GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

CLIENT-BASED SECURITY IMPROVEMENT FOR USING IDENTICAL IP ANALYSIS AND REDUCE PHISHING ATTACKS IN CYBER SECURITY

Dr. Raju Rameshkumar*[1], B.Satishkumar[2], B.Ganesh[3] & G.Hymavathi[4]
[*1]Prof. in CSE and Dean R&D, Lendi Institute of Engg.& Tech., VZM,
[2]Asso.Prof. in CSE, Lendi Institute of Engg.& Tech.,VZM,
[3]Asso.Prof. in CSE, Sri VenkateswaraEngg. College, SKLM,
[4]Asst.Prof. in CSE, Lendi Institute of Engg.& Tech.,VZM

ABSTRACT

The phishing attack is maybe the most customarily announced type of cyber-attack, There are different sorts of phishing attacks, and the kind that is utilized as a rule relies upon the business whether it's close to home passwords, firewall or deficiency in that department, or unpatched status security programming. In this proposed system introduce for phishing attacks used to Identical IP Analysis For Reduce Phishing Attacks**(**IIPA) this technic provided Single device equal for same ID access the cloud data in every time, In this technic mostly used to personal data or based on the industries details maintains purpose.It naturally isolates the info information into three parts with various significance levels and scattered them into various storage room which gives an extra layer of security than the sole encryption. This plan empowers stockpiling administration in term of cost-viability by utilizing open cloud and delivering with a consistent level of assurance in the meantime. We have concentrated on the appropriated check convention to insurance the information stockpiling security in distributed computing. This paper presents the application field the value of distributed computing, for example, to decrease the clients' phishing assault. It gives a safe and tried and true information stockpiling focus.

Keywords: *Phishing Attacks, Identical IP Analysis, Data Fragments.*

I. INTRODUCTION

The correspondence systems and the advancements in social web and portable advances have prompted a mind-boggling development of the Internet. Cyberspace has been reshaping the manner in which individuals convey, learn, and work, giving quick and savvy business openings. The fast development of the cyberspace additionally prompts open doors for vindictive plans and multiplication of cyber-attacks. Previously, cyber dangers have progressively advanced from straightforward.

Also, significant attacks on modern ones, for example, multi-arrange staged attacks focusing on business tasks, physical resources, and necessary frameworks. Consequently, there is a critical requirement for dynamic risk checking and discovery frameworks, which can avert and battle these dangers. To address these issues, organize security circumstance mindfulness is perceived as a promising innovation, which can improve the security of big business arranges in portraying, observing, identifying, and moderating cyber dangers expeditiously. As a rule, the circumstance mindfulness is characterized as an innovation to screen arrange exercises for security and guard reason. With regards to the endeavor arrange, cybersecurity circumstance mindfulness plans to give essential data on big business organize activities for necessary leadership forms, secure against penetration and control of information, guarantee venture organizes flexibility and guard against cyber dangers.

In any case, there is an expanding number of end client implementation appropriated in the undertaking system and a lot of information stream gathered from various applications, working frameworks, and system gear for the cybersecurity examination. Productively putting away and preparing such substantial scale stream information is a testing issue. Cybersecurity applications, for example, arrange to observe, organize investigation, arrange extortion and interruption recognition are portrayed by high volume information streams (colossal information) and constant handling necessities. Consequently, the expanding volume of information put away in focal databases and the upper calculation control prerequisite can seriously upset the adequacy of cybersecurity circumstance mindfulness.

To address the difficulties said above, we propose a distributed computing based engineering to help cybersecurity circumstance mindfulness, which offers plenteous capacity, adaptable organization, more calculation assets, more affordable framework venture, and universal sharing of data over all individuals from the cloud. Our proposed framework engineering comprises of four primary parts: information sources, cloud foundation, Map Reduce, and activity focus. We use the cloud framework to build up a financially savvy information stream stockpiling. By utilizing Map Reduce-based information preparing, we enhance information storing productivity, accelerate access to information, and take out operational postponements. Furthermore, we consider a parallel cloud-based risk discovery that coordinates both mark based and irregularity based recognition methods. To decide the attributes related with attacks, we propose the attack scene examination in both strategic and spatial areas to give the essential data to the human examiner, for example, attack purpose, practices and plans to picture the recognized attack data. To approve the viability of our proposed engineering, we show a proving ground set up and the work process of framework usage.

