Babylonian Journal of Internet of Things
Vol.2025, **pp**. 66–76
DOI: https://doi.org/10.58496/BJIoT/2025/002; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

Integrated A Robust Intelligent System for Secure Network

Tamara Saad Mohamed [1,*], Saad Mohammed khalifah [2]

1 Computer Science Department, kut university college , kut , Iraq.
2 Head of Department of Engineering of Medical devices techniques department Communication security, kut university college, kut ,Iraq.

ARTICLE INFO

Article History

Received 18 Dec 2024
Revised 02 Jan 2025
Accepted 20 Jan 2025
Published 07 Feb 2025

Keywords

Intelligent networks-intrusion detection

Intelligent Firewall

Virus Monitors

Intelligent Detection Engine

Intelligent Web Filter

ABSTRACT

An increasing number of assaults on network security that are related to the Internet are caused in malicious software. Firewalls, intrusion detection systems (IDS), and proxy servers that check for viruses are examples of safety technology that have been used by organizations that value safety. Not all high-priced safety features are easy to use. Having only one safety mechanism in place is insufficient to protect users' private information on privacy networks due to the fact that multiple safety schemes exhibit distinct traits, particularly hostile and DoS attacks. Integrating intrusion detection subsystems with different approaches to network security protection is detailed in this article. The subsystem employs AI techniques to detect unusual actions taken by known attackers and threats using the patterns recorded in the system's memory. Conversely, in order to prevent spyware documents from accessing the network, the proposed Intelligent Network Security System which contents intelligent web filter ,intelligent networks intrusion detection systems ,intelligent firewalls ;could detect the malicious URL and websites.

1. INTRODUCTION

Firewalls are utilized to secure and seclude connected Internet segments. Areas inside the system are ensured against untrusted information from outside [1].The flexibility and velocity are the main benefits of packet filter firewalls These systems can be used to ensure close protocols or any type of network interaction. In any business network in a structure, they can easily prevail. But the network can not be protected from extensive assaults because the data on the to player are not tested.It does not support sophisticated user authentication mechanisms, for example, itcan not detect netw ork packets" that change an addressing information on the OSI's third layer. Tasteful firewalls for inspection adds to the fourth layer a consciousness to the normal architecture of the packet filter. The pros and cons of packet filter firewalls are shared by these schemes. The real state-of - the-art search technology only applies to "TCP / IP." In addition, their use is very costly as the link status is always monitored[2].

Application-proxy-gateway firewalls have more comprehensive logging capacities, are immediately eligible to authenticate users, and can be rendered less susceptible to attacks with "address spoofing." However, these schemes are usually not suitable for high-bandwidth and real-time applications[3]. Using firewall, linked internet parts are protected and isolated. Inner network domains are shielded from external untrusted networks or network components are shielded from other components. Three main firewalls are available.

First, packet filter firewalls are available. The main focus of packet filtering is acceptance or denial. It is not suitable for gardings and is therefore suitable as other safety measures against intruders . Flexibility and fastness are the main benefits of “packet filter” firewalls, These schemes can be used to secure network communication or protocols of any kind carefully. They can readily prevail in any network infrastructure of corporations. Second, state of the art check firewalls add layer four, sensitivity to the normal architecture of the packet filter. They share the advantages and disadvantages of firewalls from packet filters. The current state-of – the-art search technology only applies to “TCP / IP.” In addition, their use is very costly as the link condition is constantly monitored. Third, application-proxy gateway firewalls have wider logging capacities that can be authenticated immediately by users and are less susceptible to assaults by’ email spoofing.’ However, these schemes are usually not suitable for high-bandwidth and real-time

*Corresponding author. Email: tamara.mohhh@gmail.com

applications.[4][5] Intrusion is essentially an action-based network. Detection of intrusion includes sympathize machines or people performing or endeavoring intrusion. Network Intrusion Detection Systems (IDS) are programs of computer that try to reveal intrusion by testing intrusion process behavior . The topic of intrusion has acquired importance with growing worldwide network connectivity, stimulating active studies on efficient(IDS)[6].

Virus controls test network traffic with the aim of preventing malicious packets network nodes entered by identifying unusual patterns of malicious code, which can only be detected by recognized viruses, for example in an email attachment. Every major retailer of anti-virus products has developed networked products and equipment to scan records. It is because Trojan horses, worms and viruses can spread via local networks, common hard disks, and individual documents files and the internet; virus controls on every user's computer should always be carried out on internet gateways. Samples of fresh malware are often not prepared until days or weeks have passed or even after weeks of severe damage[7].

2. RELATED WORKS

The traffic monitoring service checks the packet headers against the regulations for traffic monitoring, which are comparable to the regulations for packet filtering. J. Gary C. Kessler[8] suggests the architecture of the policy cache. Only the first cell that includes the IP header, protocol, TCP / UDP ports and TCP flags will be inspected to determine if a packet is secure or not. However, there are constraints; IP packets with areas of IP possibilities are not recognized because IP alternatives can be as big as 40 bytes and can push the "TCP" headers to the second cell. It does not seem that examining only the header data is adequate to overcome firewall disadvantages. Kaplan, David E., and Surjeet Rajendran [9] proposed that various safety methods should be integrated. This project's primary aim is to combine as many safety features in the firewall as possible. The idea of a smart firewall that includes a smart detection engine is discussed and implemented for possibly malicious data packets.
Aljawarneh, Shadi, Monther Aldwairi [10]outlined an off-line anomaly detection scheme that uses a neural network of back-propagation. It is talk about how the feature selection analysis and building hybrid efficient model through using Anomaly-based intrusion detection system by adding secure layers to the system.

