International Journal of Advanced Science and Research
ISSN: 2455-4227; Impact Factor: RJIF 5.12
Received: 26-07-2020; Accepted: 11-08-2020; Published: 29-08-2020
www.allsciencejournal.com
Volume 5; Issue 5; 2020; Page No. 14-20

An inventive technique of recital and data methodologies in ids of cloud computing technology

Ravichandran S[1], Rajkumar R[2]
[1] Professor, Computer Science Department, Annai Fathima College of Arts and Science, Madurai, Tamil Nadu, India
[2] Assistant Professor, Computer Science Department, Annai Fathima College of Arts and Science, Madurai, Tamil Nadu, India

Abstract
The main objective of Intrusion Detection System (IDS) is to dissect occasions on the system and distinguish assaults. The expanding number of system security related episodes makes it vital for associations to effectively ensure their touchy information with the establishment of interruption identification frameworks (IDS). Individuals are given more consideration on interruption location which as a significant PC organize security innovation. As per the improvement pattern of interruption recognition, recognizing a wide range of interruptions successfully requires a worldwide perspective on the checked system, Here, examine about new interruption identification component dependent on distributed computing, which can compensate for the lack of customary interruption discovery, and end up being incredible adaptable.

Keywords: cloud computing, ids, security issues, denial-of-service, grid computing, attack exposure

1. Introduction
Distributed computing is another and developing data innovation that changes the way IT compositional arrangements are advanced by methods for moving towards the subject of virtualization: of information stockpiling, of nearby systems (foundation) just as programming [1] [2]. The achievement of cutting edge advancements exceptionally relies upon its viability of the world's standards, its usability by end clients and in particular its level of data security and control. Worldwide Data Corporation (IDC) led a study of IT chiefs and their line-business associates to check their sentiments and comprehend their organizations' utilization of IT cloud administrations. Security positioned first as the best test or issue of distributed computing.

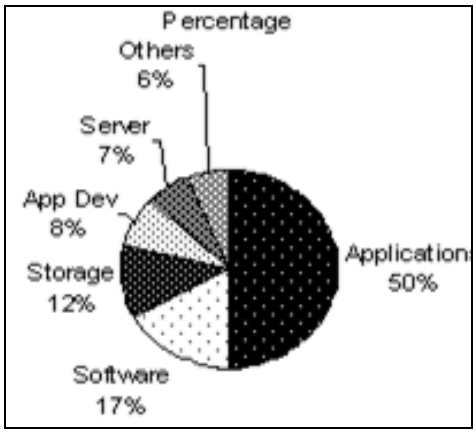

Fig 1: Worldwide IT Cloud Design

In the seller viewpoint of driving of distributed computing is simpler for application merchants to arrive at new clients; ease method of conveying and supporting applications; capacity to utilize product worker and capacity equipment; capacity to drive down server farm operational expenses, and the client point of view of distributed computing is quicker, less complex and less expensive to utilize cloud applications; no forthright capital required for workers and capacity; no continuous costs for running server farm; applications can be gotten to from anyplace and whenever. Some normal distributed computing difficulties are: information insurance, information recuperation and accessibility, the board abilities, and the administrative and consistence limitations. A portion of the distributed computing common advantages are: decreased cost, expanded capacity, speedy and simple usage, and adaptability. The interruption discovery innovation is the way toward distinguishing system movement that can prompt a tradeoff of security strategy. Homegrown exploration foundations and system security Products Company Also did related examination, yet the homegrown interruption recognition items are less. In any case, current interruption identification frameworks have a few disadvantages: lacking location rates, an excessive number of interruptions recognized or missed. In The new interruption recognition component dependent on distributed computing, With it, on any system site, a neighborhood location motor examinations the information gathered by distributed computing place to discover interruption designs. Thereafter, all the created cautions are handled by a worldwide interruption Detection motor to discover more perplexing interruptions and to give a worldwide perspective on the system security. In this paper portrayed in segment 2 distributed computing outline like distributed computing administrations and security issues, and area 3 cloud based interruption recognition framework - interruption location framework techniques and interruption discovery framework administrations with assessment of approaches and end.

