

# The Performance Evolution of Antivirus Security Systems in Ultradense Cloud Server Using Intelligent Deep Learning

G. Ramesh<sup>1</sup>, J. Logeshwaran<sup>2,\*</sup> and V. Aravindarajan<sup>1</sup>

<sup>1</sup>Department of Information Technology, KLN College of Engineering, Madurai, India

<sup>2</sup>Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India

\*Corresponding author: [eshwaranece91@gmail.com](mailto:eshwaranece91@gmail.com)

**Abstract.** When creating an antivirus, not only the latest security mechanisms are taken into account, but also the needs of users. That's why this antivirus works together at high speed. The program interface allows it to choose the most optimal function. Free delivery allows a large number of users to rate this product. With the help of an intelligent deep learning model, a smart solution was proposed in this article to identify the security threats. It enables rapid detection and efficient treatment of polymorphic and encrypted viruses. Infected archives can now be detected when opened. This helps prevent its software from getting infected again. The program has the ability to create a confidence zone, which allows reducing the scanning time by creating a list of objects subject to scanning. This list should only contain sources that you are sure of. This application is designed to provide reliable protection for your computer. The proposed model allows it to protect its computer from all types of viruses and various Trojans, root kits, worms, and other malicious objects.

**Keywords:** Antivirus, security, high speed, threats, detection, scanning, Trojans.

## INTRODUCTION

If the antivirus blocks sites by mistake, it should not be a mistake. The fact is that in communication or with classmates, where it wants to enter, in reality, they may turn out to be fake [1]. They have almost the same address (one letter changed) and the same content, but they are created by fraudsters to steal passwords [2]. These sites in communication and classmates (and not only) are almost indistinguishable from the real thing. Nodes, avast, and AVG know about them-so they block them to protect it from stealing passwords or viruses [3, 4]. If it fully trusts the reliability of the blocked sites, it can fix this without disabling the antivirus [5]. It can do the same with other antiviruses that block malicious sites. Everyone employs these techniques [6]. It can add files (programs) to exclusions in the same way, so that the antivirus does not block them, only the settings are slightly different (it needs to select other options) [7]. Of course, it is antivirus, but it is better not to do it. Never send SMS [8].

It can dial a phone number, which sometimes it needs, but it can't send SMS in any case. A phone number

is entered so it can retrieve the password [9]. Such activities include classmates, emails, Skype, bank sites and more [10]. There is nothing wrong with this; on the contrary, it is even better because no one can change its password without its knowledge [11]. If in doubt, they warn, though the developers take great care to ensure that their antiviruses do not block trusted sites and programs [12]. They have their own reasons (they protect their interests), then manually add sites and files to the exceptions, using the method described earlier, or disable them for a while, although disabling does not always help [13, 14].

When it changes its antivirus program, it often happens that it faces the problem of complete inability to visit previously accessible sites [15]. Why is this happening? Is antivirus really a virus? Of course not, because here everything is very simple: the antivirus program blocks websites because it cares about the security of its computer! Yes, this problem is solved very simply: in the exceptions it needs to include sites that it has visited before (now the antivirus program does not allow it) [16].

## LITERATURE REVIEW

Before looking for methods to solve problems with network and router settings, check the status of its account with the provider and the reliability of the network cable. This solves the problem in half of the cases [1]. Sometimes, Internet access may be blocked by the computer's own security agents, such as a firewall or antivirus. Define the obstacle. Windows Firewall 8 is very easy-turn it off in the system settings and check the connection. If the network appears, then the problem is detected [2].

If the block comes from an antivirus, it needs to disable the program directly or complete the relevant processes through the task manager. The main function of a firewall is to check data coming from the Internet and block it from causing concern [11]. There are two modes of listing: "white" and "black". White-blocks everything except allowed and black-allows everything except forbidden. Even after that, the full customization firewall needs to set permissions for new applications. There is a special list of programs that are allowed to exchange data with the Internet, and if what it needs is blocked, then it needs to configure permissions for it in this list [17]. In addition, it can set notifications so that if a new application is blocked, it has the option to leave everything as it is and allow access to this program. For example, it can block Internet access to Skype or Google Chrome, or vice versa, leave access only to certain work programs [18].

