International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Performance Improvement of Intrusion Detection Systems

Debi Prasad Mishra, Satyasundara Mahapatra, Sateesh Kumar Pradhan

Abstract*: Intrusion Detection Systems (IDSs) have been crucial in defending intrusive attacks (both active and passive) in various application scenarios in recent trends. Over the years, many research activities have been carried out on intrusion detection systems. The IDSs have been evolved over times with various detection methodologies, approaches, and technology types. The IDSs after several evaluations and different approaches still face a major challenge-performance improvement. This improvement can be quantified in two broad ways- the detection rate and the rate of false positives. The improved performance involves the efficiency and accuracy of detection. The efficiency can be attributed to performance in case of a very high amount of attacks and the accuracy can be attributed to a significantly low amount of false positives. In the same context, we have found that the IoT networks which are in high demand in recent trends also suffer from such types of attacks in operational environments due to limited storage and processing capabilities. In order to protect the IoT application, the scenario necessitates the need of IDS that is lightweight in implementation and provides a significantly higher amount of accuracy which is at par with the IDSs implemented in conventional networks. In this work, we have proposed an improved technique for performance improvement of IDSs in IoT domain.

***Keywords*: IDS, detection rate, false positives, IoT, performance improvement**

I. INTRODUCTION

The growth of computing facilities has yielded a multitude of benefits to the field of computing. In earlier days, the security of computing systems was not perceived as a potential threat. The growth in the field has also given rise to threats in manifolds. Over the last few decades, attackers have been of illicit intentions to gain access to various computing networks. This kind of illegitimate access to a network can be attributed to intrusion into a network. Intrusion detections have been of critical importance as intrusions are likely to hamper the efficiency and availability along with possible instances of data theft.

Till date researchers have come up with various solutions to prevent the threat of intrusion detection. The systems have been designed with various detection methodologies, detection approaches, and various technologies.

Manuscript published on 30 August 2019.
*****Correspondence Author(s)
Debi Prasad Mishra*, Department of Information Technology, College of Engineering and Technology, Bhubaneswar, India. Email: dp.mishra.07@gmail.com
Satyasundara Mahapatra, Department of Computer Science and Engineering, Pranveer Singh Institue of Technology, Kanpur, India. Email: satyasundara123@gmail.com
Sateesh Kumar Pradhan, Post Graduate Department of Computer Science, Utkal University, Bhubaneswar, India. Email: sateesh1960@gmail.com

Signature-based detection systems are simplest and proven to be effective while detecting known attacks and also provides the facility for detailed contextual analysis. Anomaly-based systems have been found to be effective in scenarios where the threat are not previously present in the system [4]. These systems require very less operating system resources and they possess the ability to detect abuse of privilege usages. The stateful protocol analysis systems are helpful in tracing the different states of protocols that are being used in the network. They can distinguish unexpected sequences of commands. The signature-based systems cannot detect unknown attacks. The anomaly bases systems are unavailable during the rebuilding of behavior profiles. The stateful protocol analysis systems are resource consuming and might be incompatible to dedicated operating systems and access points. However, in all such detection methodologies, the false positive rate plays a crucial role to define the accuracy of an Intrusion detection system. Along with the rate of false positives, the rate of detection of attacks needs significant improvement so as to provide timely protection against malicious attacks.

II. METHODOLOGIES OF INTRUSION DETECTION

The various methodologies for intrusion detection can be categorized into three major categories: Signature-based Detection (SD), Anomaly-based Detection (AD) and Stateful Protocol Analysis (SPA) [1-3] [5].

A. Signature-based detection methodology

A signature in the IDS terminology is perceived as a pattern or some strings which are related to some previously known threats. SD is the process of comparison of patterns against previously captured security events to recognize possible intrusions. Due to the usage of previously-stored knowledge to analyze attacks, SD is also known as Knowledge-based Detection.

B. Anomaly-based detection methodology

Anomalies are typically a deviation to a known behavior and behavioral pattern derived from various regular activities on a network over a certain period of time. The various activities can include user activities within a network, network connection, and disconnection requests, etc. The generated behavioral profiles of the user data can be either static or dynamic. Each of the profile may correspond to different activities, e.g., unsuccessful attempts to log in, the usage of processors, e-mails count, etc. Thereafter, regular profiles are compared with experimental events to segregate significant attacks. In some contexts, this method is also known as behavior-based method.

These types of IDSs can be helpful in the prevention of attacks ranging from external forceful intrusion, inconspicuous intrusion by genuine users, Denial of Service attacks or even some forms of passive attacks.

C. Stateful Protocol Analysis Methodology

Using this methodology, IDSs are capable of tracing the protocol states (e.g., pairing of requests with replies). Though the attack processing in SPA is somewhat similar to ADs, they are subtly different in usage [6]. AD adheres to previously-stored host or network specific profiles, whereas SPA relies on custom-made generic protocols.