2. Related Work
2.1 Cloud Computing Services
The Cloud computing is a model for empowering universal, advantageous, on-request network admittance to a common pool of configurable figuring assets (e.g., networks,

workers, stockpiling, applications, and administrations) that can be quickly provisioned and delivered with insignificant administration exertion or specialist co-op collaboration [3]. There are three conveyance models; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

2.1.1 Securing Infrastructure-as-a-service

The facilitating of equipment in an outer server farm is some of the time called as foundation as an assistance. In this model allows client's rent to lease, stockpiling, organization, and different assets in a virtualized condition. The client doesn't oversee or control the fundamental cloud framework however has power over the OS, stockpiling, conveyed applications, and potentially certain systems administration segments. Amazon's Elastic Compute Cloud (EC2) is a genuine case of IaaS. At the cloud foundation level, CSP can authorize network security with interruption identification frameworks (IDS), firewalls, antivirus programs, dispersed forswearing of-administration (DDoS) safeguards, etc.

2.1.2 Securing Platform-as-a-service

Stage benefits additionally called as middleware as an assistance. Cloud stages are based on head of foundation administration with framework mix and virtualization middleware uphold. Such stages let clients convey client manufactured programming applications onto the cloud framework utilizing supplier upheld programming dialects and programming instruments, (for example, Java, Python, or. NET). The client doesn't deal with the fundamental cloud framework.

Table 1: Cloud Computing Models

Types	Amenities	Instances
IaaS	In this model is pay per utilize model, administrations like stockpiling, information base administration and register abilities are offered on request.	Tera, Go Grid, Amazon Web Services
PaaS	The stage used to configuration, create, assemble and test applications are given by the cloud foundation.	Azure service platform, Google App Engine
SaaS	Profoundly versatile web put together applications are facilitated with respect to the cloud and offered as administrations to the end client.	Google Docs, acrobat.com, Amazon Docs

Famous stages incorporate the Google App Engine (GAE) or Microsoft Windows Azure. This level requires making sure about the provisioned upholding security consistence, overseeing expected danger, and setting up trust among all cloud clients and suppliers.

2.1.3 Securing Software-as-a-service

Application facilitating is at times called as programming as an assistance. This administration utilizes program started application programming to serve a great many cloud clients, who make no forthright interest in workers or programming authorizing. From the supplier's viewpoint, costs are fairly low contrasted and regular application facilitating. Programming administration as intensely pushed by Google, Microsoft, Salesforce.com, etc.—necessitates that information be shielded from misfortune, twisting, or burglary. Conditional security and copyright consistence are intended to ensure all licensed innovation rights at this level. Information encryption and shading offer alternatives for maintaining information uprightness and client protection.

2.2 Security Issues

Cloud computing security issues recognized seven issues that should be tended to before undertakings consider changing to the distributed computing model. They are as per the following:

- Privileged client access - data sent from the customer through the Internet represents a specific level of danger, due to issues of information proprietorship; undertakings ought to invest energy becoming acquainted with their suppliers and their guidelines however much as could reasonably be expected before appointing some unimportant applications first to try things out.
- Regulatory consistence - customers are responsible for the security of their answer, as they can pick between suppliers that permit to be reviewed by outsider associations that check levels of security and suppliers that don't.
- Data area - relying upon gets, a few customers may never comprehend what nation or what purview their information is found.
- Data isolation - encoded data from numerous organizations might be put away on a similar hard plate, so a component to isolate information ought to be sent by the supplier.
- Recovery - each supplier ought to have a catastrophe recuperation convention to secure client information.
- Investigative help - if a customer presumes broken action from the supplier, it might not have numerous legitimate ways sought after an examination.
- Long-term feasibility - alludes to the capacity to withdraw an agreement and all information if the current supplier is purchased out by another firm.

The following table 2 consists of comparison of Cloud computing and Grid Computing.