3. PROPOSED SYSTEM METHODOLOGY

The Intelligent Security System is the latest generation of internet and intranet protection technologies. It is valuable and effective software program for network security that provides data, controls, and alarms to protect network users from intrusions, external assaults, and internal corruption. The scheme suggested is intended to fix lots of network attacks; (DoS, viruses , DDoS, spyware and worms). It offers the most worldwide alternative for the network to regulate the efficient use of Internet technologies in an open setting, it offers this control with very advanced, user-friendly, monitoring software; detects, blocks, alerts and logs particular access incidents and related information.

The suggested INSS (Intelligent Network Security System) security system is intended for:

- Easy set-up.
- Operating easily.
- Total user acceptance of the operation.
- Access to and documentation with easy control.
- The capacity to provide such facilities, even at elevated concentrations of network traffic, without any modifications or network delays.

The proposed protection systems, monitors and protects private network shown in Fig.1:

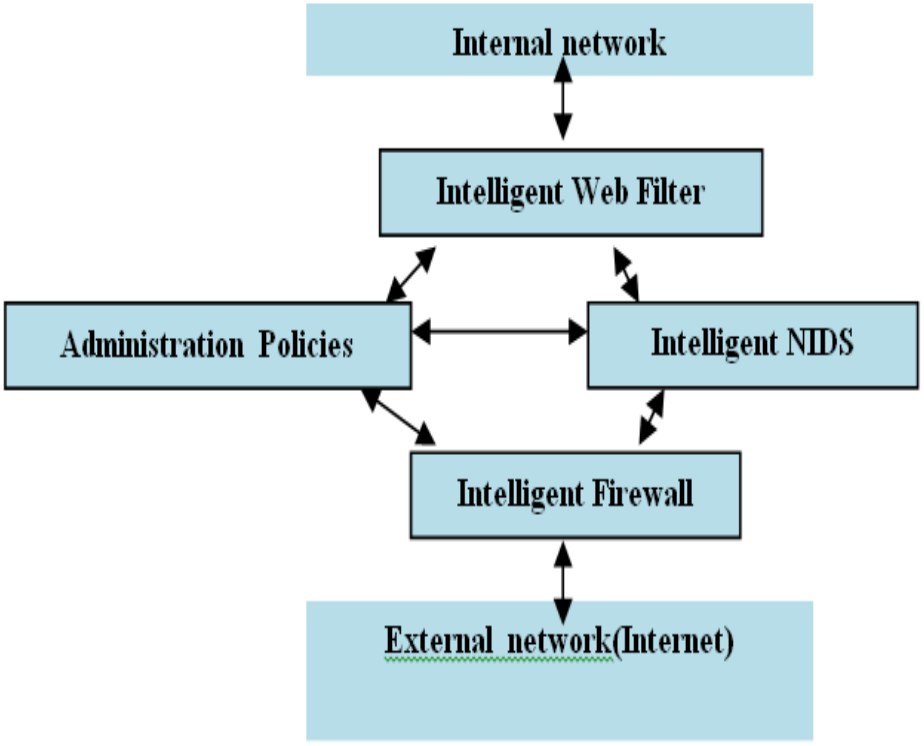

Fig.1 The Block diagram of the Proposed System.

- Intrusions, attacks, viruses, worms and other abusses are detected.
- Network activity monitoring.
- Supply summary and comprehensive reporting.
- Actions to perform or invoke certain occurrences.
- Alerts to send.
- Unwanted business blocking.
- Many URLs are identified as they are accessed.

The following main protection methods used in the suggested scheme are :

- Intelligent Firewall (IFW).
- Intelligent networks-intrusion detection subsystem (INIDS).
- Intelligent Web Filter (IWF).

Figure 2 illustrates a typical Corporate security network suggested, This typical system network used for testing, protecting the network connection to the Internet via corporate protection network (consisting of INIDS, firewall, Web filter, antivirus and anti-Spyware). The suggested scheme is tested with another typical network using certain attack kinds, such as DoS , viruses, worms and spyware." The system that is openly available from the outside world and that accessed locally is clearly distinguishing.[11]

Suppose a native virus and associated content filters like spam detection are implemented, firewalls often use antivirus interface to scan malicious traffic content. In Fig. 2, the avoidance scheme is displayed for Corporate Firewalls and network intrusion detection. They are extremely important to deal with network attacks on your network's individual hosts[7].[12] [13] The significant "network" defense methods that have been suggested will be discussed in the following parts.

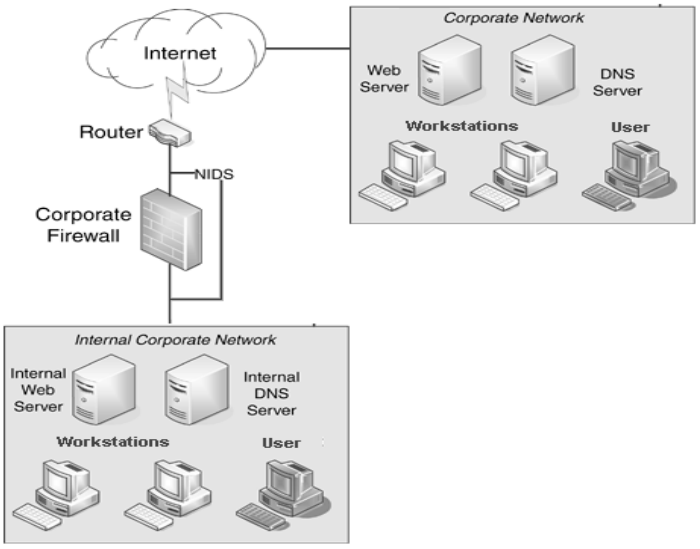

Fig. 2 The Typical Corporate Network With Proposed Security Zones.[14]

3.1 The Proposed Intelligent Firewall Protection

Tasteful solutions for Firewalls, as the name suggests; monitor and compare Network Traffic Status (such as links). The suggested state-of - the-art firewall can scan some application protocols to see if certain established protocols, including (SMTP) use only periodic commands. If SMTP server gets orders that are not SMTP, then the firewall pretends that the sender accepts the bogus instructions.