If it has problems connecting via Wi-Fi, it needs to determine the source of the problem. It can be a laptop, router, or provider. If all devices are connected to the router and work normally with the Internet, the reason is in the laptop. If vice versa, the network cable is connected to the computer and the Internet works, it needs to do the router settings [19]. If all else fails, contact its provider's technical support. If the problem is with the laptop but all the above settings are in order, run system diagnostics for viruses and device activity [20].

## PROPOSED MODEL

The proposed application works several times faster than its competitors. At the same time, even paid antiviruses can be jealous of ensuring security. Encrypted and polymorphic viruses can be detected using deep emulation technology. The use of other technologies used by third-party programs may not provide useful results. Attackers sometimes hide viruses in archives. Most free programs cannot scan rar or zip archives. The proposed antivirus copes well with this task. In 99% of cases, the threat will be detected. When a user accesses any type of file, the antivirus starts scanning it. The same happens with the operating system accessing the files. Thus, system protection is carried out continuously, in real time. If a dangerous file is detected, it will be blocked. An intuitive

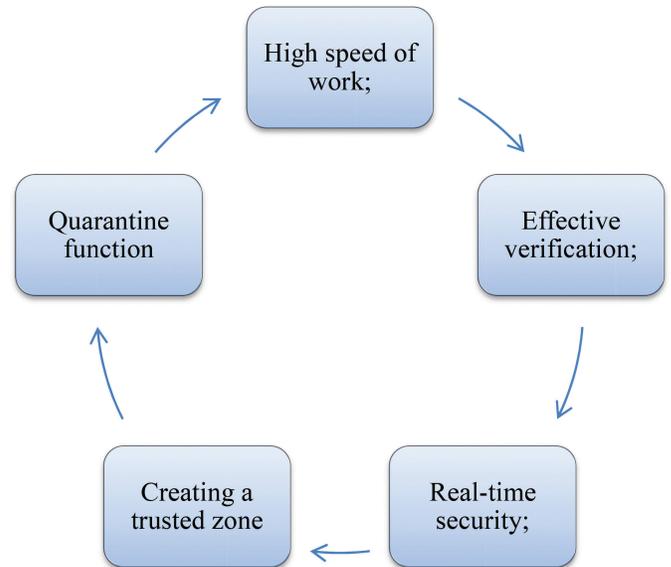


Figure 1. Selection of the optimal interface.

clear interface allows even an inexperienced user to cope with antivirus management. The program allows it to add any applications to the exceptions. Selection of the optimal interface includes the following, as shown in Figure 1.

A function that starts an antivirus function on behalf of another user (this is useful for system administrators and allows them to integrate the entire complex into another infrastructure). Antivirus was created to protect against various types of threats and computer data waiting for users on the Internet or when using unverified programs. It can protect against the following misfortunes shown in Figure 2.

- Viruses
- Trojans
- Worms
- Cryptographic malware
- Polymorph malware

It can find its laptop's MAC address by typing IP configuration/all in the command prompt. Also, the router has speed limit settings for each client, so it can allow the speed to be maximum or limit it to two kilobits per second. The proposed model provides real-time quality protection. This can greatly improve the accuracy of archive tests and uncompiled files. An advanced analysis system allows it to detect all types of malicious files that have not yet been included in the virus database. The latter is updated at least once a day. This is shown in Figure 2.