D. Hybrid Methodology

No IDS is single-handedly capable enough to provide quite a promising rate of intrusion detection and protection. Hence, some of the IDSs prefer to utilize the methodologies of more than one category of IDSs. This kind of mixing of various methodologies can be attributed to a hybrid IDS methodology. For instance, the signature-based and anomaly-based methods are complementary to each other, the reason being the SD method focuses on known attacks whereas the AD method tends to prevent unknown attacks.

III. APPROACHES TO DETECTION

Stamp in [2] discussed a technique of classification to further split IDS methodologies into three subcategories including approaches based on computations and other ANN (Artificial Neural Network) based methods. Liao and Tung [3] have presented a much more generalized classification of five subclasses with a comprehensive outlook of features of detection systems: Statistics-based, Pattern-based, Rule-based, State-based and Heuristic-based.

A. Statistics Based

The statistic-based approach can be further subdivided into three more categories.Statistics-based approaches gather resources from audit data usage of disk and memory. These gnature-based detection. This mechanism is simple but lacks to provide accuracy. The implementation can be host-based or network-based. The distance-based systems gather data from audit sources and network packets. These are implemented using anomaly-based methods. This mechanism is real-time and active. These are implemented using a network approach.

Bayesian-based approaches gather data from audits, prior events, and network traffic and user profiles. These can be implemented using anomaly-based detection or signature-based detection. The results are mostly optimal statistical.

Game theory-based approaches gather data from system events or incidents, system logs. These can be implemented mostly using anomaly-based approaches. These are mostly used for experimental purposes in both hardware and network environments.

B. Pattern-based

Pattern matching includes methods like pattern-matching, keystroke monitoring, and file-system checking.

In pattern-matching systems, the data is collected from audit records and known intrusion signatures. These are conceptually simple and produce graphic depiction. These are implemented using signature-based methods in hardware.

Pattern matching systems sometimes involve keystroke monitoring which is carried out using the user's typing pattern.

C. Rule-based

These are based on audit records and patterns generated from users' database and system administration policies. These can be implemented using both anomaly or signature-based methods. The implantation can be done using hardware or over a network. Sometimes it can involve audit data or even the knowledge base for association rule discovery.

D. State-based

State-based approach mostly uses anomaly detection technique and can be implemented in a hybrid or network scenario. The knowledge is often derived from the state transition diagram of known attacks.

E. Heuristic-based

These IDSs can be implemented using both anomaly and signature detection methods and can be implemented in a network or hybrid environment. It accumulates data from audit records, network traffic and it is highly scalable, easily configurable and flexible [18]. This is mostly inspired by bio-inspired computing intelligence.

IV. IDS TECHNOLOGIES

There are several categories of IDS technologies that are in use in recent trends. They can be categorized into four classes according to their deployment mechanisms and the type of events the IDSs can distinguish.

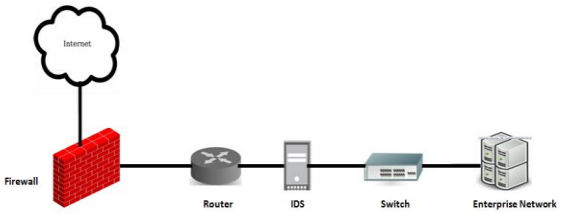

Fig. 1. A Network BAsed IDS Example

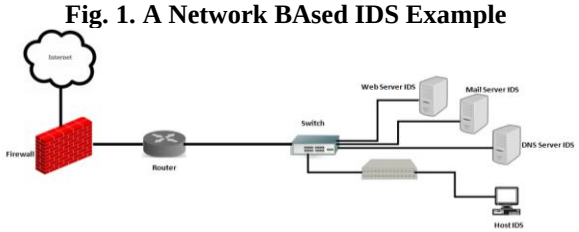

Fig. 1. A Host-based IDS Example

A NIDS is capable of capturing demand for incoming data traffic at certain specific sections by utilising sensors and investigates functions of various application protocols in order to distinguish distrustful events. A wireless based intrusion detection system in its implementation is akin to NIDS. In addition to the similarities with NIDS, WIDS is capable of capturing wireless network traffics of even mesh networks (wireless) and even that of ad-hoc networks. A system based on network behavior can also inspect data streams to identify attack having unforeseen data patterns.

Retrieval Number: J96690881019/19©BEIESP
DOI: 10.35940/ijitee.J9669.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Adoption of compound IDS technologies as MIDS can be useful for a more comprehensive and precise discovery. The general architecture for a NIDS is shown in Figure-1.

A HIDS is mostly a software-based IDS comprising of one or more management servers and database servers and a single host. It can be implemented in both managed and standard networks. The detection methodology here is a combination of signature and anomaly-based detection. It can gather information in high-speed networks in a very efficient manner[40]. But sometimes it may occur delays in error reporting and also consumes significant resources. It is mostly used for network traffic analysis and event logs.

A NIDS may comprise of a more than one inline or passive sensors with one or more management and data servers deployed in a managed network with multiple subnets catering to multiple hosts.

It can gather information from OSs, hosts, APs and network traffic. But it cannot monitor wireless protocols and cannot detect attacks within encrypted traffic.