There is a packet based detection component in the firewall model suggested. Figure (3) illustrates the suggested architectural firewall model. These detection elements are not only about the header but also about the payload of a packet.

The principal function of the packet verifier is to identification of protocol defects, to clarify which packets could be malicious with how much probability, and to find and interpret malicious patterns on the data packets that possess a certain probability. This classification engine can be used as a packet-based classification engine. Not only are the anomalous network traffic detected in these detection parts as in "IDSs," but also uncommon information packets which may be part of "Internet worms / viruses[15].

The packet verifier and the packet-based classification engine are transferred to the decoded packet sequentially. The packet verification verifier controls Protocol Rightness and validates the anticipated protocols's use using the Protocol Specifications such as "TCP / IP" protocol specifications. The package-based classification engine classifies packages into various kinds of maliciousness[16].

Maliciousness is calculated according to the validation values of the packet verifier. The scheme then decides, depending on the probability of sending or deleting the packet to the intelligent detection engine. This detect step is performed to confirm the classification step choice of the Fig. 3 packet in the proposed Intelligent Firewall Packet Detection Components .There should be a certain probability that a malicious code, or a virus location, will be included in a packet that is likely an infected file.

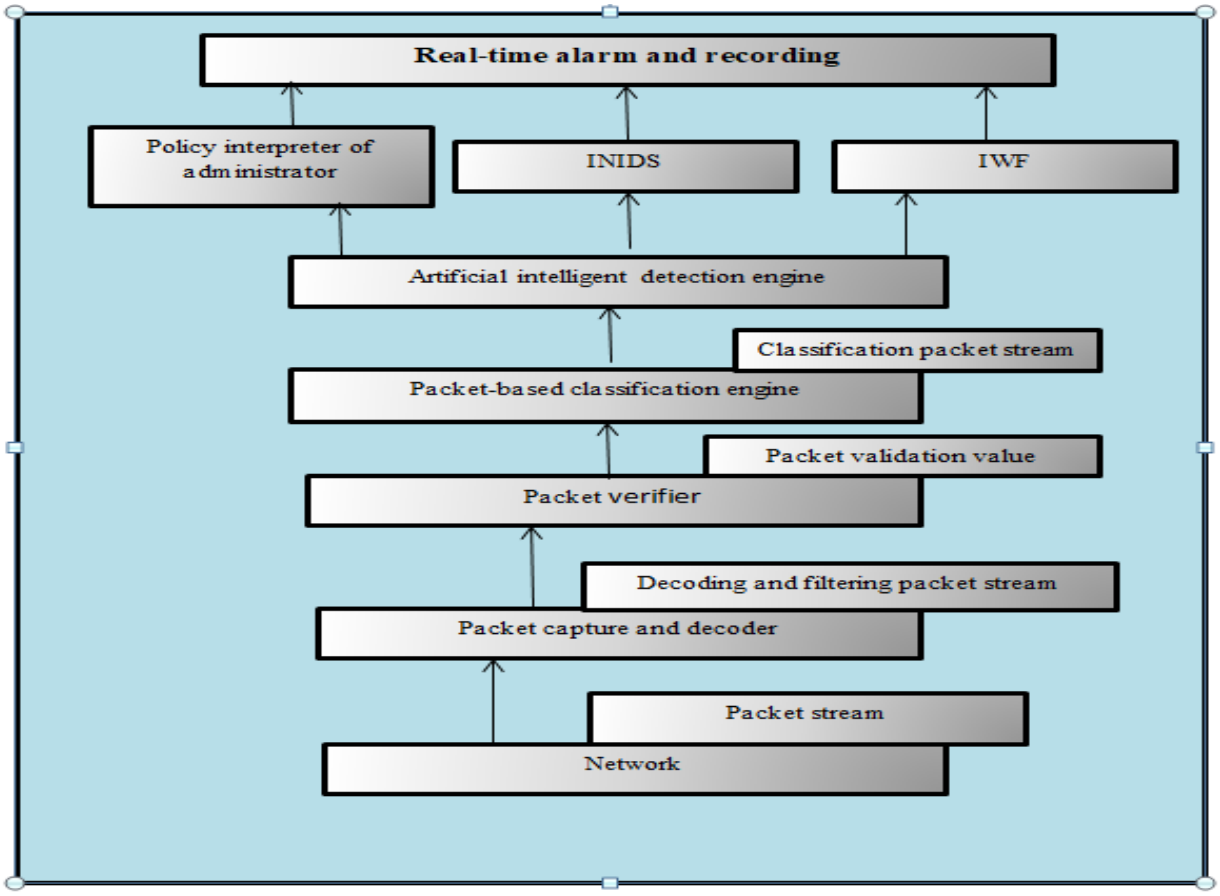

Fig. 3. The Proposed Packet-Based Detection Components

The detection motor therefore, improves the classification outcomes and finds possibly malicious content. The classification engine for packets deals with researching the relationships of packets based on some of the evidence and the intelligent detection engine acknowledges malicious trends based on an uncertain argument (the likelihood of malicious information is high).

The intelligent detection engine addresses malicious packages that are filtered by the classification engine based on the packet and that are highly likely to be malicious.

Finally, the policy interpreter analyzes the data it receives from the two engines and decides on the possibility of a packet containing malicious material and a particular security policy that governs policy interpreter decision whether to drop a packet or allow it to cross the firewall.

3.1.1 Packet Verifier

The aim of the packet verifier is to validate standard submission and validate anticipated procedures, such as protocol detection by anomaly. This is to be covered by the protocols (TCP / IP / ICMP) .

The packet verification will test the packet protocol header portion, verify packet size, verify TCP flags verify the header (TCP / UDP) length , and all packet parameters, analyze and verify TCP protocol type flags and header and of TCP protocol.