Therefore, there is no need to constantly remove a useful application from quarantine that is considered antivirus malware. A specially developed mode for optimizing its system resources will allow it to ensure comfortable work even when the antivirus is running. Access to the most common tasks is more conveniently organized. It can fully

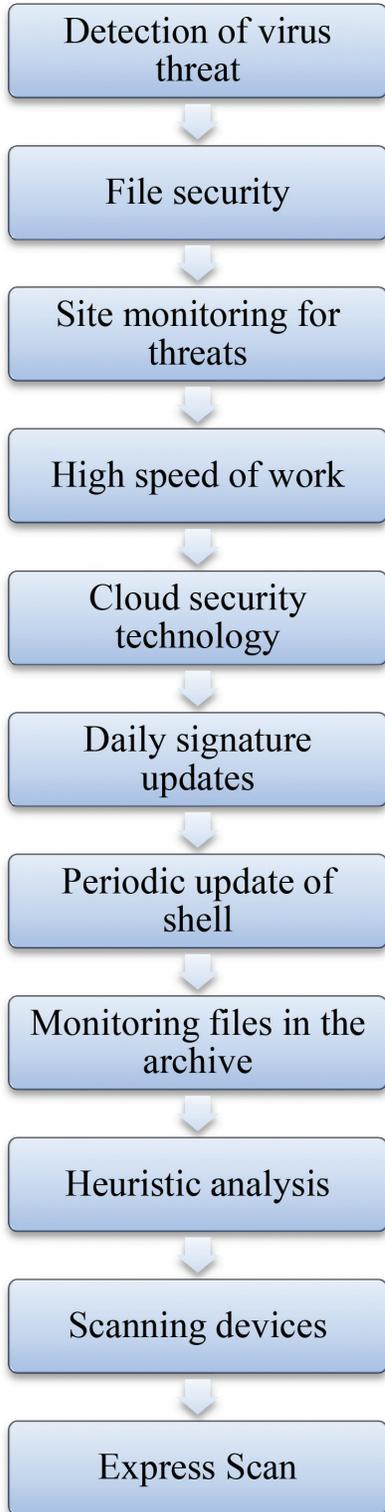


Figure 2. Proposed model structure.

scan its computer or removable media in a limited number of steps with the Express Scan feature. In this mode, the system scans the most dangerous areas. Updating the app is very quick and easy. It is activated by a table and

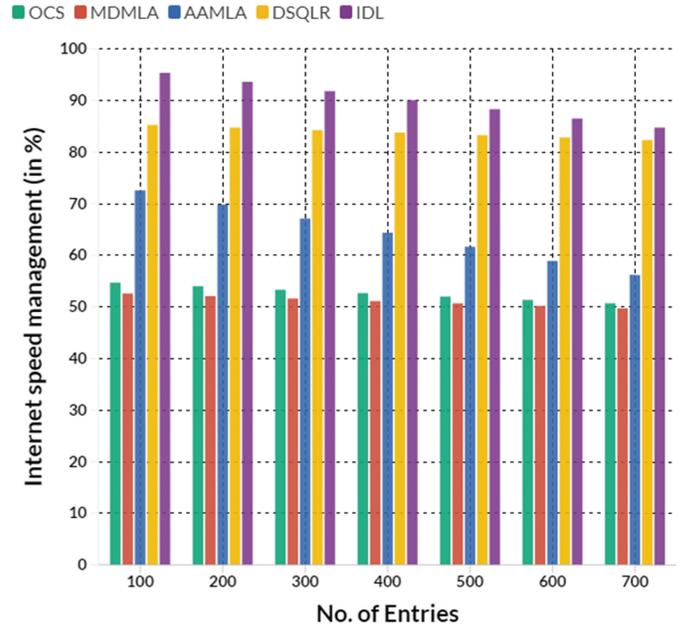


Figure 3. Comparison of internet speed management.

pressing a few interface buttons. The full automation of the program is very efficient and helps detect and remove any threat as soon as possible.

## RESULTS AND DISCUSSIONS

The proposed intelligent deep learning (IDL) was compared with the existing Optimal control strategy (OCS), Malware Detection Using Machine Learning Algorithms (MDMLA), and Adoption, Assessment of Machine Learning Algorithms (AAMLA), and distributed scheduling and QoS localized routing (DSQLR).