Table 2: Comparison of Cloud Computing and Grid Computing

Characteristics	Cloud Computing	Grid Computing
Service oriented	Yes	Yes
Strong fault tolerant	Yes	Half
TCP/IP based	Yes	Half
High security	Half	Half
Loose coupling	Yes	Half
Virtualization	Yes	Half
Ease use	Yes	Half
Commercial pattern	Yes	No

Given that not everything of the above require to be improved relying upon the current application, it is as yet fundamental that agreement is reached on the issues with respect to normalization. The equivalent qualities of distributed computing and framework figuring are recorded in Table 2. The—yes‖ and—no‖ represent distributed

computing or framework registering has the unique trademark or not. The―half‖ implies not possessing the entire trademark partially. This paper doesn't give a lot of consideration on the similitudes and distinction among them and spotlights on the fundamental attributes of distributed computing [4]. The characteristic or saw danger of distributed computing is probably going to be the most limiting variable in its conceivable achievement. Danger can happen in regions of accessibility, protection, enactment, and information robbery and client security.

The interruption discovery framework meets two topics of necessities, for example, utilitarian and execution prerequisites [5].

The practical necessities are: IDS should consistently screen and report interruption; IDS ought to have a low bogus caution rate; IDS ought to give enough data to fix the framework on account of discovery of interruption. This trademark relies upon interruption recognition framework objectives.

Truth be told numerous interruption recognition framework arrangements center just around alarming managers without recommending any restorative activities. Interruption identification framework must recognize and respond to disseminated and composed assaults. This identification highlight is one of the most troublesome on the grounds that it needs immense appropriated measure of data notwithstanding the hard assignment of synchronization between various hosts.

The IDS should versatile to arrange geography and setup changes. The presentation prerequisites are: interruption ought to be recognized progressively as it ought to be accounted for quickly so as to limit network harm; the IDS must be versatile so as to deal with extra computational and correspondence loads.

The most well-known IDS impediments incorporate the accompanying: high number of bogus positives; absence of proficiency: typically when an IDS is confronted with an exceptionally enormous number of occasions in the organization, it hinders a framework or drops network bundles; weakness to assaults: various leveled structures, aggressors the chance to hurt the IDS by removing a control branch or even by attaching out the root order.

3. Problem Statement

3.1 IDS Based Cloud Computing

The Grid and Cloud Computing Intrusion Detection System coordinates information and conduct examination to recognize interruptions.

On account of their dispersed nature, network and distributed computing conditions are obvious objectives for gatecrashers searching for potential weaknesses to abuse. By mimicking authentic clients, the gatecrashers can utilize a help's bountiful assets vindictively.

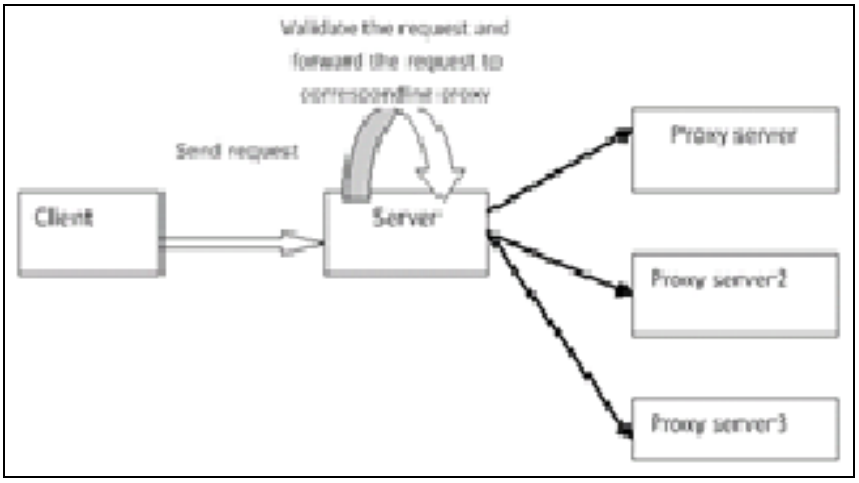

Fig 2: Client request with proxy server

To battle assailants, interruption identification frameworks (IDS) can offer extra safety efforts for these conditions by exploring designs, logs, network traffic, and client activities to recognize run of the mill assault conduct [1]. Be that as it may, IDS must be conveyed to work in a lattice and distributed computing condition. It must screen every hub and, when an assault happens, alert different hubs in nature. This sort of correspondence requires similarity between heterogeneous hosts, different correspondence instruments, and authorization command over framework support and updates—run of the mill highlights in network and cloud situations [6].