It has a similar architecture as that of NIDS apart from the functionality that it can be deployed over wireless LAN. It can acquire data from WLANS, APs, clients, etc. It combines the advantages of two categories of systems: one category utilizes previously stored data and another looks for the deviations in the data pattern.

The IDS includes two components: sensors and agents. Sensors are generally used for monitoring activities NIDS, WIDS, and NBA systems. Agents are mostly used in Hybrid IDSs to inspect and examine network events. Sensors and agents both are capable of relaying information to the individual servers responsible for different management and database operations. Management part id deals with the stored events and the database part handles the event data in centralized storage for future reuse. There are two categories of network architectures: the first is the Managed Network (MN) that is a secluded network and is deployed to disguise the presence of IDS from attackers. Managed Networks increase the hardware overheads and carry certain management inconveniences for network administrators. A Standard Network (SN) is another form of a network, mostly a public network without any defense mechanism. One way to improve the security of the standard network is to configure a virtual and isolated network by means of a virtual local area network. Alternatively, most IDS technologies facilitate four common capabilities for defense purpose: information collection, logging, attack detection, and prevention. The observed activities of users are used to collect information inside the hosts/networks. The logged data for detected events can be utilized for validation alerts and for research of intrusion-related incidents.

The accuracy rate of intrusion detection is a crucial parameter of IDS technologies. The accuracy of IDSs is indicated by two parameters-the rates of false positives (FP) and the rate of false negatives (FN). The false positives are said to be generated when genuine requests are wrongly identified as malicious attacks and in cases when the IDS fails to classify an attacks scenario, it is referred to as a case of false negatives. In experimental setups, the administrators may increase more suspicious events and then segregate false positives from real suspicious incidents.

V. PERFORMANCE IMPROVEMENT TECHNIQUES FOR IDS

We have come to the observation that each technique has its own set of advantages and disadvantages. Hence, it is of utmost importance to select the right type of IDs for our requirement. In spite of the features like easy application and effective scrutiny mechanism for known threats, it is not possible on the part of pattern-based IDS to identify known attacks. In many other research findings, several rule-based approaches that can detect unknown attacks have been proposed. However, the implementation of such techniques may result in more computational overhead for the purpose of hard-creation and updating of records. In addition to this, approaches based on heuristics can effectively identify unknown attacks but they lack in efficiency while being used in real-time systems because of increased demand for computational complexity. We present a more comprehensive technique to to improve the performance of IDSs.

A. Performance improvement by efficient packet capturing

In a PC based NIDS, the packet capturing technique plays an important role in increasing the efficiency of intrusion detection. This issue is generated mostly due to operating system limitations.

A NIDS implemented on a PC is preferred over an FPGA or hardware-based NIDS because of the capacity of the former to accommodate complex and dynamic rules required for ever-changing network attack patterns. However, a GHz CPU can match only 100 Mbps traffic, [6, 7] as it exploits quite a large number of computationally demanding pattern matching and co-relation rules. With a NIDS of this type, there are still possibilities of packets being skipped [7, 8] and may result in a detection rate which is far below the expected rate during peak hours[9,10]. An attacker may be able to attack such NIDS with overwhelmed packets with encapsulated packets to deter real attack packets, which the NIDS may ignore at some point of time. In addition to this, for more efficient packet capturing rate, computationally powerful hardware, multiprocessor or distributed systems are deployed [6, 9] , [12-14].

This technique uses a DMA ring in a distributed NIDS environment. For improved throughput, the detection rules on the sensor side need to be stored in an in-memory database which can further be updated through a management interface

B. Correlation as a Sample Selection Method

In this work, the authors have proposed an instance selection method using KDD CUP99 dataset for evaluating anomaly detection techniques. The growth of network resources has also given a way for the growth of threats and hence, IDSs have become important to protect networks from attacks. The process of categorization between a legitimate and an attack packet is actually a classification process. The difference between normal and abnormal behavior is referred to as a two-class problem. In cases of more number of classes, it can be named as a multi-class problem. In the field of intrusion detection, several techniques are currently in use for feature selection in attack datasets. In [15], the authors have proposed an automatic feature selection method which relies on a correlation measure.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In [16] another such algorithm is described to retain useful features those result in improving the accuracy of the classifier.

Correlation is a scale between two variables and the values of variables lie in the range of [-1, +1]. A correlation value of 0 indicates no correlation, -1 shows a perfectly negative correlation and +1 shows perfectly positive correlation.

For the assessment of the above method in the raining function of the classifier, a three-layer feed-forward network is used that is trained by the reduced dataset for effective classification of intrusion and normal datasets.

C. Performance improvement of intrusion detection with the fusion of multiple sensors

The basic function of an IDS in akin to a classifier for collection of pieces of evidence to find out the presence of intrusion and generate the necessary alarm. A typical IDS system mostly uses more than one IDSs that tend to be unalike in nature. The previously described dissimilarity in the individual systems may be in terms of detection algorithm or the network traffic [17].