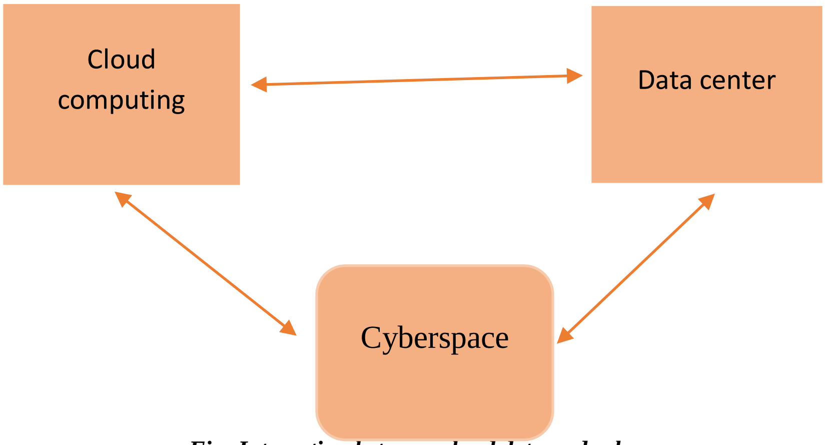


Fig: Interaction between cloud data and cyberspace

Cyber-Security Cloud

As shown by the National Institute of Standards and Technology (NIST), conveyed registering is described as a model for engaging all-inclusive, invaluable, on-task for mastermind access to a shared pool of configurable figuring resources that can be immediately provisioned and released with unimportant organization effort or authority community affiliation. This cloud indicate is made out of five fundamental traits (on-request self-benefit, extensive system get to, asset pooling, fast flexibility, estimated benefit), three administration models (programming as an administration, stage as an administration, framework as an administration), and four sending models (private cloud, network cloud, open cloud, crossbreed cloud)." In this paper, we center on the issue of building a particular kind of haziness, one that is committed to the discovery of cyber-security attacks. Our shadow will take after a stage as an administration demonstrate whereby the purchaser will have control over the sent cyber-security applications and their setup, and it will offer help for any of the four arrangement models. We will utilize the term cyber-security cloud or CSC to allude to this sort of darkness.

II. RELATED WORKS

The power framework is one of the essential modern control frameworks in the present society. To ideally incorporate frames and diminish costs, heaps of cutting-edge data advancements are associated with control frameworks. Current power frameworks are presently presenting to people in the general system, and data security is turning into another danger to versatility. In this process, we investigate the reasonableness of troupe learning strategies as a method for recognizing power framework cyber-attack [1]. Web keeping money has turned out to be one of the quickest and least complicated techniques for managing an account. We initially break down in brief instruction thecyber security of online transaction in three developing nations then after that methods to diminish the cyber security hazard to cross over any barrier amongst banks and clients. The proposed display depends on the consequences of reviews led on Internet managing an account in some of countries. The examination concentrated on clients' practices in Internet saving money [2].

Transportation-based Cyber-Physical Systems as one of the critical services in Real-time route guidance schemes, have been introduced to data transmission optimal routing with low traffic congestion and travel time. We first inspect security issues of route guidance schemes via modeling and analysis of data reliability attacks on the route guidance process, and then develop similar mitigation mechanisms to combat the investigated assault [3]. The article is devoted to the improvement of neural network technologies for detection of cyber-attacks of the "denial of service" type. It is suggested to increase the adaptation due to the application of the target function of optimizing the values of the weight coefficients in the form of a quadratic reduced learning error. This target function is integrated into the mathematical apparatus used to train the multilayer perceptron. The suitability of the developed solutions is confirmed experimentally [4].

To guarantee computerized security of a meander, classically, Security Information and Event Management framework is set up to systematize instancessecurity from various preventive advances and banner cautions. We build up a client driven machine learning structure for the computerized security development revolve around the satisfied undertaking condition. We examine the normal information sources in their execute strategy, and execution steps following information aggregations to implemented machine understandingconfiguration [5], A sorted out mechanism structure under both computerized and real component strikes is measured. An adjustedsignificance of the issue basedcarnal ambushes, information double dealing, and false information blend strikes are utilized for controller blend. In perspective of the extraordinary blame tolerant disclosure (FTD) mechanical congregations, a leftover generator for strike/blame ID in light for followed by the system. An occasion started, and BMI(Bilinear Matrix Inequality) execution is proposed to accomplish better security method [6].Cyber-physical system is analyzed from the security perspective. A double closed-loop security control structure and algorithm with defense functions are proposed. From this structure, the features of several cyber-attacks are considered respectively. By this structure, the models of information disclosure, denial-of-service (DoS) and Man-in-the-Middle Attack (MITM) are proposed. According to each kind attack, different models are obtained and analyzed, then reduce to the unified models [7].