The IP Protocol should always be equal or larger than the minimum internet header size (20 octs) and the complete length of a packet should always be larger than its header size in accordance with the Internet Protocol Standard. Testing IP addresses will also be essential because property assaults use the same source and destination IP address.

Under TCP, no TCP source or target can be null, and no TCP flag, for example. Flags for URG and PSH are only available if a packet carries information. The URG and SYN , or PSH and SYN combinations will be invalid, for example. More than one RST , SYN and FIN flags are not valid for any combinations.

Moreover, there is a filtration phase in the packet inspector. Using the filtration process, the packet is removed or allowed into the network in accordance with filtration and policy regulations, which is the classic firewall's packet filter feature. In the construction of a firewall two kinds are used; the driver "Filter-Hook" and the driver "Firewall-Hook." These derivatives are used to store packets and cache them in driver buffers (as shown in Fig. 4. [17][9][7][18]

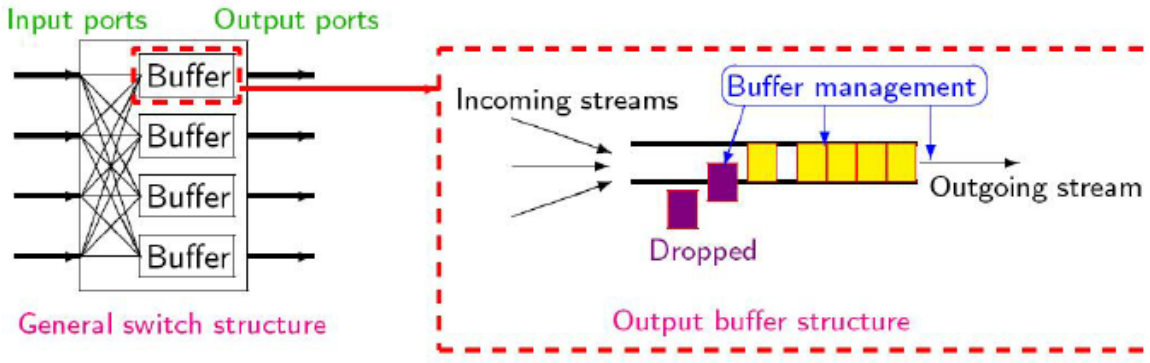

Fig. 4 .The packet buffering layers.[18]

The driver Filter-Hook only enables the system to install one feature filter. If an app uses this functionality already, other applications don't operate; you can install all the required filter features on the Firewall-Hook driver. Each filter function is given priority so that one function (in priority order) is named by the scheme until a function is returned (DROP PACKET). The priority value for each feature in the chain.

received from a Firewall Hook filter function is more complex than that received by the Filter Hook driver ; more similar to the packet structure found in the "NDIS" driver, where the whole packet is collected by a buffer chain as shown in Figure (4).[19]

A feature used to filter incoming packets using the packet filtering method is used in this suggested scheme. Finally, the validation results are sent to the package-based classification motor by this packet verifier. The packet filtration flowcharts are shown in Fig. 5.

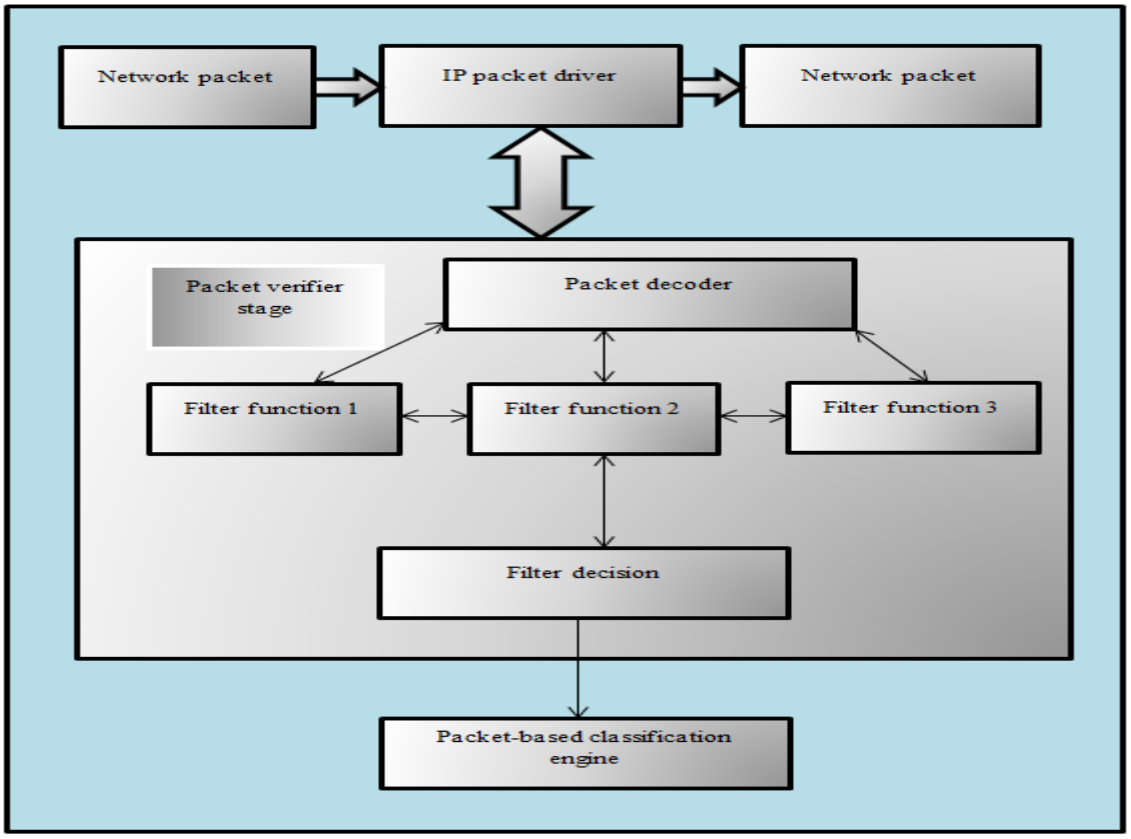

Fig. 5 . The Packet Verifier Stage.