Cloud middleware for the most part gives these highlights, so we propose an IDS administration offered at the middleware layer (rather than the foundation or programming layers). An assault against a distributed computing framework can be quiet for an organization based IDS conveyed in its condition, since hub correspondence is normally encoded. Assaults can likewise be undetectable to have based IDS, since cloud-explicit assaults don't really leave follows in a hub's working framework, where the host-based IDS dwell. Thusly, customary IDS can't suitably recognize dubious exercises in a matrix and cloud condition [7]. The customer framework is the framework which needs to get administration or reaction from a worker by sending solicitation to the worker.

A mysterious intermediary fills in as a broker between your internet browser and an end worker. Rather than reaching the end worker straightforwardly to get a Web page, the program contacts the intermediary, which advances the solicitation on to the end worker. At the point when the end worker answers to the intermediary, the intermediary sends the answer on to the program. No immediate correspondence happens between the customer and the objective worker; hence it shows up as though the HTTP demand started from the moderate intermediary worker.

4. Implementation

4.1 Intrusion Detection System Methods

The Intrusion Detection System (IDS) administration expands a cloud's security level by giving two strategies for interruption recognition.

First methodology is execution approach which arranges how to contrast ongoing client activities with the standard conduct. The subsequent methodology is data approach that notification realized path left by assaults or certain arrangements of activities from a client who may speak to an assault.

The inspected information is sent to the IDS administration center, which examines the conduct utilizing man-made brainpower to identify deviations.

This has two subsystems specifically analyzer framework and ready framework.

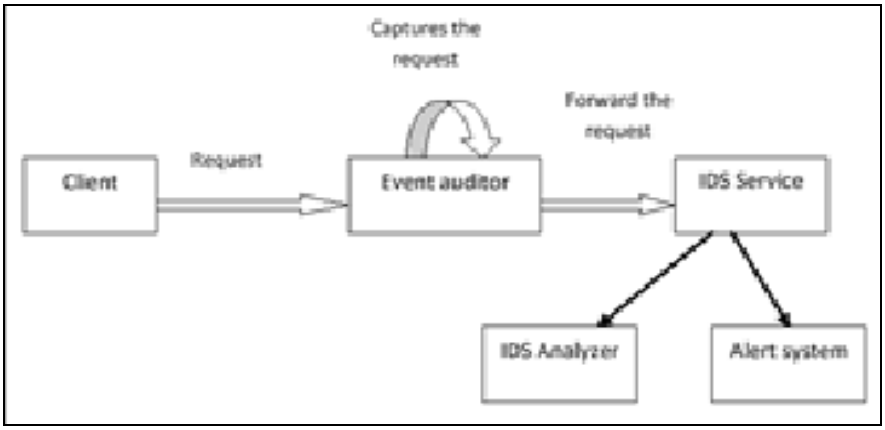

Fig 3: Client request with IDS Service

The analyzer utilizes a profile history information base to decide the separation between a run of the mill client conduct and the presume conduct and conveys this to the IDS administration. The guidelines analyzer gets review bundles and decides if a standard in the information base is being broken. It restores the outcome to the IDS administration center. With these reactions, the IDS ascertain the likelihood that the activity speaks to an assault and cautions different hubs if the likelihood is adequately high. This subsystem will work when interruption is identified. In the event that any hub among the cloud framework is influenced by interruption, at that point this ready framework will alarm the rest of the hubs about the interruption. This paper utilized review information from both a log framework and the correspondence framework to assess the data based framework. The made a progression of rules to outline security strategies that the IDS should screen. The data administration is only arrangement of rules which is framed from past assaults. Following things goes under this classification:

- Password breaking and access infringement,
- Trojan ponies,
- Interceptions most habitually connected with TCP/IP taking and interferences that frequently utilize extra instruments to bargain activity of assaulted frameworks (for instance by flooding) man in the center assaults.
- If any parcels accompany. exe expansion
- Packets containing worms

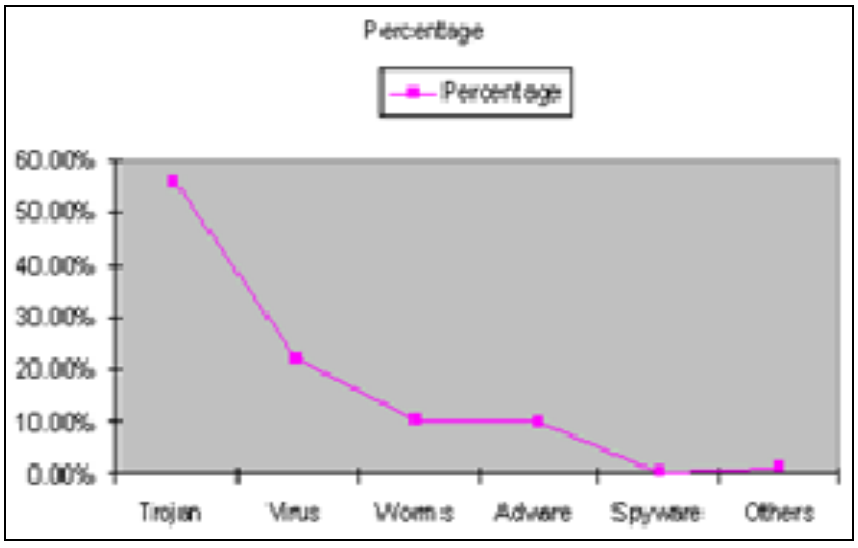

Fig 4: Recent Breakdown of the types of Malware program

In our answer, every hub recognizes neighborhood occasions that could speak to security infringement and cautions different hubs. Every individual interruption identification framework helpfully partakes in interruption discovery. The hub contains the assets, which are gotten to homogeneously through the middleware. The middleware sets the entrance control approaches and supports a help arranged condition. The administration gives its usefulness

in nature through the middleware, which encourages correspondence. The occasion reviewer is the key piece in the framework. It catches information from different sources, for example, the log framework, administration, and hub messages. The IDS administration breaks down this information and applies recognition procedures dependent on client conduct and information on past assaults. On the off chance that it recognizes an interruption, it utilizes the middleware's correspondence instruments to send alarms to different hubs. The middleware synchronizes the known-assaults and client conduct information bases. The capacity administration holds the information that the IDS administration must investigate. It's significant for all hubs to approach a similar information, so the middleware should straightforwardly make a virtualization of the homogeneous condition.

4.2 Intrusion Detection System services

The IDS administration builds a cloud's security level by applying two strategies for interruption location. The exhibition approach arranges how to contrast late client activities with the standard presentation. The data approach sees realized path left by assaults or certain successions of activities from a client who may speak to an assault.

The evaluated information is sent to the IDS administration center, which breaks down the exhibition utilizing man-made consciousness to identify deviations. The analyzer utilizes a profile history information base to decide the separation between an average client execution and the presume execution and imparts this to the IDS administration. The standards analyzer gets review bundles and decides if a standard in the information base is being broken. It restores the outcome to the IDS administration center. With these reactions, the IDS compute the likelihood that the activity speaks to an assault and alarms different hubs if the likelihood is adequately high. To recognize an interruption, need review information portraying the earth's state and the messages being traded. The occasion examiner can screen the information that the analyzers are getting to. The principal part screens message trade between hubs. In spite of the fact that review data about the correspondence between hubs is being caught, no organization information is considered just hub data. The subsequent segment screens the middleware logging framework. For each activity happening in a hub, a log section is made containing the activity's sort, (for example, blunder, caution, or cautioning), the occasion that created it, and the message. With this sort of information, it's conceivable to distinguish a continuous interruption.