DNS is server portrayed utilizing usual technic to lessen DNS liabilities to advanced ambushes. We emerged Open-source Domain Name System include in Windows DNS, and unmistakable DNS main system on the two operating system GUI and CUI based all operating system supported. Our outcomes show Open-source Domain Name System performs phenomenally differentiated and unmistakable DNS main system, dual restrictive and public-source, especially assign the advantages used in its change [8].Cyber security data sharing is enhancing digital occurrence recognition and counteractive action by decreasing the misfortune caused by assaults and taking out the expenses of duplication endeavors for digital guard. We propose a novel mechanism which consists of four components Registration, Sharing, Dispute, and Rewarding. Our device enables the organizations to share their cyber security information without revealing their identities. Security analysis and performance evaluation are conducted showing the effectiveness and efficiency of the proposed invention [9].

Cyber-Physical Systems (CPS) speak to a key connection between data innovation (IT) systems and the implementation that control the mechanical creation and keep up essential framework benefits that help our cutting-edge world. These techniques are suitable result find to close honesty and privacy holes in Cyber-Physical Systems and procedures to feature the security chances that remain. This are technic additionally diagrams ways to deal with decrease the overhead and multifaceted nature of security techniques, and look at novel methodologies, including secret correspondences channels, to expand Cyber-Physical Systems security [10]. Current motorized control systems and other complex cyber-physical systems, for example, shrewd network, unscrewed vehicles, artificial plants, and atomic reactors are perplexing consistent systems with broad cyber and physical parts, requiring hearty cyber-security procedures. By adjusting the data stream or the computational conduct of the framework, processmindful occurrences can disturb the working of the CPS to in this way hamper the execution or dependability of the general structure or its segments [11].

Industrial Control Systems (ICS) are fundamental for nations' shrewd frameworks and basic foundations. Notwithstanding the favorable circumstances, for example, controlling and observing topographically conveyed structures, expanding profitability and proficiency, ICS has brought some security issues. Particular arrangements should have been delivered some unsecure problem occur. The maximum critical data safety part for Industrial Control Systems is accessibility, and the most pulverizing risk to this segment is DoS attack. [12]. Scientific classifications have been created as a component for cyber-attack order. In any case, when one thinks about the ongoing and fast advancement of attacker strategies and focuses on, the pertinence and adequacy of these scientific categorizations ought to be addressed. This systemassigned two ways to deal with the assessment of seven scientific classifications. The primary utilizes a basis set, inferred through investigation in previous method is essential segments to the formation of scientific categorizations are characterized. A another one method is assigned chronicled attack information to every scientific classification based audit, all the more particularly, attacks manufacturing maintained system have been focused on [13].

Late advances in unavoidable processing have produced a fast development of the Smart Household market, where some generally ordinary bits of innovation are equipped for associating with the Internet and communicating with other comparable implementation. Notwithstanding, with the absence of a usually received arrangement of rules, a few IT organizations are creating shrewd devices with their exclusive principles, prompting exceptionally complex Smart Home systems in which the interoperability of the present components isn't generally actualized generally distinctly. In that capacity, sympathetic the replicated danger of these cyber-physical systems past the separate implementation has turned into a relatively unmanageable issue. This paper handles this issue by presenting a Smart Home orientation design which encourages security investigation [14]. The regularly developing number of cyber-attacks in the course of the most recent couple of years has put the two people, and additionally large-scale associations, in a highly sensitive situation circumstance. At the beginning of a Big Data Internet-of-Things old-fashioned, the revelation and utilization of individual data for singular profiling raise critical data security concerns, testing controllers around the world. As portable amplifiers are regularly the best remedial measure for a person with hearing misfortune, the quantity of dynamic implementsmaybe cyber management and utilized for vindictive whys and wherefores proposes. The ID of probable pony-trekking and cyber-attacking approaches went for these implementation and the requirement for conceivable countermeasures and moves to be made all the additional genuinely to assurance patients' protection [15].

Workers of all little, medium or venture associations kind utilization of copiers, copiers, scanners and multi-functional implementation for everyday operational elements of the association. These implementation are either out-properly bought or got on a rent convention. At the point implement's End-of-Life is achieved, the devices are any discarded, at times over gifts to not benefit associations or returned to the Original Apparatus Manufacturer toward the finish of a rent assertion convention. Obscure to mainlyinformation technology tasks faculty and data security workforce, these implements convey a natural weakness. These implementation have secure and insecure organize interchanges conventions; hard plate drives; unstable memory; and non-unpredictable memory. This paper closes with rules on the most proficient method to securely utilize and decommission such implementation to go around the loss of delicate data [16].