3.2 Intelligent Detection Engine

The ‘Intelligent’ detecting engine handles the filtered packet classification engine that are likely to be malicious. The smart detector engine needs to know to differentiate from ordinary packets abnormal information packets .

This engine does not have to suit the infected part of a program, unlike antivirus software. The anti-virus software has the purpose of identifying a system or file with recognized viruses. The smart detection engine deals with infected files for recognized viruses and worms. The packet-payload can be used in this engine to identify a file worm using context data. Wavelet neural networks WANN are applied to "malicious incoming packet patterns” in the Intelligent Detection Engine”.

The Intelligent Detection Engine addresses infected viruses and worms. The' packet-payload' can be used for detecting file worm based on context data in this engine. The (WANN) input packet patterns is detected by an intelligent detection engine. Instead of viruses or worms, WANN is interested in infected file formats patterns. A virus is a part of the software; it contains a number of documents and as a result of infection changes their forms. when multiple files are infected in one system by a virus program ;Internal files have a virus code in the form of the other virus infected program, The work of intelligent detection engine shown in Fig. 6 [20][21][22][23][24].

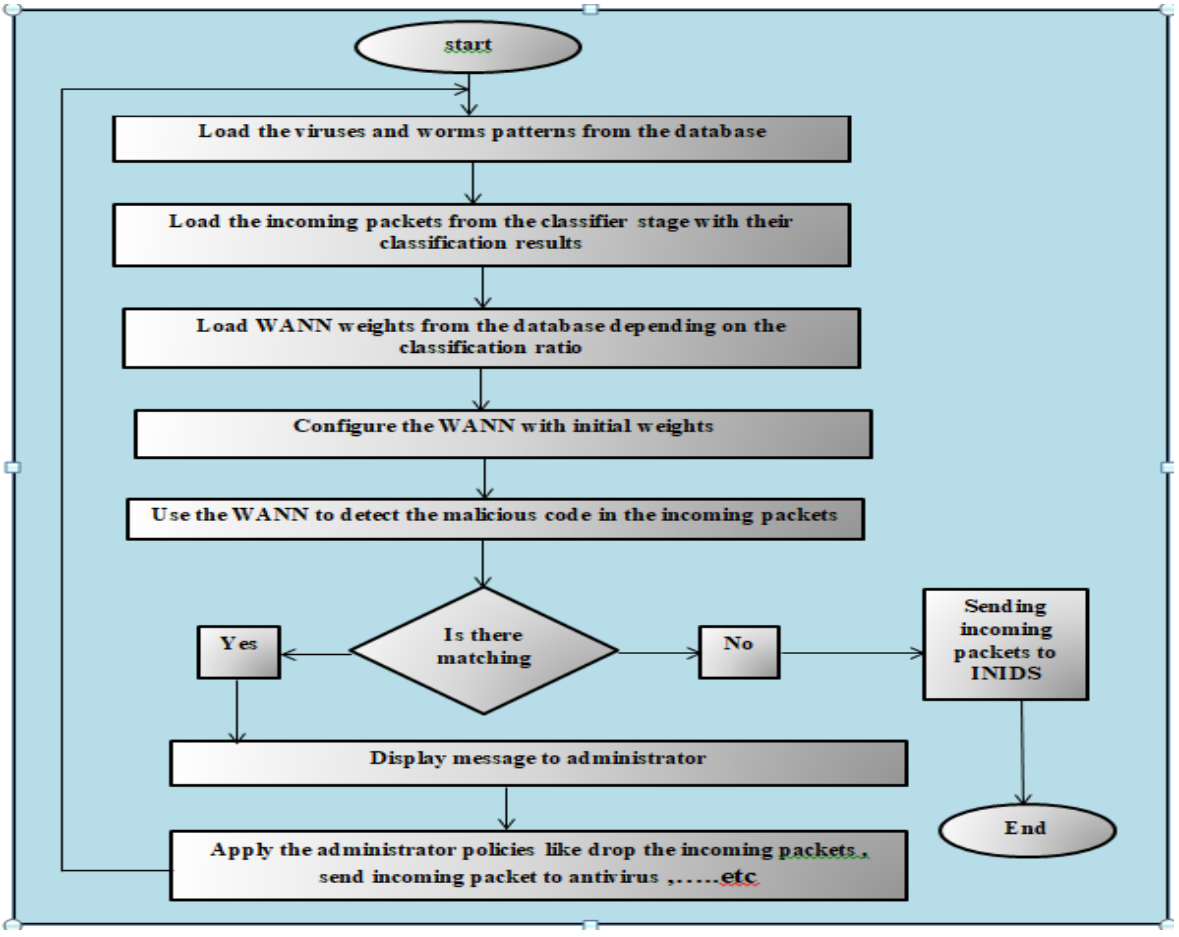

Fig. 6. flow chart of the proposed intelligent detection engine

3.3 The Proposed Intelligent Network Intrusion Detection Subsystem

With computer networks expanding rapidly during the last decade, safety has become a major problem for computer systems. Different methods and techniques for the creation of intrusion detection systems were suggested for "soft computing" in latest years.

The suggested smart intrusion detection via WANN is discussed in this research. The main focus of past researches were the classification of documents in either general class-normal and attack, which suggested research aiming at the solution of a multi-class issue, where the sort of attack is also identified through the (wavelet neural network). The research is based on a study of the WANN and a classification approach to the intrusion.