Authors in [15] have presented the technique of fusion of alerts and prove that in a scenario of simultaneous application of anomaly detection technique and signature recognition techniques, these two techniques tend to complement each other to achieve an improved detection rate and a low false alarm rate.

The dependence on an efficient rule is crucial to this process of detection. Along with this, the reliability of an IDS is also a major concern. This paper presents a new rule for the fusion of alert databases to incorporate the accuracy of evidence and also resourcefully handle the information for an improved IDS.

The proposed alert fusion system combines results receive from various data sources and utilizes Demster-Shafer theory of evidence [11] to correctly classify the attack pattern.

D. Improvement of Intrusion detection with advancement in sensor fusion

Many of the erstwhile IDSs have reasonable accuracy in the detection of a certain category of attack while diminishing the performance for other classes. It has been found that most of the attacks are characterized by features that are not so much discriminating. Authors in [19] have made a novel effort to demonstrate the capability of multiple detection systems using rule-based fusion techniques.

The experiment revealed that fusion-based systems are ideal only for input data of smaller threshold and there is also a requirement for a machine learning algorithm for the handling of the said type of data in the network. These systems are highly dependent on individual IDSs which further come out as a shortcoming using sensor fusion technique. In order to a considerably good amount of security, a combined arrangement of shallow and deep sensors can be utilized in IDSs [19]. From the two sensors used for fusion, one is used to monitor the traffic packet header whereas the other is used for the packet content. The same has been proposed by authors in [20]. The choice of sensors is of critical attention for utilization of advantage received from multiple fusion of sensors in the IDS [2]. Further, complementary IDSs are utilized to ensure versatility and consistency. The PHAD [20] being a method based on packet-headers and detecting only a single packet at a time is completely unable to detect the slow scans. However, PHAD [20] detects the silent scans much more effectively. The ALAD being a content-based mechanism will complement the PHAD by detecting R2L (Remote to Local) and U2R(User to Root) attacks with a considerably high amount of efficiency.

E. Improving the efficiency of IDS through QoS Configuration and Parallel Technology

This work emphasizes the requirement of high-quality network infrastructure for better protection from the network attacks. The authors experimented with Snort NIDPS and have found that there are some chances of packets being dropped and in the presence of enormous network traffic and high-bandwidth networks without being examined. A typical IDS' performance metrics may include factors like the number of packets sent, number of packets dropped, and number of packets filtered, analyzed, dropped, injected and outstanding. Hence, the authors have suggested QoS configuration using a Cisco Catalyst 3560 series switch and parallel Snort IDSs for improving performance by means of reduced dropped packets. The experiment described in this work uses performance metrics like Packet generators. Timing statistics, Packet I/O totals, protocol Statistics, Snort-NIDS throughput. This paper is focused on the failure of NIDPS for prevention of threats that may occur in high-speed network collectively. Use of a Multi-core IDS could be an efficient alternative for high-speed data network connectivity as they provide enhancement with high capabilities while securing the network side by side. The work of detection by utilizing multiple processors is yet to be explored. But, the speed, the volume of attacks and the complexity of attack categorization in various stages of attacks pose a significantly greater amount of challenges to network security. Appropriate use of multiple processor cores can further fine-tune a NIDPS to withstand such attacks. Further, we need to develop parallel systems with efficient computational algorithm and capable hardware that can address high complexity attack incidents in future prospects.

VI. PREVENTION OF INTRUSION DETECTION-AN INTERNET OF THINGS PERSPECTIVE

Smart environments have proven their ability to improve the comforts of life. The IoT ecosystem has been an integral part of the development of smart environments. Along with the efficiencies, risks like security and privacy threaten the IoT environment. This necessitates the need for an intrusion detection system for the IoT environment. Conventional IDSs may not be able to provide adequate efficiency in detection due to the fact that IoTs have limited computing and storage capability. [37] IoT (Internet of Things) is a dynamic infrastructure with self-configuring capabilities based on standard and interoperable communications. [21]