4.2.1 Performance Approach

Performance approach is ordinary or expected execution extricated from reference data is contrasted and the current movement, any deviation watched, is identified as an interruption [8]. The upsides of utilizing execution approach are: recognize endeavors to misuse new and unexpected weaknesses and add to the programmed disclosure of new assaults; don't confront the speculation issue; they help distinguish maltreatment of benefits sorts of assaults that don't really include abusing any mechanical weakness.

The weaknesses of utilizing execution approach are: high bogus caution rate; intermittent internet retraining of the presentation profile is required which results in the either inaccessibility of the interruption discovery framework or the extra bogus alerts. Various strategies exist for execution based interruption location, for example, information mining, counterfeit neural organizations, and fake immunological frameworks. This paper utilize a feed-forward counterfeit neural organization, in light of the fact that—rather than customary strategies—this kind of organization can rapidly handle data, makes them learn abilities, and can endure little execution deviations. These highlights help beat a few IDS impediments [9]. Using this strategy, need to perceive anticipated execution (real use) or a serious exhibition deviation. Preparing assumes a key part in the example acknowledgment that feed-forward organizations perform. The organization must be accurately prepared to productively identify interruptions. For a given interruption test set, the organization figures out how to distinguish the interruptions utilizing its retro spread calculation. Nonetheless, center on recognizing client execution examples and deviations from such examples. With this procedure, spread a more extensive scope of obscure assaults.

4.2.2 Information Approach

Information approach contains data about explicit assaults and weaknesses and searches for endeavors to abuse these weaknesses. At the point when such an endeavor is recognized, a caution is set off. Precision relies upon the standard update of data about assaults [8]. The benefits of utilizing data approach are: the potential for low bogus alert rates; logical investigation proposed by the interruption location framework is itemized, making it simpler to make preventive or remedial move.

Data based interruption location is the regularly applied strategy in the field since it brings about a low bogus caution rate and high certain rates, despite the fact that it can't recognize obscure assault designs. It utilizes rules (likewise called marks) and screens a flood of occasions to discover noxious qualities. Utilizing a specialist framework, portray a malignant conduct with a standard. One bit of leeway of utilizing this sort of interruption recognition is that include new principles without adjusting existing ones.

4.2.3 Increasing Attack Exposure

The two interruption discovery strategies are particular. The presentation approach interruption recognition is portrayed by a high hit pace of known assaults, yet it's insufficient in distinguishing new assaults. Consequently, the supplemented it with the exhibition strategy, which can find deviations from worthy use and hence help recognize benefit misuse.

Quick increment in the quantity of weaknesses has brought about an exponential ascent in the quantity of assaults. As indicated by the Computer Emergency Response Team (CERT), the quantity of weaknesses in programming has been expanding and a large number of them exist in profoundly conveyed programming [10, 11]. Taking into account that it is close to difficult to manufacture _perfect' programming, it gets basic to fabricate compelling interruption identification frameworks which can identify assaults dependably. The possibility of getting significant data, because of a fruitful assault, die down the danger of lawful feelings. The failure to forestall assaults advances the requirement for interruption recognition. The issue turns out to be more significant since approved clients can abuse their benefits and aggressors can take on the appearance of valid

clients by misusing weak applications. The volume of information in a distributed computing condition can be high, so overseers don't watch every client's activities they watch just alarms from the IDS.

4.3 Experimental Analysis

In testing our model, it has a low preparing cost while as yet giving an acceptable presentation to ongoing usage. Sending information to different hubs for handling didn't appear to be vital. The individual investigation acted in every hub decreases the unpredictability and the volume of information in contrast with past arrangements, where the review information is amassed in single focuses. Later on, execute our IDS, assisting with improving environmentally friendly power (vitality productive), white (utilizing remote organizations), and intellectual (utilizing psychological organizations) distributed computing situations. And furthermore mean to investigate and improve distributed computing security.