The usage of interruption recognition for cyber security for quite a while been a fundamental research subject ([17], [18], the essentialness of mapping covers malignant has in like manner been included [19], and these methodologies said above may even now make them challenge issues to be settled. For instance, the parcel substance and stream attributes can be effectively changed to keep away from the discovery by the framework. Further, the malware projects can be effortlessly altered or adapted to modify the stream attributes through the use of various sizes of bundles and the alteration of parcel transmission speed every second amid correspondence. Once the parcel substance is changed by including additional, pointless characters, the strategy because of bundle movement highlights must be enhanced further to learn new element designs, and, therefore, the trouble of breaking down and considering the encoded bundles will be multiplied. Likewise, clients have turned out to be progressively more worried about their security and may not permit the bundle substance including a lot of their data to be gotten explicitly to by others [20].

III. METHODS AND IMPLEMENTATIONS

In the venture organize, and a lot of information stream gathered from various applications, working systems, and system gear for the cyber security investigation. Proficiently putting away and preparing such colossal scale stream information is a testing issue. High volume information describes cyber security applications, for example, arrange to check, organize investigation, and arrange misrepresentation and interruption recognition streams cloud information and ongoing handling necessities. Thus, the expanding volume of details put in database and accurate mathematical control prerequisite can extremely impede the viability of cyber security.

The fundamental supposition is the private section of information is put away nearby which is an end client's PC and is measured as secure. So in this area, just the ensured and open part will be examined with various tests to demonstrate its abnormal state of irregularity which keeps any conceivable recuperation from it. In our trials, a 32 KB, English content record, encoded with ASCII coding is utilized for instance to demonstrate the entire assurance process. For the outcomes, the secured L2 and L3 sections have related factual assets so just investigation consequences for the L3 piece in this framework.

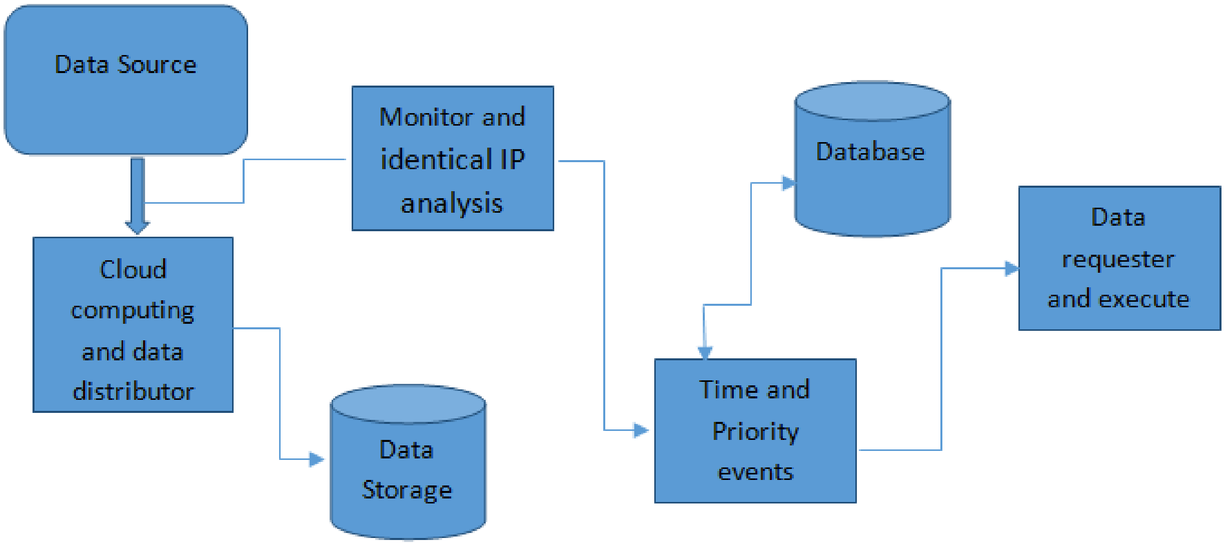

Data Source
Monitor and identical IP analysis
Database
Data requester and execute
Cloud computing and data distributor
Time and Priority events
Data Storage