The amount of concealed layers is taken into account in analyzing different wavelet neural network structures to determine the ideal neural network. In the training stage, an early stop validation method or technique will also be used to improve the generalization capacity of the neural network.
Networks intrusion detection system NIDS design is based on two primary methods. A search for operations which match recognized signatures of intruders or vulnerabilities identified in an abuse-based IDS. And an anomaly-based "NIDS" detects intrusion in search of unnatural traffic in the network. The abnormal pattern of traffic can either be described as the breach of accepted event frequency thresholds or as a user infringement of the legal profile for user normal behavior.
In Fig. 7, the block diagram demonstrates the suggested intrusion-detection intelligent-network subsystem:

- Probation: consisting of host or network traffic; summarizes traffic in statistical factors reflecting network status; and reports to an "event preprocessor" periodically.
- Pre-processor: gets reports from both the lower level (sample and IDAs), converting the data into the statistical model format.
- Statistical Processor: maintains the typical network activity indication model, compares the "event preprocessor" reports to the models indicated and forms a vector motive for feeding into the neural network classification models.
- Classifier of the Neural Network: analyze a' statistical model ' vector motivation to decide whether or not network traffic is normal.
- Post Processor: generates reports to the higher levels, and the results can be viewed at the same time via the user interface.

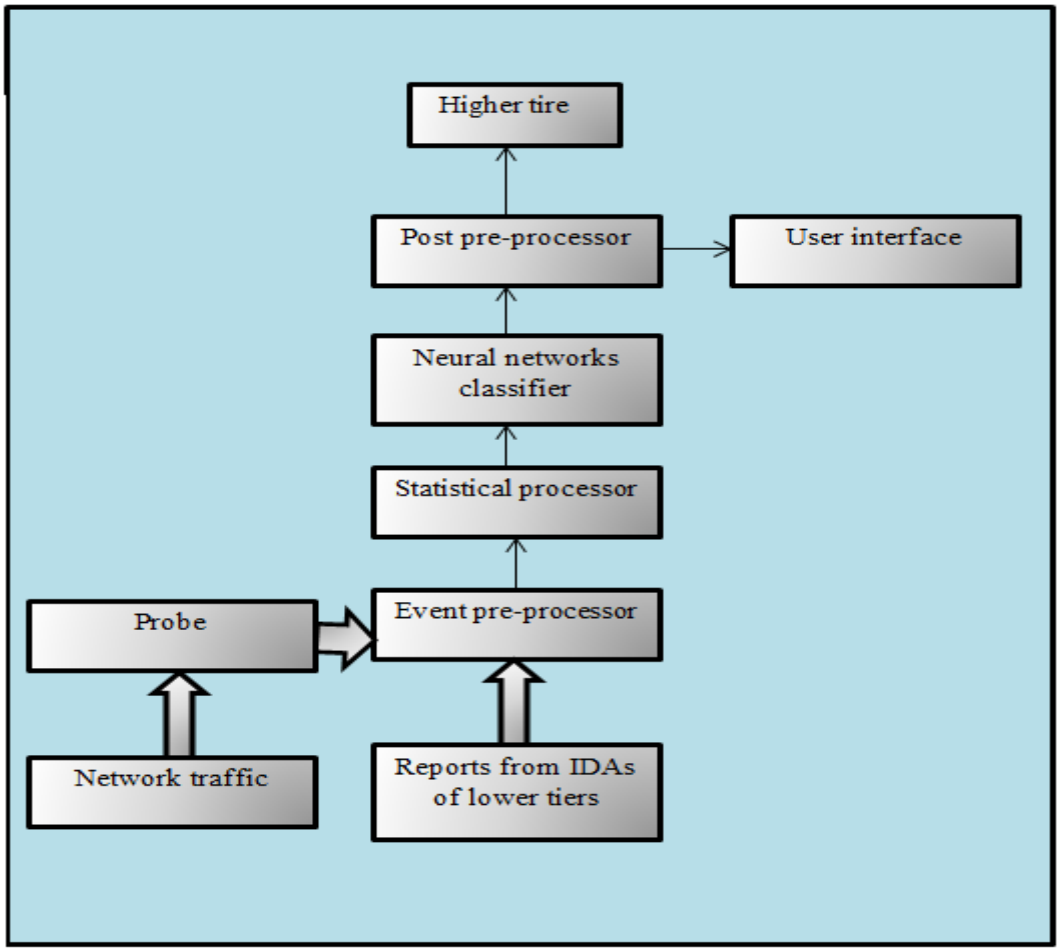

Fig. 7 . The Block Diagram of The Proposed NIDS.

3.4 Intelligent Web Filter

Web filter is a scheme which scans a number of laws on the incoming internet page for a set of regulations supplied by the business or the individual who has installed the web filter that cannot display any or all of it to the user and tests the source or content of the web site[25].
The suggested scheme enables a worldwide or an individual user to block websites that may contain unpleasant publicity, pornography content, spyware, viruses as well as other unpleasant content in the suggested scheme.
The suggested web filter method also offers reporting in order for the installer to see which traffic is filtered and who requested it. In addition, the suggested internet filter blocks the administrator with an alert and a warning message rather than the required page.
While a Web filter can scan some malware, safety advisors also recommend other types of protection such as desktop and network antivirus software installation. As portion of a proxy server and firewall, a suggested Web filter is generally mounted.
The flow chart of suggested intelligent web filter is shown in Fig. 8