The occasion examiner catches all solicitations got by a hub and the relating reactions, which is key for execution approach. For each activity a hub plays out, a log passage is created to enlist the techniques and boundaries summoned during the activity. In the examinations with the presentation-based IDS, considered utilizing review information from both a log and a correspondence framework. Tragically, information from a log framework except for the message component has a restricted arrangement of qualities with little variety. This made it hard to track down assault designs, so selected to investigate correspondence components to assess this procedure.

In the Evaluated exhibition strategy utilizing computerized reasoning empowered by a feed forward neural organization [12]. Expanding the example time frame for the learning stage improved the outcomes.

4.4 Evaluating the performance Approach

To quantify IDS productivity [13] thought about exactness as far as the framework's capacity to distinguish assaults and dodge bogus alerts. A framework is defective in the event that it blames an authentic activity for being malignant. Thus, estimated exactness utilizing the quantity of bogus positives (genuine activities set apart as assaults) and bogus negatives (the nonattendance of a ready when an assault has happened).

Inconsistency recognition models work by building a model of framework execution dependent on the standard activity of the organization or segment under perception. After this model of \normal framework execution has been made, current action is contrasted with it. At the point when the deviation becomes more prominent than an edge level, an alarm is set off [14]. Such a framework has the benefit of having the option to identify assaults that are not as of now known. The disadvantage of such frameworks is that they regularly have a high bogus positive rate, which can prompt an absence of trust in the product.

The exhibition test planned likewise assessed the examination strategy's expense. It outperforms the typical information volume and filled in as a base for understanding framework execution in an over-burdening condition. The preparation was irregular to design updates to the exhibition profile information base as per an everyday practice in the execution condition (since a client's conduct will in general change with time). This helped us recognize an advantageous time of days for deciding the profile of a real client. Fake neural organizations aren't deterministic, so the quantity of bogus positives and bogus negatives didn't speak to a straight diminishing movement. The neural organization would in general abstain from recognizing authentic activities as assaults there were in every case more bogus negatives than bogus positives when utilizing a similar amount of information.

No bogus cautions happened during the preparation with recreation periods, in spite of the fact that the vulnerability level was still high, with a few yields close to zero. The calculation indicated a low number of bogus positives, however after a few redundancies, the amount of bogus positives shifted, again speaking to the nondeterministic idea of neural organizations.

4.5 Evaluating the Information Approach

As opposed to the presentation approach, utilized review information from both a log framework and the correspondence framework to assess the data based framework. The made a progression of rules to outline security arrangements that the IDS should screen. Gathered review information alluding to a course disclosure administration, administration revelation and administration solicitation and reaction. The arrangement of approaches made tried the framework's presentation, despite the fact that our extension did exclude finding new sorts of assaults or making an assault information base.

Our objective was to assess our answer's usefulness and the model's exhibition. The standard underneath portrays an assault in any message identified with the capacity administration. The elements of the standard are as per the following:

- At fire up, the standards put away in a XML record are stacked into an information structure.
- The reviewer begins to catch information from the log and correspondence frameworks.
- The information is preprocessed to make an information structure partitioning log information from correspondence information to give simple admittance to every component.
- The relating strategy for the review bundle is checked.
- An alarm is created if an assault or infringement happened.

A few procedures have been created to sidestep location of an assault by interruption discovery frameworks. Organization based instruments, the most famous apparatuses today, especially experience the ill effects of these assaults including hand-made organization parcels: Attack by IP discontinuity interruption recognition frameworks experience issues reassembling IP bundles. Consequently, parting an assault misleadingly into various bundles makes confuse between the information in the parcel and the mark, in this way concealing the assault.

Assault by means of the TTL (Time to Live). By changing the TTL of IP bundles, it is conceivable to make the interruption recognition framework see parcels that won't show up at the objective of the assault. By embedding counterfeit information into the correspondence stream, an aggressor can interleave the assault with sham data, accordingly concealing the assault from the interruption identification framework while the objective effectively reproduces this assault information and responds to it.

Interruption identification frameworks are starting to shield themselves from these assaults, however little data is delivered by sellers with respect to the viability of these insurance measures. It is frequently hard to attest the arrangement of an interruption recognition framework, as a rule there is no simple method to check the design and the best possible discovery of the assaults.