### INTERNET SPEED MANAGEMENT

Problems with Internet speed can be a signal for help from the router-maybe it hasn't removed the factory image from it, it's covered by something, or it's overheating for other reasons. As shown in Figure 3, if it does not provide the device with normal ventilation, it will not last long and will be very inefficient. The comparison of Internet speed management is discussed in Table 1.

### ROUTER MANAGEMENT

If it suspects a problem with the router, it should connect the network cable to its laptop or computer to check. If the Internet does not work automatically, create a new cable connection and enter the login and password provided by the provider. It may need to enter additional settings. The comparison of router management was discussed in Table 2.

**Table 1.** Comparison of internet speed management.

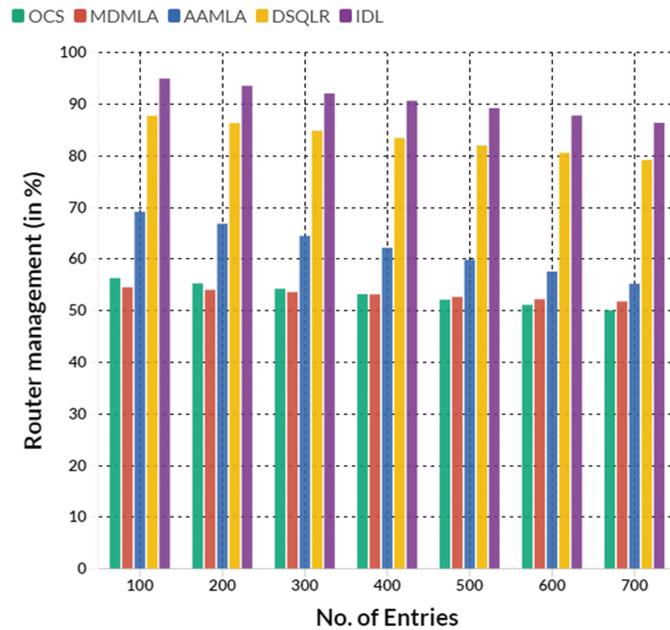
No. of Entries	OCS	MDMLA	AAMLA	DSQLR	IDL
100	54.65	52.58	72.58	85.22	95.35
200	53.99	52.10	69.85	84.74	93.58
300	53.33	51.62	67.12	84.26	91.81
400	52.67	51.14	64.39	83.78	90.04
500	52.01	50.66	61.66	83.30	88.27
600	51.35	50.18	58.93	82.82	86.50
700	50.69	49.70	56.20	82.34	84.73

**Table 2.** Comparison of router management.

No. of Entries	OCS	MDMLA	AAMLA	DSQLR	IDL
100	56.33	54.48	69.15	87.74	94.94
200	55.29	54.03	66.83	86.31	93.51
300	54.25	53.58	64.51	84.88	92.08
400	53.21	53.13	62.19	83.45	90.65
500	52.17	52.68	59.87	82.02	89.22
600	51.13	52.23	57.55	80.59	87.79
700	50.09	51.78	55.23	79.16	86.36

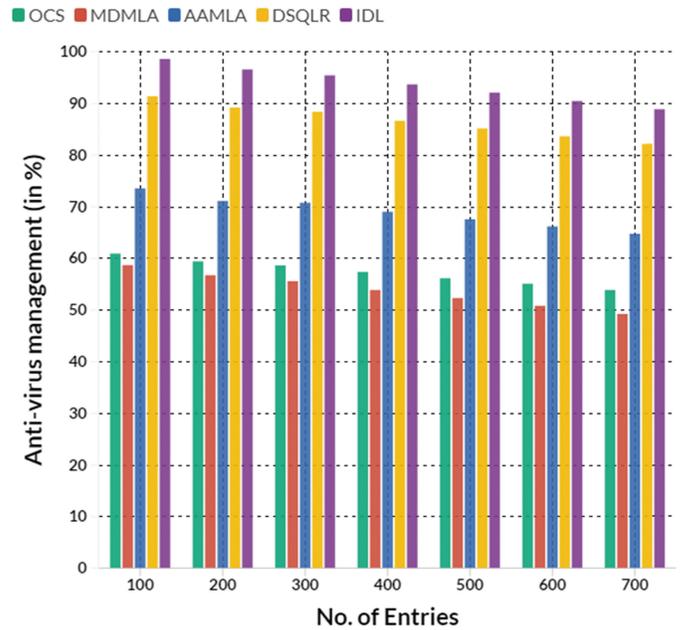
**Table 3.** Comparison of antivirus management.