Cole and Ranasinghe [22] identified a number of attacks associated with RFID. For example, 1) cloning - duplication of security features, so that they can be passed as authentic during verification. 2) obfuscation- Use of misleading protection technologies. 3) tag omission, i.e. the abdication of the security features by counterfeit producers 4) removal-reapplication attacks refer to the application of genuine security features from (mostly discarded) genuine products to counterfeit articles. 5) DoS attacks targeted to diminish a network's capacity to perform.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The authors in [23] discussed the model for node capture attack and presented a framework for threat analysis and network response strategies in case of the attack.
In [24], the authors have discussed potential security concerns involving smart home appliances and even wearable personal IoT devices.
In [25], a central IDS is presented where packets passing through both physical and network domain are analyzed in order to prevent the botnet attacks. In their work in [26], authors have shown a hybrid placement strategy for building monitoring attacks in an organized network. The placement of monitoring nodes is typically in the fashion of one node per region.
The work described in [27, 28] proposes another alternative for the prevention of DDoS attacks over IoT middleware. This method being a specification-based method utilizes the ability of each of the middleware layers for detection of attacks. The system produces an alert when requests to a particular layer exceed the specified threshold that has been set in the network.
Lee et. al [29] proposed a computationally lighter IDS for IoT systems. This technique utilizes a distributed placement strategy for monitoring the node energy consumed for intrusion detection, namely DoS attacks. The rate of energy consumption for each node is kept track of and in the event of energy consumption increasing beyond the threshold limit, nodes are classified as malicious by the system and the same is eliminated from the routing table.
Oh. Et al [30] have described a lightweight IDS for IoT which can make a match between attack payloads and attack signatures. In this approach, an algorithm has been designed which can skip checking a large number of unnecessary matching operations in the process of verifying packet payloads. This process is aimed at minimizing the computational cost of comparison between packet payloads and attack signatures.
Cervantes et. al [31] proposed an IDS for detection of sinkhole attacks in 6LoWPAN for IoT. This technique had a hierarchical structure of nodes and the placement of nodes was done in a distributed fashion. The approach in this work was a combination of trust and reputation along with specification-based method and anomaly-based method for monitoring of packet exchange between nodes.
The IDS described in [32] presents an IDS having a hybrid placement strategy. In this technique, the nodes are required to scan their neighborhood for changes and send the changelog to central modules in the border router of networks.
Summerville et al. [34] developed an IDS for IoT based on a deep-packet anomaly detection method. The detection method used here uses bit-pattern matching for feature selection. Network payloads are termed as a sequence of bytes and feature selection operates on overlapping tuples of bytes called n-grams. A match between a bit-pattern and an n-gram occurs when the corresponding bits match all positions. The evaluation of the above approach resulted in very low false-positive rates for four common types of threats.
In [35], the authors have represented an IDS for IoT named (Kalis)- "Knowledge-Driven Adaptable Lightweight Intrusion Detection Systems". This technique employs a centralized placement technique for IDS. This system utilizes a self-adaptation and knowledge-based approach to provide security for systems running on different communication protocols.

In the 2017 paper [36], Shreenivasn at.al presented a solution on IDS for IoT. This solution aims to improve security within 6LoWPAN networks. The authors have extended SVELTE with intrusion detection module that uses expected transmission metric. In addition to this, the authors have proposed geographic hints to identify malicious nodes that conduct attacks against ETX-based networks. The experimental results yield improved true-positive rates in comparison with rank-based mechanisms.

According to [38], the issue of security in IoT can be classified into four categories- authentication and physical issues, confidentiality issues, data integrity issues, and privacy. The relationship between these issues is shown in Figure-3.

A. *Authentication Problem*

This is the foremost kind of security threats for IoT systems. This layer mostly includes IoT devices like sensors depending on their own security, which makes them promiscuous to physical damages from external entities.

B. *Confidentiality risks*

These kinds of risks come up between the IoT device and gateways in the network layer. Controlled nature of resources being a characteristic of low-level devices in IoT, it emerges as a challenge to the privacy of data transmission in IoT networks [39].

C. *Integrity issues*

Data integrity problems emerge in the event of spoofing attacks and attacks like DoS, DDoS which can significantly hamper IoT services and applications.

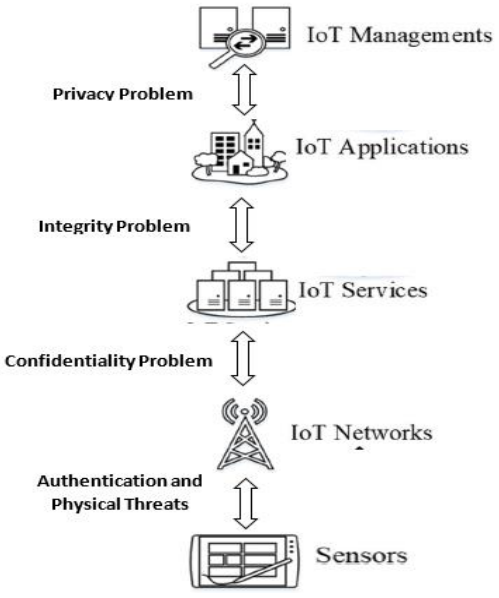

Fig. 2. Various IoT Layers with their Security Issues

D. Privacy

Data privacy is a crucial characteristic of security in IoT systems. Every object in the IoT environment have their own identification technologies and so every device is uniquely identified by its identification tags carrying personal, location and movement information.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Any kind of unauthorized access to the management systems puts the information privacy of users at risk.

In their work described in [40], Raza, et. al have proposed SVELTE, a novel model for real-time intrusion detection in the Internet of Things. The authors have expressed their views that even though security services that encryption and authentication are prevalent, there are chances of breach of security by means of wireless attacks from within the 6LoWPAN networks and from the Internet. The authors have also found that at present there are no intrusion systems that provide protection for IPv6 connected networks as some of them have been specialized for wireless sensor networks or for the traditional Internet.

In the proposed model in [40], that has been named as SVELTE, the model is targeted to block wireless attacks such as spoofing attacks, sinkhole attacks, and selective-forwarding attacks.