Later on, actualize our IDS, assisting with improving environmentally friendly power (vitality productive), white (utilizing remote organizations), and psychological (utilizing intellectual organizations) distributed computing conditions. And furthermore, expect to investigate and improve distributed computing security.

5. Conclusion

Interruption recognition as of now draws in impressive enthusiasm from both the examination network and business organizations. This paper is giving an agreeable presentation to ongoing usage. In this framework execute a best healing method to conquer the disadvantages in the current cloud and matrix framework. The individual investigation acted in every hub decreases the unpredictability and the volume of information in contrast with past arrangements, where the review information is amassed in single focuses. This methodology speeds up which meets the prerequisites of organization correspondence. It improves the intelligent presentation of interruption location framework for upgrading the security of the entire framework. It is moderately minimal effort. Later on, actualize our interruption identification framework, assisting with improving vitality effective, utilizing remote organizations, and utilizing psychological organizations distributed computing conditions. We likewise mean to investigate and improve distributed computing security.

6. Acknowledgments

The authors are thankful to Dr. C. Chandrasekar, Mrs. M. Rekha and Zaim, KG. Khan Ceylan for providing the necessary facilities for the preparation of the paper. Also thanks to IJASR Journal staffs to publish this paper.

7. References

1. Ali M, Aydin Halim A, Zaim khan KG. Ceylan. "A hybrid intrusion detection system design for computer network security," Computers and Electrical Engineering, 2009, 517-526.
2. National Institute of Standards and Technology (NIST) Definition of Cloud Computing, http://csrc.nist.gov/g r oups/SNS/cloud-computing/.
3. Abdoul Karim Ganame, Julien Bourgeois, Renaud Bidou, Francois Spies. "A global security architecture for intrusion detection on computer networks", computers & security, 2008, 30-47.
4. “Authentication and Privacy”, by Thomas M. Chen Department of Electrical Engineering, Southern Methodist University, Dallas, Texas, USA and Nhut Nguyen Network Systems Lab, Samsung Telecommunications America, Richardson, Texas, USA, 2018.
5. “Analysis on Mobile WiMAX Security”, by Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu, Department of Systems and Computer Engineering Carleton University, Canada and Anand Srinivasan EION Inc. Canada.
6. “Security Enhancement and Solution for Authentication Frame work in IEEE 802.16”, by AKM. NAZMUS SAKIB, Chittagong University of Engineering & Technology, 2019.
7. “Formal Analysis of the Handover Schemes in Mobile WiMAX Networks”, by Ahmed M. Taha, Amr T. Abdel-Hamid, and Sofiene Tahar, Faculty of Information Engineering and Technology German University in Cairo (GUC), Cairo, Egypt, 2018.
8. David Fick, Andrew DeOrio, Gregory Chen, Valeria Bertacco, Dennis Sylvester, David Blaauw, *et al.* “A Highly Resilient Routing Algorithm for Fault Tolerant No Cs”, Design, Automation & Test in Europe Conference, 2019.
9. “Trust based authentication technique for security in WiMAX networks”, by Mrs. M. Rekha and Dr. C. Chandrasekar, Department of computer science, 2017.
10. “Security Issues of IEEE 802.16 (WiMAX)”, by Jamshed Hasan, School of Computer and Information Science, Edith Cowan University, Australia, 2018.
11. “SPIN-based Verification of Authentication Protocols in WiMAX Networks”, by Beth N. Komu, Mjumo Mzyece and Karim Djouani, 2017.
12. “Enhancing Security Using the Discarded Security Information in Mobile WiMAX Networks”, by Youngwook Kim and Saewoong Bahk, School of Electrical Engineering and Computer Science, INMC.
13. “An Enhanced Authentication Mechanism for IEEE 802.16(e) Mobile WiMAX”, by Deepak Kumar Mehto, and Rajesh Srivastava, 2018.
14. “Mobile WiMAX Network Security”, by Rainer Falk, Christian Gunther, Dirk Kroselberg, and Avi Lior, Siemens Corporate Technology, 2018.