No. of Entries	OCS	MDMLA	AAMLA	DSQLR	IDL
100	60.92	58.71	73.58	91.41	98.61
200	59.43	56.74	71.16	89.21	96.62
300	58.63	55.61	70.75	88.41	95.42
400	57.37	53.92	69.00	86.68	93.69
500	56.22	52.37	67.58	85.18	92.10
600	55.08	50.82	66.17	83.68	90.50
700	53.93	49.27	64.75	82.18	88.91



**Figure 4.** Comparison of internet speed management.

Figure 4 demonstrates the comparison of internet speed management. Protocols in adapter properties set up a connection through a router occur through the device's web interface. The router sometimes comes with a setup disk, but it can do without it. For the initial setup, it is best to connect the router directly to the laptop, then via an internet cable. Connecting to the mains is done last.



**Figure 5.** Comparison of antivirus management.

## ANTIVIRUS MANAGEMENT

First, immediately after installing and running the program, the antivirus blocks sites it considers dangerous. Naturally, not all sites are classified, but a real antivirus program means that a reinsurer operates according to the rule that it's better to walk around than step on the rack. The comparison of antivirus management was discussed in Table 3.

Figure 5 shows the comparison of antivirus management. The sad thing is that the MBR virus cannot be deleted because it is written on the first line. Boot sector settings. In short, the only way is a complete reinstallation setting, naturally with a complete loss of all data.

## CONCLUSION

If it does not have enough time to wait for a specialist, does not want to spend money, and feels like a confident personal computer (PC) user, then it can try to set up the Internet connection itself, using various instructions and

recommendations. It will take two to three times more time and energy than going to the master, but it will give useful experience in the future. In this age of new technologies, an antivirus for a computer can be compared to a virus vaccine for a person. If its antivirus is not working properly, the PC will not last long. But after installing the antivirus, it will not be able to access the Internet. This condition often occurs in the workplace. A router, with incorrect settings, can distribute Wi-Fi without access to the network. Read on to learn how to properly set up its router. One of the reasons for connecting without a network is to protect the Wi-Fi network from unauthorized access by blocking it by MAC address. It can find out how to fix this problem on the router manufacturer's website, or it can find the list of allowed or blocked addresses in the settings itself and add/remove the address of its laptop.