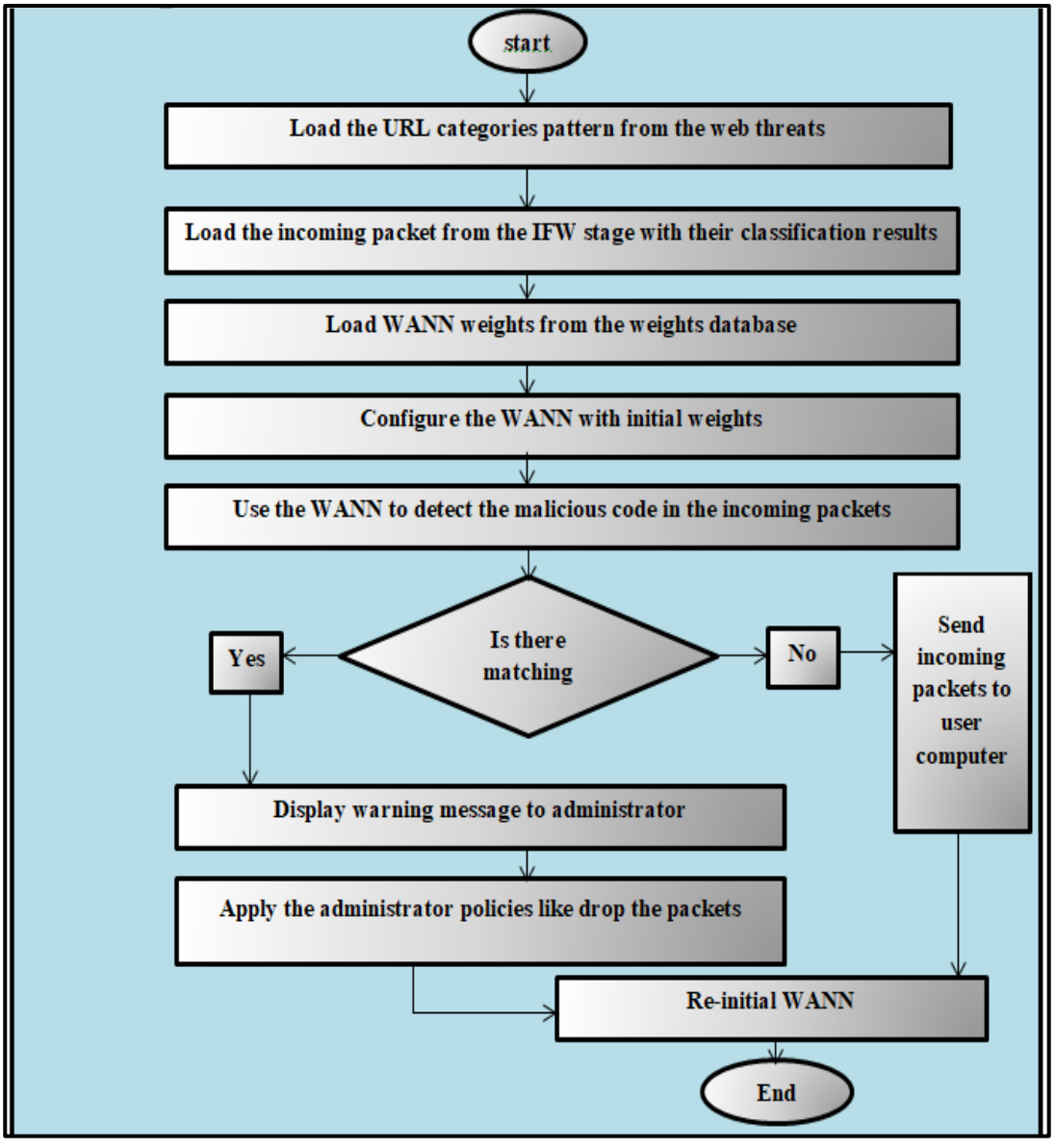

Fig. 8. Proposed Intelligent Web Filter

4. CONCLUSIONS AND FUTURE ENHANCEMENTS

The key idea is the integration into a firewall, intrusion, anti-sip ware and antivirus of an intelligent detection engine, which results in what is termed the "intelligent safety system" .we indicate that this scheme has the ability to achieve the following steps :

1. The smart final reaction approaches are efficient in reducing false-positives and improving "INSS" responsiveness in present complex infrastructure, as well as to the state malicious traffic.
2. Due to its integration of the security methods (in one scheme interconnected) the effectiveness of the system output suggested improved the performance from the classically segregated protection scheme.
3. The scheme that is suggested to know anomalies attacks the structures and behaviors of one AI. In addition, the scheme suggested can improve the amount of assaults after learning.
4. The suggested firewall is capable of identifying threat "like hidden worms and viruses in picture files" in other applications.
5. The Suggested smart approaches include safe communication traffic Management packet analysis content tracking and detection using adaptive packet filters smart co-processors as well as smart network infrastructure detection and reaction.
6. The suggested system capable of adapting the sensor motor and the WANN database to fresh kinds of attacks learned from logging, network traffic and data on network operations, tracking and connections.
7. These techniques are used to decrease the attacking traffic and to improve the efficiency of network facilities.
8. Wavelet transformations are evident from outcomes of the average system rate suggested on neural network learning velocity, neural choices, and neural behavior.
9. With the Wavelet neural network strategy, precision and efficiency are significantly better than the random test, as there is a considerably tiny chance that all defects will be missed.

In order to develop the current research in future, There are two features in the suggested internet filter:
The first is to use the internet filter database to filter the URL. In order to determine the web site URL, the internet filter turns the decoder packet into ASCII code. The internet filter will look up the URL in the database after extracting the URL and will then deter the administrator from warning about malware internet URLs.
Secondly, malware detection is suggested through the use of the malware model of the Wavelet neural network "WANN." The internet filter database also includes 54 models of malware such as spyware. Furthermore the attack scenarios can test and investigates this proposal by any type of dataset which related to intrusion detection system such as CICID or KDD beside other types ,which are contains a multiple kinds of attacks of IDSs.

Conflicts Of Interest

The paper states that there are no personal, financial, or professional conflicts of interest.

Funding

The absence of any funding statements or disclosures in the paper suggests that the author had no institutional or sponsor backing.

Acknowledgment

The author extends appreciation to the kut university college for their unwavering support and encouragement during the course of this research.

References

[1] R. Alsaqour, A. Motmi, and M. Abdelhaq, “A Systematic Study of Network Firewall and Its Implementation 1 1,” vol. 21, no. 4, 2021.