Fig: Identical IP Analysis and Reduce Phishing Attacks

Danger Detection

To address the testing issue of recognizing dangers through an expansive number of information streams, we research the cloud-based risk recognition utilizing parallel figuring strategies. For instance, signature-construct danger discovery depends in light of an arrangement of tenets that are being used to coordinate bundles. Guidelines can be used for speak to attributes of referred to attacks, for example, the convention composes, port number, parcel estimate, bundle content (the two strings and standard articulations), and the situation of the suspicious substance. Both mark based discovery and abnormality based recognition will be incorporated to look at framework logs, arrangements methodically, and activity logs put away in the cloud. Flooding attacks are gifted by communicating a group of bundles, for the most part, the ping parcels. The thought is to send a lot of information to the casualty. In the meantime with the goal that the casualty backs off so much and gets separated on account of timeouts. Surge attacks endeavor to fill a system by sending a nonstop arrangement of reverberating asks for over a high-transfer speed association with an objective host on a lower-data transmission association. The recipient must post back a reverberate answer for every application. The CMS will distinguish these attacks and creates principles to keep the offense, and these standards are conveyed to the system and criticisms are assessed. From that point onward, the invalid arrangements are killed, and the new guidelines are distributed to the framework. At whatever point the attacks are identified, these procedures are rehashed.

Phishing Attack Prevention

Phishing attack prevention is online attacks this are the attacks compare to anotherattack very difficult and affected website, for example, online base managing account security code and change security code from the user card. A full phishing attack includes three parts of phishers. Right off the bat, mailers convey many messages (more often than not through botnet), which guide clients to fake sites. Also, authorities set up deceitful destinations (customarily facilitated on bargained machines), which effectively provoke clients to give secret data. At last, cashers utilize the private data to accomplish a compensation out. Cash trades frequently happen between those phishers. Distributed computing stage was being used for disconnected phishing attack proper examination. In the first place, our CNSMS gathered the system follow information and answered to the security focus. At that point, the security focus disperses the security principles to every hub in the system. All phishing separating activities depended on distributed computing stages and keep running in parallel with a gap and overcome plot.

Security Center

The necessary capacity in the security focus is the legal examination of the gathered movement and system security issues. The cloud-based security focus is utilized to store an expansive volume of movement information of various roots and led information examination to produce new security manage sets. It makes security rules for implementation in the UTM to stifle the correspondence amongst bots and bot ace. The most crucial element of this framework is its shut circle control qualities, i.e., gathering the input occasions coming about because of the conveyed standards, preparing and examining in control hubs, expelling wrong directions to make the framework more proficient and stable and the tenets are redistributed.

Algorithm:

```
Start
 Initialize process Np
 Node placed Ns.
 For (Data source)-$D_s$from(Data destination) -$D_d$
ValueT = Decrypted values fromData source-Ds.
For Number of nodeN
            Start communication route path
For path Cs from Cd
If Cs€through data
 Each data transferred
 Else
Discover route direction fromattribute table
 End
                       End
For each security code k
Generate source nodesecurity code Sk.
New node placed in network to Nn.
                End.
               For interchange source node security code
For security codethroughKh
If Kh€ then
Find the suitablesecurity codes.
Base Station Guide for data travelling to reach destination
 End
End
            End
```

Ds-data source, Dd-Destination data, Cs-communication source, Cd-communication destination. Above the algorithm is find out correct destination identified and delivery the data and include the security for encryption key generation and the target is found same packet key find and decrypted data in the mark. Huge segments of Cloud Service Subscription Information are the cloud asset rundown, and information get to control approach and character data. An Administrator needs to keep up the rundown of cloud assets to which its association buys in, which incorporates information, applications, equipment, and administrations. The menu is data that might be imparted to the next inside associations. By actualizing cyber security data distinguished in this level, quality digital security tasks in distributed computing is a dicey situation. We recognized three main considerations that influence cyber security data in distributed computing: information resource decoupling, a creation of different assets and outside asset utilization.

IV. RESULT AND DISCUSSION

The proposed Data Alternative CirculationPattern Analysis (DACPA) algorithm basedintrusion detection system cyber securitynetwork has been performed and examinedfor its efficiency. Intrusion detection hasbeen achieved in network simulator NS2.28 version under various scenarios. The conduct of the recommended approaches is dissected with an assortment of recreation parameters. A hub can straightforwardly identify with the centers that exist in its transmission go. On the off chance that a center needs to connect with a hub that isn't instantly inside its conveyance extend, it utilizes the middle of the road hubs as switches. In the portability demonstrate, the development of a center from an area to another area can be empowered using the watchword goal in Tool Command Language (TCL) content. Our proposed framework is contrasted and existing systems; they are Cyber Threat Intelligence (CTI).

Phishing Attack Detection Accuracy

Phishing detection is found out for comparison to DACPA protocols to proposed protocols improve the accuracy detection for IIPA defined below show in the graph

$$Attack\ detection\ accuracy = \left(\frac{Ep + Pp}{no\ of\ packets}\right) X100$$

Here Ed-existing positive, Pd – proposed positive.