## REFERENCES

- [1] Raja, S., Logeshwaran, J., Venkatasubramanian, S., Jayalakshmi, M., Rajeswari, N., Olaiya, N. G., & Mammo, W. D. (2022). OCHSA: Designing Energy-Efficient Lifetime-Aware Leisure Degree Adaptive Routing Protocol with Optimal Cluster Head Selection for 5G Communication Network Disaster Management. *Scientific Programming*, 2022.
- [2] Dašić, D., Vuëtić, M., Ilić, N., Stanković, M., & Beko, M. (2021). Application of deep learning algorithms and architectures in the new generation of mobile networks. *Serbian Journal of Electrical Engineering*, 18(3), 397–426.
- [3] Gopi, B., Logeshwaran, J., Gowri, J., & Kiruthiga, T. (2022). The moment probability and impacts monitoring for electron cloud behavior of electronic computers by using quantum deep learning model. *NeuroQuantology*, 20(8), 6088–6100.
- [4] Li, Y., Qiu, L., Zhang, Y., Mahajan, R., & Rozner, E. (2008). Predictable performance optimization for wireless networks. *ACM SIGCOMM computer communication review*, 38(4), 413–426.
- [5] Logeshwaran, J., Malik, J. A., Adhikari, N., Joshi, S. S., & Bishnoi, P. (2022). IoT-TPMS: An innovation development of triangular patient monitoring system using medical internet of things. *International Journal of Health Sciences*, 6(55), 9070–9084.
- [6] Lin, X., Shroff, N. B., & Srikant, R. (2006). A tutorial on cross-layer optimization in wireless networks. *IEEE Journal on Selected areas in Communications*, 24(8), 1452–1463.
- [7] Ramesh, G., Logeshwaran, J., Aravindarajan, V., & Feny Thachil. (2022). Eliminate the interference in 5g ultra-wide band communication antennas in cloud computing networks. *ICTACT Journal On Microelectronics*, 8(2), 1338–1344.
- [8] Wu, Q. & Zhang, R. (2019). Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts. *IEEE Transactions on Communications*, 68(3), 1838–1851.
- [9] Yeshwanth, M. V., Kalluri, R., Rao, M. S., Kumar, R. K., & Bindhumadhava, B. S. (2022). Adoption and Assessment of Machine Learning Algorithms in Security Operations Centre for Critical Infrastructure. In ISUW Springer, Singapore, 2020 (pp. 395–407).
- [10] Logeshwaran, J. & Karthick, S. (2022). A smart design of a multi-dimensional antenna to enhance the maximum signal clutch to the allowable standards in 5G communication networks. *ICTACT Journal on Microelectronics*, 8(1), 1269–1274.
- [11] Johansson, M. & Xiao, L. (2006). Cross-layer optimization of wireless networks using nonlinear column generation. *IEEE Transactions on Wireless Communications*, 5(2), 435–445.
- [12] Jasmine, J., Yuvaraj, N., & Logeshwaran, J. (2022). DSQLR-A distributed scheduling and QoS localized routing scheme for wireless sensor network. In *Recent trends in information technology and communication for industry 4.0*, Vol. 1, pp. 47–60
- [13] Wang, F., Lu, Y., Li, Q., Wang, C., & Bai, Y. (2022, June). A Co-evolutionary Algorithm-Based Malware Adversarial Sample Generation Method. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)* (pp. 1–8). IEEE.
- [14] Ramkumar, M., Logeshwaran, J., & Husna, T. (2022). CEA: Certification based encryption algorithm for enhanced data protection in social networks. In *Fundamentals of Applied Mathematics and Soft Computing*, Vol. 1, pp. 161–170.
- [15] Choudhary, S., & Sharma, A. (2022). Comparison study of Machine Learning Algorithm and Data Science based Machine Learning Algorithm Malware Detection. *Mathematical Statistician and Engineering Applications*, 71(3s), 01–07.
- [16] Logeshwaran, J. (2022, March). The control and communication management for ultra dense cloud system using fast Fourier algorithm. *ICTACT Journal on Data Science and Machine Learning*, 3(2), 281–284.
- [17] Verma, N. K., & Singh, V. (2022). A Rational Approach to Improve Access Time of Apriori Algorithm by Applying Inner Join in a Arm to Redefining Fis in Textual Data. *ECS Transactions*, 107(1), 7749.
- [18] Saravanakumar, K., & Logeshwaran, J. (2016, February). Auto-Theft prevention system for underwater sensor using lab view. *International Journal of Innovative Research in Computer and Communication Engineering*, 4(2), 1750–1755.
- [19] Tian, Z., & Gao, Z. (2022). Multi-carrier Steganography Algorithm Based on Executable Program. In *International Conference on Artificial Intelligence and Security* (pp. 363–372). Springer, Cham.
- [20] Sutharasan, M., & Logeshwaran, J. (2016, May). Design intelligence data gathering and incident response model for data security using honey pot system. *International Journal for Research & Development in Technology*, 5(5), 310–314.