[2] P. P. Mukkamala and S. Rajendran, “a Survey on the Different Firewall Technologies,” *Int. J. Eng. Appl. Sci. Technol.*, vol. 5, no. 1, pp. 363–365, 2020, doi: 10.33564/ijeast.2020.v05i01.059.

[3] T. Abdelghani, “Implementation of Defense in Depth Strategy to Secure Industrial Control System in Critical Infrastructures,” *Am. J. Artif. Intell.*, vol. 3, no. 2, p. 17, 2019, doi: 10.11648/j.ajai.20190302.11.

[4] M. G. Gouda and A. X. Liu, “A model of stateful firewalls and its properties,” *Proc. Int. Conf. Dependable Syst. Networks*, pp. 128–137, 2005, doi: 10.1109/DSN.2005.9.

[5] S. Pozo, R. Ceballos, and R. M. Gasca, “Model-Based Development of firewall rule sets: Diagnosing model inconsistencies,” *Inf. Softw. Technol.*, vol. 51, no. 5, pp. 894–915, 2009, doi: 10.1016/j.infsof.2008.05.001.

[6] T. S. Mohamed and S. Aydin, “IoT-Based Intrusion Detection Systems: A Review,” *Smart Sci.*, vol. 10, no. 4, pp. 265–282, Oct. 2022, doi: 10.1080/23080477.2021.1972914.

[7] F. A. Rafrastara and F. M. A, “Advanced Virus Monitoring and Analysis System,” *Int. J. Comput. Sci. Inf. Secur.* , vol. 9, no. 1, pp. 35–38, 2011, [Online]. Available: http://sites.google.com/site/ijcsis/.

[8] Gary C. Kessler, “An Overview of TCP/IP Protocols and the Internet,” 2019, [Online]. Available: https://www.garykessler.net/library/tcpip.html.

[9] D. E. Kaplan and S. Rajendran, “Firewalls in general relativity,” *Phys. Rev. D*, vol. 99, no. 4, p. 44033, 2019, doi: 10.1103/PhysRevD.99.044033.

[10] S. Aljawarneh, M. Aldwairi, and M. Bani, “Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model,” *J. Comput. Sci.*, vol. 25, pp. 152–160, 2018, doi: 10.1016/j.jocs.2017.03.006.

[11] Z. Trabelsi, S. Zeidan, and H. Saleous, “Teaching Emerging DDoS Attacks on Firewalls: A Case Study of the BlackNurse Attack,” in *2019 IEEE Global Engineering Education Conference (EDUCON)*, 2019, pp. 977–985, doi: 10.1109/EDUCON.2019.8725133.

[12] Z. S. Younus and M. Alanezi, “A Survey on Network Security Monitoring: Tools and Functionalities,” *Mustansiriyah J. Pure Appl. Sci.*, vol. 1, no. 2, pp. 55–86, 2023, [Online]. Available: https://mjpas.uomustansiriyah.edu.iq/index.php/mjpas/article/view/33.

[13] Z. Zhang, “Analysis of Malware Hidden Behind Firewalls with Back Scans,” *2019 7th Int. Symp. Digit. Forensics Secur.*, no. 1, pp. 1–6.

[14] S. Jingyao, S. Chandel, Y. Yunnan, and Z. Jingji, “Securing a Network : How Effective Using Firewalls and VPNs Are ? Securing a Network : How Effective Using Firewalls and VPNs Are ?,” no. March 2019, 2020, doi: 10.1007/978-3-030-12385-7.

[15] Tamara Saad Mohamed and Saad Mohammed Khalifah, “Intrusion Detection Systems: A Revisit of Performance Evaluation Parameters,” *Acad. Int. J. Eng. Sci.*, vol. 2, no. 01, pp. 15–21, 2024, doi: 10.59675/e212.

[16] T. S. Mohamed, “Security and Privacy matters of Grid Computing,” no. November 2014, 2019, doi: 10.13140/RG.2.2.21032.11529.

[17] G. C. Kessler, “An overview of TCP/IP protocols and the internet,” *InterNIC Doc. Dec*, vol. 29, p. 42, 2004.

[18] Z. Zhang and F. Li, “Extra Buffer Resources Improving Competitiveness in Minimizing Energy Consumption,” no. GMU-CS-TR-2010-6, 2010.

[19] X. Li, “A Research and Model of Host-Firewall Based on Windows Hook Technology,” pp. 2892–2895, 2011.

[20] M. Pawlicki, “Neurocomputing A survey on neural networks for (cyber-) security and (cyber-) security,” vol. 500, pp. 1075–1087, 2022, doi: 10.1016/j.neucom.2022.06.002.

[21] J. Yan, H. Zhou, and W. Wang, “Intelligent Network Element : A Programmable Switch Based on Machine Learning to Defend Against DDoS Attacks,” 2025, doi: 10.1007/s10796-024-10577-9.

[22] Y. B. Abushark *et al.*, “Cyber Security Analysis and Evaluation for Intrusion Detection Systems,” *Comput. Mater. Contin.*, vol. 72, no. 1, pp. 1765–1783, 2022, doi: 10.32604/cmc.2022.025604.

[23] Q. Xu, M. T. Arafin, and G. Qu, “Security of Neural Networks from Hardware Perspective: A Survey and beyond,” *Proc. Asia South Pacific Des. Autom. Conf. ASP-DAC*, pp. 449–454, 2021, doi: 10.1145/3394885.3431639.

[24] L. T. Dechevsky and K. M. Tangrand, “Wavelet Neural Networks versus Wavelet-based Neural Networks,” no. November, 2022, doi: 10.48550/arXiv.2211.00396.

[25] T. S. Mohamed, “Analytical View of Web Security and Sophisticated Ways to Improve Web Security,” *J. Phys. Conf. Ser.*, vol. 1530, no. 1, 2020, doi: 10.1088/1742-6596/1530/1/012023.