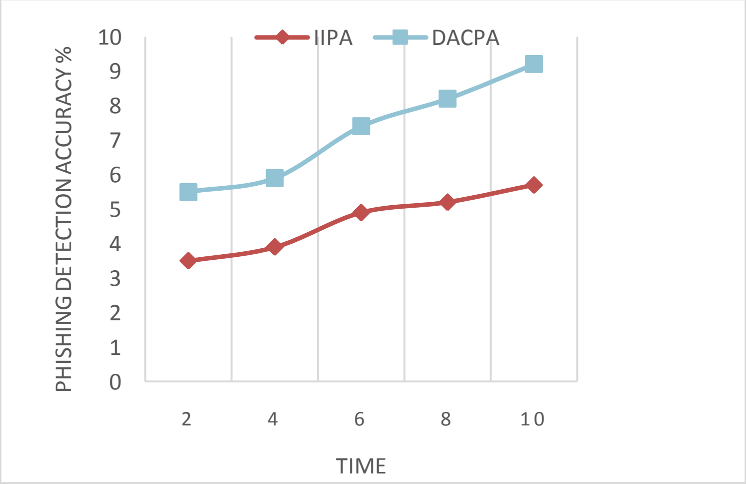


Fig: Detection Accuracy Ratio

False Detection Ratio

Identical IP Analysis for Reduce Phishing Attacks **(**IIPA) used to false detection is to reduce compare to DACPA protocols provide the result for below show in the graph. In this graph is declare Time is mille seconds and false detection is Ratio divisible of proposed and existing system following formula.

False Detection $=\frac{Ep}{Pp}X100$;

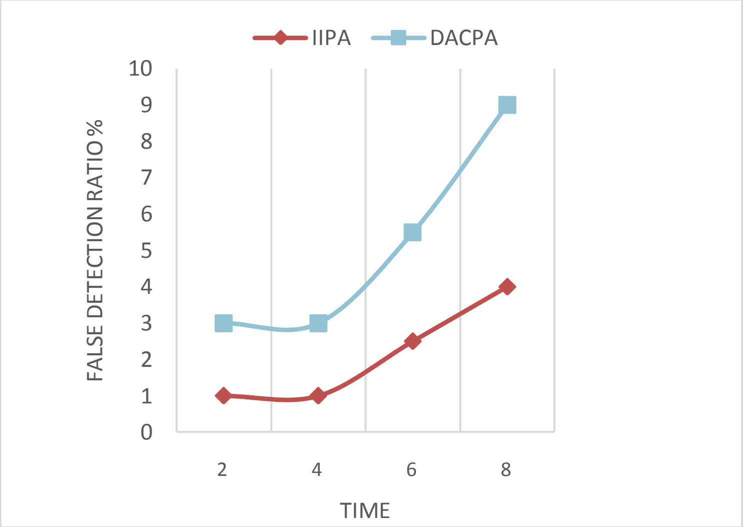
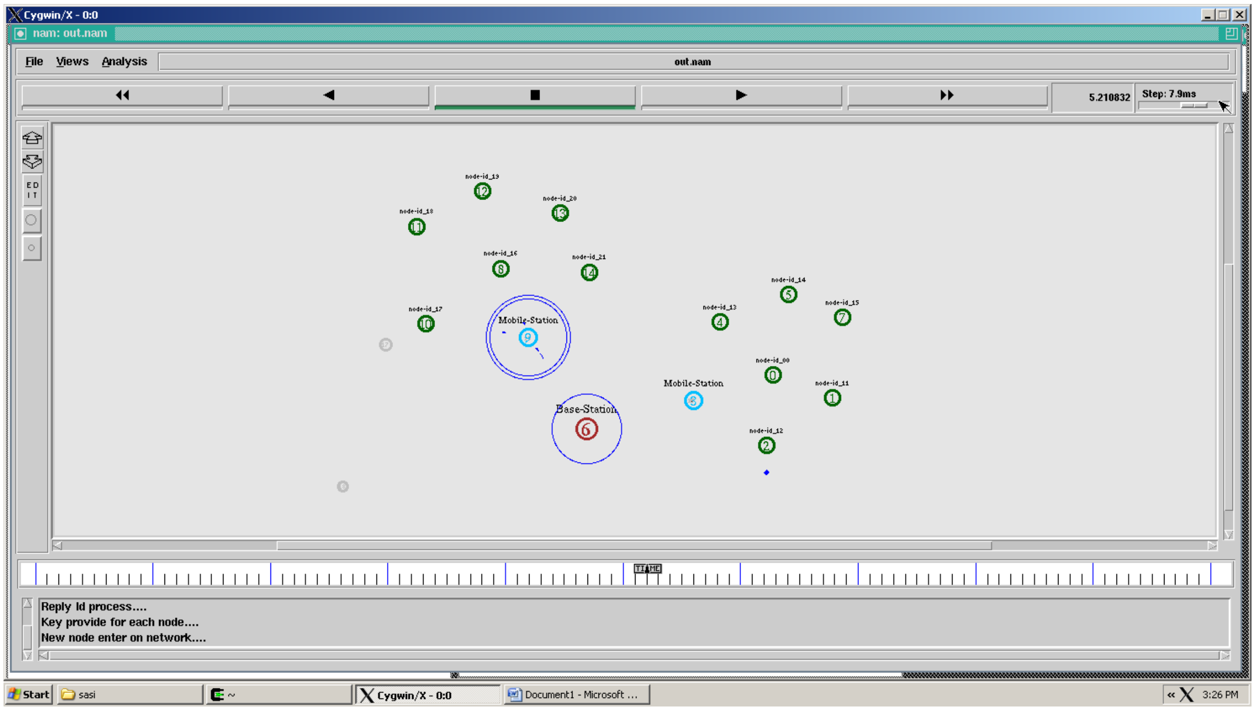


