently doing post-doctoral work in Cloud Computing.

Prof. Dr. P. Sreeramana Aithal, Currently Vice-Chancellor of Srinivas University, Karnataka. he has 29 years experience in Teaching & Research and 18 years experience in Administration. Dr. P. S. Aithal has secured the First Rank in TOP 12,000 Business Management Authors in the Global Ranking of Elsevier’s SSRN (USA) for maximum number of Research papers publications during 2017 & 2018. He has worked as Principal at Srinivas Institute of Management Studies, Mangalore from 2001-2017. Dr. P. S. Aithal studied his B.Sc. (Physics, Chemistry, & Mathematics) from Poornaprajna College, Udupi during 1985-88. Having four Master degrees in Physics with Electronics, Computer Science, Information Technology, and E-Business, he got his first Ph.D. degree in Physics from Mangalore University in the area of nonlinear optical materials and second Ph.D. degree in Business Management from Manipal University, Manipal, in the area of mobile banking.

He worked as Post Doctoral Research Fellow at “Lasers & Quantum Optics Division, Physical Research Laboratory, Ahmedabad for two years from 1999-2000. In the year 2002, he has been selected for the prestigious Oversee Fellowship of Dept. of Science & Technology, Govt. of India – Better Opportunity for Young Scientists in Chosen Area of Science & Technology (BOYSCAST) Fellowship and did Post Doctoral Research at Centre for Research & Education in Optics & Lasers (CREOL), at University of Central Florida, Orlando, U.S.A. During his Post Doctoral Research at Ahmedabad & USA, he has worked in the area of Nonlinear Optics, Photonics, Optical Limiters and Optical Solitons. Dr. Aithal has got SERC Young Scientist Project on Nonlinear Optics funded by Dept. of Science & Technology, India. Dr. Aithal also had a visiting Associateship at Physical Research Laboratory, Ahmedabad, and Visiting Professorship of Grimsby Institute of Further & Higher Studies, Grimsby, U.K. He has 42 research publications in refereed International Journals in the area of Nonlinear Optics and Photonics, and 350 in refereed International Journals publications in Business Management, Higher Education, and Information Technology.

He has presented more than 300 research papers in National & International Conferences/Seminars. Presently he is guiding research scholars for their M.Phil. and Ph.D. degrees in Electronics, Information technology, and business management. Dr. Aithal has developed Teaching Materials in Operations Research, Quantitative Techniques, Research Methodology, Management Information Systems, International Business, Communication networks and Mobile Communication for MBA & MCA Courses. He has also written textbooks on Engineering Physics and Basic Electronics for Engineering Students, which have been published by ACME Publishers, New Delhi. He has research interest in Nonlinear optical absorption, Optical Phase Conjugation, Photorefractive materials, e-business, m-business, ideal business, and nanotechnology business Opportunities. Dr. Aithal is member of World Productivity Council, U.K., member of Strategic Management Forum, India, member of Photonics Society of India, CUSAT, Cochin, senior member of IEDRC.org, Singapore. Dr. P. S. Aithal has edited Twenty Conference Proceedings with ISBN numbers and recently published a book on "Quality in Higher Education" a case study of SIMS. Being a pioneer researcher, Dr. Aithal has developed a new Theory of Organizational Behaviour in 21st Century called Theory on Accountability (Theory A).

He has also developed a new model for measuring Research productivity called ABC model. He has developed a new Analysis framework for Concepts, ideas, systems, strategies and models called ABCD analysis technique. He has developed and published a new model of nanotechnology commercialization and Analyzing practical systems based on Ideal system Characteristics. Apart from teaching and research, Dr. Aithal has been involved in institution building activities since 15 years as a team member of Srinivas group and presently there are 18 institutions imparting quality education under Srinivas Group (www.srinivasgroup.com) and during 2013, Srinivas Group of Institutions became a Private University as Srinivas University and Dr. Aithal has got an opportunity to serve as first Vice-Chancellor of the University.

With the successful leadership of Dr. P. S. Aithal, Srinivas Institute of Management Studies has been Ranked #1 among Top International Business Schools other than USA and Ranked #4 among Top World Business Schools including USA in the Total number of research paper publications during 2018 by Elsevier’s Social Science Research Network (SSRN), USA.

Google Scholar : 550 Articles, Citations - 3,400; H-Index – 30, i-10-Index – 117.

SSRN : Full Papers – 360, Citations – 3,360, Top Business Author Ranking – 03.

ResearchGate : Papers -445, My Readers – 3,75,000, Citations – 3,340. Score – 98.5% as on 30/10/2019.