SVELTE is an IDS integrated with a mini-firewall for the IP connected IoT and it uses RPL (Routing Protocol for Low-power and Lossy Networks). RPL is a specialized routing protocol designed for routing of IoT networks [41]. There are two main components of SVELTE: the 6LoWPAN Mapper and an intrusion detection module. The RPL's current routing state which is a directed acyclic graph is modified by the 6Mapper and extensions are made to it with additional routing parameters at the 6BR (6LoWPAN Border Router) [33].

In IoT networks wormhole attacks are of critical importance and the networks need to be secured from such attacks [42]. SVELTE with 6Mapper being extended to the signal strength of each node's neighbor can detect wormhole attacks [43]. SVELTE is highly flexible which is needed to be a feature of any modern intrusion detection system. In case of new packets requiring to be added to the routing graph, they can be easily extended [] as per the requirement. In addition to this, the data collected using 6Mapper can be used to apply anomaly-based detection methods by using support vector machine [44], feature vector [45] or automata-based approach [46].

In [48], the authors have presented a security framework for intrusion detection in a virtual network of cloud computing. As per the perceived knowledge, a typical cloud has mainly three types of networks: a virtual network, an internal network and an external network which is shown in Figure 4.

The work in [48] describes the use of a hypervisor level distributed network security (HLDNS) positioned on each processing nodes of the cloud. At each server level, the underlying machine traffic is monitored taking the following things into account: the network traffic to and from the network, the internal network, and the external network.

The feature extraction mechanisms along with a binary bat algorithm (BBA) [49] derive significant features from the network traffic and then the features are applied to the Random forest classifier for intrusion detection and alert generation.

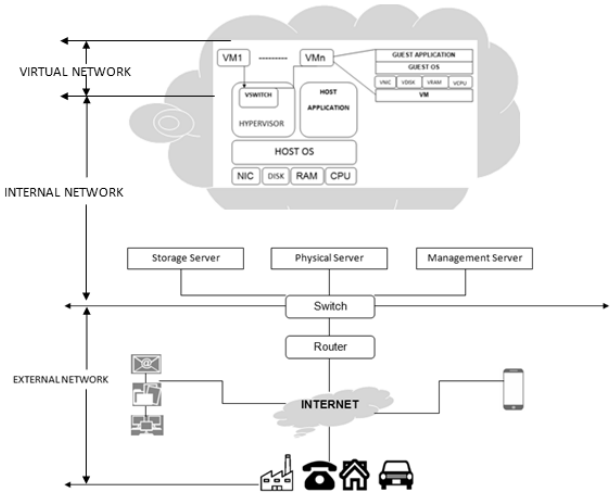

Fig. 3. Cloud Network Infrastructure

The proposed model in [48] using the HLDNS is depicted in Figure 5.

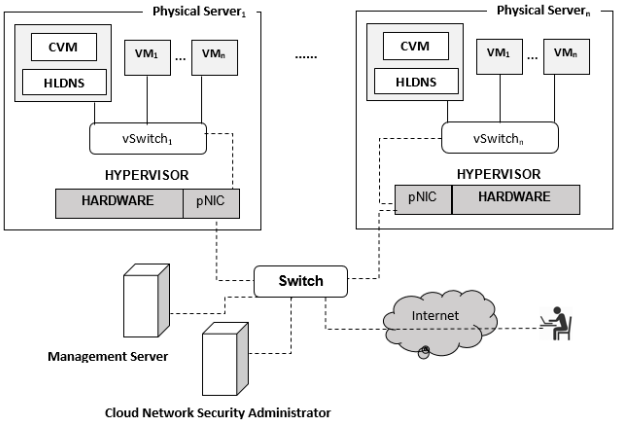

Fig. 4. Deployment of HLDNS in Cloud Framework

VII. CONCLUSION

The growth of the Internet and cyber-crimes have led to the research of IDSs. Many researchers have identified potential needs and requisite solutions, which have showed results in some directions, but there are scopes for improvement and in some cases, there are some loopholes or drawbacks, which is still unattended.

The following table represents a comparison between HIDS and NIDS as shown in [47].

Table 1: HIDS Vs NIDS in terms of performance

Performance in terms of:	HIDS	NIDS
Deterrence of Intruders	Ideal for internal intruders	Ideal for external intruders
Response Time	-Low real-time response -Improved performance for long time attacks	High response time against external intruders
Damage Assessment	-Excellent estimation	-Weak estimation
Intruder Security	Excellent for external attackers	Excellent for external attackers
Threat expectancy	Excellent in determining suspicious behavior patterns	Excellent in determining suspicious behavior patterns

As per the available studies, we have found that there are no such IDS that provides complete detection coverage. In the case of increased performance, reduction in false alarm rate is also a crucial factor.

We need to find effective ways to detect network intrusions by combining one or more currently available techniques. In addition to the designing of IDS, we need to set the focus to some design metrics like threshold rate, detection rate, rate of false positives, performance in high-speed networks, computational complexity, etc.