Fig: False detection ratio

Throughput performance

Each area in the progressive multicast system reports its information to the sink along the multicast chain of importance, and any in the middle of information can total information ordinary from its locale. The arranged Geocast locale first finds a course since the sink hub to the region utilizing vitality useful calculation in NTB-GRT and inside the Geocast area constructs a multicast progression by methods for another vitality proficient telecom system. In this way, the vitality utilization is concentrated amid the locale following stage. At the point when information is gathered and depicted in the district, the data is conveyed along the multicast tree.



```
Reply Id process....
Key provide for each node....
New node enter on network....
```

Amid the information conveyance, all objective area can work as an information collection point. Along these lines, the consequent multicast tree misuses the in-organize information accumulation between Geocast hubs and diminishes vitality utilization amid the objective area information revealing stage.

Algorithm:

```
Initialize Network ProvinceNp.
Get Target Province Tp.
Discover starting Province, neighbor Province
 For neighbor Province$N_p$
DecryptrecordsNl = $\int_1^{province\ (L)} L \times Np$
DecryptdataProvincepresent in Nl.
 NR = Ω(Nl).
              For route direction p from Nr
Make network communicationspeed NCS-GRT = $\int(Np$ ∗objectiveProvince)/Np
NCS(j) = NCS(j)+Tp.
              End.
         End.
          For Time window $T_i$
If NCS($T_i$)>Starting point
Allegation = False
SelectProvinceas malicious node Province.
New node assignedID to wickednode table information. Ml = ΣProvince(Ml)+Tp.
                   End
                End.
   Stop
```

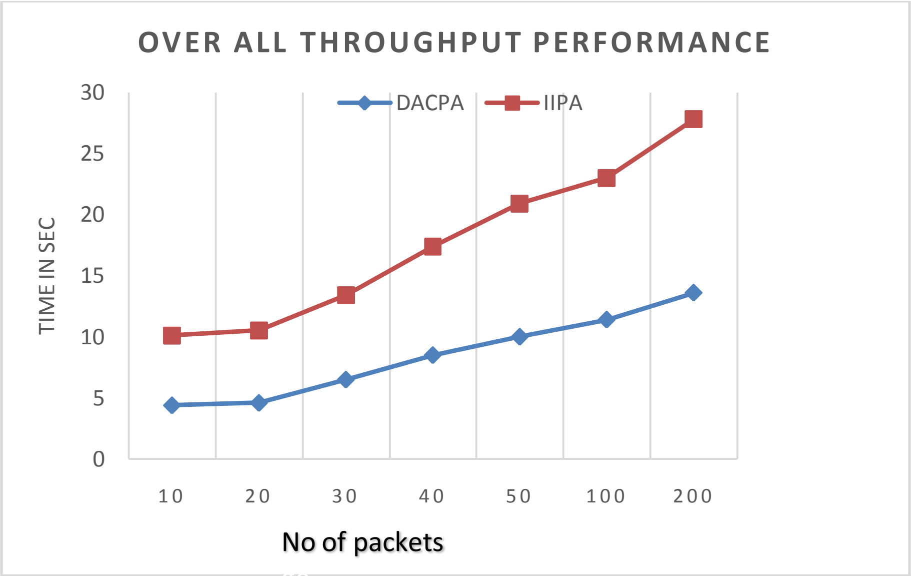


Fig: Throughput performance

Throughput execution is processed in light of the quantity of parcels being conveyed to the goal anytime of the time interim. The measure characterizes how quick a node can send the information through a system.Average throughput is the rate of strong messages shows the high figure delivery over a channel during a communication.

ISSN 2348 – 8034
Impact Factor- 5.070

V. CONCLUSION

Active arranging and recognition of vulnerabilities for Identical IP Analysis for Reduce Phishing Attacks IIPA in distributed computing will distinguish the deadly attacks in parallel. By utilizing the Identical IP Analysis for similar subtle elements gathering and order will build the performance speed. Vulnerabilities can proficiently break down from the grouped information. Expanding the rate of gathering the data and its rankings are finished by utilizing the ACO enhancement system. Botnet concealment, forensic analysis of phishing and flooding attacks are available in this paper. This arrangement is sparing for vast scale forensic analysis for interruptions information in Phishing attacks.

REFERENCES

1. *Ensemble learning methods for power system cyber-attack detection, Xiayang Chen, Lei Zhang, Yi Liu IEEE 18 June 2018.*
2. *Cyber security analysis of internet banking in emerging countries: User and bank perspectives, Jaafar M. Alghazo, Zafar Kazmi, GhazanfarLatif IEEE 01 February 2018.*
3. *Data Integrity Attacks against Dynamic Route Guidance in Transportation-based Cyber-Physical Systems: Modeling, Analysis, and Defense, Jie Lin, Wei Yu, Nan Zhang IEEE 08 June 2018.*
4. *Adaptation of the neural network model to the identification of the cyber-attacks type "denial of service," OleksandrOksiiuk, LiudmylaTereikovska, IhorTereikovskiy IEEE 12 April 2018.*
5. *A user-centric machine learning framework for cybersecurity operations center, Charles Feng, Shunning Wu, Ningwei Liu IEEE 18 August 2017.*
6. *A contribution to cyber-security of networked control systems: An event-based control approach, SouadBezzaouchaRebaï, HolgerVoos, Mohamed Darouach IEEE 31 August 2017.*
7. *Analysis of cyber-physical systems security via networked attacks, HuiGe, Dong Yue, Xiang-pengXie IEEE 11 September 2017.*
8. *Making DNS Servers Resistant to Cyber Attacks: An Empirical Study on Formal Methods and Performance, Barry S. Fagin, Bradley Klanderman, Martin C. Carlisle IEEE 11 September 2017.*
9. *Privacy-preserving cyber security information exchange mechanism, ImanVakilinia, Deepak K. Tosh, ShamikSengupta IEEE 21 September 2017.*
10. *Security challenges and methods for protecting critical infrastructure cyber-physical systems, James M. Taylor, Hamid R. Sharif IEEE 21 September 2017.*
11. *Cyber security for Control Systems: A Process-Aware Perspective, FarshadKhorrami, Prashanth Krishnamurthy, Ramesh Karri IEEE 27 July 2016.*
12. *Cyber Security in Industrial Control Systems: Analysis of DoS Attacks against PLCs and the Insider Effect. ErcanNurcanYlmaz, BünyaminCiylan, SerkanGönen. IEEE 2018*
13. *An Analysis of Cyber Security Attack Taxonomies. Richard Derbyshire, Benjamin Green, Daniel Prince. IEEE 2018.*
14. *Cyber security of smart homes: Development of a reference architecture for attack surface analysis K. Ghirardello,C. Maple,D. Ng. IET 2018*
15. *A (lack of) review on Cyber-security and Privacy Concerns in Hearing Aids. PanagiotisKatrakazas, DimitriosKoutsouris. IEEE 2018.*
16. *Cyber Security Threats and Mitigation Techniques for Multifunctional Devices MuyowaMutemwa, Francois Mouton. IEEE 2018*
17. *Gedare Bloom and GianlucaCena,"Supporting Security Protocols On Can-Based Networks," IEEE, Vol-5, Issue-3, 2017*
18. *MoustafaAmmar and Mohamed Rizk," A Framework for Security Enhancement in Sdn- Based Datacenters," IEEE, Vol-4, Issue-10, 2016.*
19. *Nardon, f., &Moura, l. "Knowledge sharing and information integration in healthcare using ontologies and deductive databases." Medinfo, 62-66, 2004.*
20. *Ferrara, l., "Integrating data sources and network analysis tools to support the fight against organized crime." Intelligence and security informatics, 171-182, 2008.*