Meanwhile, IoT has emerged as an important medium for connecting to physical objects with the Internet in diversified functional domains. Considering the Internet and the underlying physical devices being connected, security from intrusion attacks of crucial importance at par with the traditional networks. From the work that we have presented, we can summarize that the research in IDS in IoT is in the rudimentary stage. Taking the placement strategy and detection method into research we have found that none of the techniques have reached a concrete point to find the right option to select characteristics of IDS for IoT.

Hence, we aim to find out a method taking both placement strategy and detection method at a level that will have a significantly improved intrusion detection for IoT devices and networks.

REFERENCES

1. Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy (Vol. 99). Technical report.
2. Stavroulakis, P., & Stamp, M. (Eds.). (2010). Handbook of information and communication security. Springer Science & Business Media.
3. Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.
4. Kumar, V., Srivastava, J., & Lazarevic, A. (Eds.). (2006). Managing cyber threats: issues, approaches, and challenges (Vol. 5). Springer Science & Business Media.
5. Xenakis, C., Panos, C., & Stavrakakis, I. (2011). A comparative evaluation of intrusion detection architectures for mobile ad hoc networks. Computers & Security, 30(1), 63-80.
6. Kruegel, C., Valeur, F., Vigna, G., & Kemmerer, R. (2002). Stateful intrusion detection for high-speed network's. In Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on (pp. 285-293). IEEE.
7. Judge, G. (2003). FPGA architecture ups intrusion detection performance. http://www. commsdesign. com/design_corner/showArticle. jhtml? articleID= 16502099.
8. Deri, L. (2004, September). Improving passive packet capture: Beyond device polling. In Proceedings of SANE (Vol. 2004, pp. 85-93).
9. Schaelicke, Lambert, Kyle Wheeler, and Curt Freeland. "SPANIDS: a scalable network intrusion detection load balancer." Proceedings of the 2nd Conference on Computing Frontiers. ACM, 2005.
10. Sekar, R., et al. "A high-performance network intrusion detection system." Proceedings of the 6th ACM Conference on Computer and Communications Security. ACM, 1999.
11. Shafer, G. (1992). Dempster-shafer theory. Encyclopedia of artificial intelligence, 1, 330-331.
12. Charitakis, I., Anagnostakis, K., & Markatos, E. (2003, October). An active traffic splitter architecture for intrusion detection. In Modeling, Analysis and Simulation of Computer Telecommunications Systems, 2003. MASCOTS 2003. 11th IEEE/ACM International Symposium on (pp. 238-241). IEEE.
13. Desai, N. (2002). Optimizing NIDS Performance.
14. Haagdorens, B., Vermeiren, T., & Goossens, M. (2004, August). Improving the performance of signature-based network intrusion detection sensors by multi-threading. In International Workshop on Information Security Applications (pp. 188-203). Springer, Berlin, Heidelberg.
15. Nguyen, H., Franke, K., & Petrovic, S. (2010, February). Improving effectiveness of intrusion detection by correlation feature selection. In Availability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 17-24). IEEE.
16. Chou, T. S., Yen, K. K., Luo, J., Pissinou, N., & Makki, K. (2007, October). Correlation-based feature selection for intrusion detection design. In Military Communications Conference, 2007. MILCOM 2007. IEEE (pp. 1-7). IEEE.
17. Katar, C. (2006). Combining multiple techniques for intrusion detection. Int J Comput Sci Network Security, 6(2B), 208-218.
18. Ye, Nong, et al. "Probabilistic techniques for intrusion detection based on computer audit data." IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans 31.4 (2001): 266-274.
19. Thomas, C., & Balakrishnan, N. (2007, April). Selection of Intrusion Detection Threshold bounds for effective sensor fusion. In SPIE Defense and Security Symposium (Vol. 6570).
20. Mahoney, M. V. (2003). A machine learning approach to detecting attacks by identifying anomalies in network traffic.
21. Smith, I. G. (Ed.). (2012). The Internet of things 2012: new horizons. CASAGRAS2.
22. Cole, P. H., & Ranasinghe, D. C. (2008). Networked RFID systems and lightweight cryptography. London, UK: Springer, 10, 978-3.
23. Bonaci, Tamara, Linda Bushnell, and Radha Poovendran. "Node capture attacks in wireless sensor networks: A system theoretic approach." 49th IEEE Conference on Decision and Control (CDC). IEEE, 2010.
24. Okpe, O. A., John, O. A., & Emmanuel, S. (2018). INTRUSION DETECTION IN INTERNET OF THINGS (IOT). International Journal of Advanced Research in Computer Science, 9(1).
25. Cho, Eung Jun, Jin Ho Kim, and Choong Seon Hong. "Attack model and detection scheme for botnet on 6LoWPAN." Asia-Pacific Network Operations and Management Symposium. Springer, Berlin, Heidelberg, 2009.
26. Le, Anhtuan, et al. "Specification-based IDS for securing RPL from topology attacks." 2011 IFIP Wireless Days (WD). IEEE, 2011.
27. Misra, Sudip, et al. "A learning automata based solution for preventing distributed denial of service in internet of things." 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing. IEEE, 2011.
28. Santos, L., Rabadao, C., & Gonçalves, R. (2018, June). Intrusion detection systems in Internet of Things: A literature review. In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-7). IEEE.
29. Lee, Tsung-Han, et al. "A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN." Advanced Technologies, Embedded and Multimedia for Human-centric Computing. Springer, Dordrecht, 2014. 1205-1213.
30. Oh, Doohwan, Deokho Kim, and Won Ro. "A malicious pattern detection engine for embedded security systems in the Internet of Things." Sensors 14.12 (2014): 24188-24211.
31. Cervantes, Christian, et al. "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things." 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE, 2015.
32. Pongle, P., & Chavan, G. (2015). Real time intrusion and wormhole attack detection in internet of things. International Journal of Computer Applications, 121(9).
33. Le, Anhtuan, et al. "A specification-based IDS for detecting attacks on RPL-based network topology." Information 7.2 (2016): 25.
34. Summerville, Douglas H., Kenneth M. Zach, and Yu Chen. "Ultra-lightweight deep packet anomaly detection for Internet of Things devices." 2015 IEEE 34th international performance computing and communications conference (IPCCC). IEEE, 2015.
35. Midi, Daniele, et al. "Kalis—A system for knowledge-driven adaptable intrusion detection for the Internet of Things." 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2017.
36. Shreenivas, Dharmini, Shahid Raza, and Thiemo Voigt. "Intrusion Detection in the RPL-connected 6LoWPAN Networks." Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security. ACM, 2017.
37. Awad, A. I., Furnell, S., Hassan, A. M., & Tryfonas, T. (2019). Special issue on security of IoT-enabled infrastructures in smart cities. Ad hoc networks.
38. Liu, Xiruo, et al. "A security framework for the internet of things in the future internet architecture." Future Internet 9.3 (2017): 27.
39. Trappe, Wade, Richard Howard, and Robert S. Moore. "Low-energy security: Limits and opportunities in the internet of things." IEEE Security & Privacy 13.1 (2015): 14-21.

40. Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad hoc networks, 11(8), 2661-2674.
41. Winter, Tim. "RPL: IPv6 routing protocol for low-power and lossy networks." (2012).
42. Hu, Y. C., Perrig, A., & Johnson, D. B. (2003, April). Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In Proceedings of INFOCOM (Vol. 2003).
43. Wang, W., & Bhargava, B. (2004, October). Visualization of wormholes in sensor networks. In Proceedings of the 3rd ACM workshop on Wireless security (pp. 51-60). ACM.
44. Kaplantzis, Sophia, et al. "Detecting selective forwarding attacks in wireless sensor networks using support vector machines." 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE, 2007.
45. Livani, Mohammad Ahmadi, and Mahdi Abadi. "A PCA-based distributed approach for intrusion detection in wireless sensor networks." 2011 International Symposium on Computer Networks and Distributed Systems (CNDS). IEEE, 2011.
46. Misra, S., Abraham, K. I., Obaidat, M. S., & Krishna, P. V. (2009). LAID: a learning automata-based scheme for intrusion detection in wireless sensor networks. Security and Communication Networks, 2(2), 105-115.
47. Kozushko, H. (2003). Intrusion detection: Host-based and network-based intrusion detection systems. Independent study.
48. Patil, Rajendra, Harsha Dudeja, and Chirag Modi. "Designing an efficient security framework for detecting intrusions in virtual network of cloud computing." Computers & Security 85 (2019): 402-422.
49. Mirjalili, Seyedali, Seyed Mohammad Mirjalili, and Xin-She Yang. "Binary bat algorithm." Neural Computing and Applications 25.3-4 (2014): 663-681.

AUTHORS PROFILE

Debi Prasad Mishra is currently working as an Assistant Professor in College of Engineering and Technology, Bhubaneswar. He completed his B. Tech in Information Technology in 2007 and M. Tech in Computer Science and Engineering in 2012. He has published his research work in several national and international conferences. His research interests include computer security, network security, and information retrieval. He has successfully guided undergraduate and post-graduate students in their projects and final dissertation work.

Satyasundara Mahapatra is an Associate Professor in the department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh. He received his Master degree and Ph.D in Computer Science from Utkal University, Bhubaneswar, Odisha in 2006 and 2016 respectively. He also holds a MCA degree from Utkal University, Bhubaneswar, Odisha in 1997. His current research interests include Machine Learning, Image Processing,, Scheduling and IoT. He has authored or co-authored in international scientific journals, two book Chapters and three patents approval in his field of expertise. .

Sateesh Kumar Pradhan is currently working as a Professor in Post Graduate Department of Computer Science in Utkal University, Bhubaneswar. He completed his Masters' Degree in the year 1983 and Ph. D. in the year 1999. He has published his research work in the areas of Neural Computing, Computer Architecture, Mobile Computing, and Data Mining in several journals and conferences. He has also written many books in his area of interest and edited many textbooks for Government of Odisha. He has been honored with various accolades from time to time for his contribution to the field of Computer Science. Apart from this, he is also heading various honorary positions in Utkal University as well as other universities of Odisha