Secure Healthcare Data Storage and Transmission: A Review of Current Technologies and Future Directions

Abhijeet Madhukar Haval[1], Md Afzal[2]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India*

KEYWORDS

Security, Public Health, Deep Learning, Data Analytics, Classification, RBFN.

ABSTRACT

The development of websites, applications, and the first social networks profoundly altered everyone's life and became the catalyst for advancement on a global scale. The days of immovable points, phones, and printing presses are long gone. But is everything really as perfect as it looks? Perhaps the most contentious thing in history is progress. We now have the freedom to express our ideas without fear, connect with individuals around the globe, and access a seemingly limitless amount of knowledge thanks to the Internet. But as time goes on, concerns about the cloudlessness of virtual existence become more and more prevalent; we have been captured by things that do not exist in reality. Apart from the well-known hazards like terrorism and global warming, the growth of the Internet has given rise to entirely unknown and novel perils that have infiltrated our life. We refer to this phenomena as "cybercrime". Any form of criminal activity carried out virtually is referred to as cybercrime. Ten to twenty years ago, this phenomena was known only to specialised specialists. IT industry, and it is currently a worldwide issue. Although everyone and the IT sector receive adequate security measures and equipment, cybercrime is nevertheless increasing at a very rapid pace in parallel. There are several security problems and cyberthreats in the modern world. With new technology emerging daily, we can predict major issues in the road. In this work a Secure Healthcare Data Storage and Transmission in WAN area is discussed.

1. Introduction

Cybercrime is increasing in both the quantity of risks it poses and the suffering it causes to its victims due to the development of new technology and strategies. Since information security, data privacy, and information technology (IT) are all dependent on systems that are based on information, there are security issues in the big data-driven digital world that is driven by social networks, online transactions, stored information, Internet management, and automated processes [1]. Millions of Internet users are affected by a cyberattack that involves service-wide password resets following a network intrusion that significantly exposed usernames and emails with encryption keys. It stands out in particular from previous assaults where a hacker gains access to a database that contains sensitive data. Four months passed during the New York Times cyberattack, which had its origins in China [2]. The data used to gain unauthorised access to employee information has compromised the network [6]. When it comes to data breaches, cyberattacks originate from outside businesses. It concerns users' personal information, national capacity, ethical concerns, and societal interests in addition to the cyberspace itself. "Information security" and "cyber-security" are synonymous phrases. Because their meanings overlap rather than diverge in important ways. Resources are often protected by security from attackers that take advantage of vulnerabilities. The distinction between "cyber" and "information" usually comes down to information vs technology. People and other non-technical components are included in the information security category. As the number of different kinds of cyberattacks rises, so does the necessity for cyber security. Owing to the widespread use, rapid expansion of computer networks, and abundance of necessary apps that people use alone or in groups for both personal and business purposes [11]. Cyberattacks that cause irreversible harm and financial losses in major networks, such as denial-of-service attacks, malware, or any other type of unauthorised access [12]. Software created with the intention of harming users, computers, or files is referred to as malware, or malicious software. Malware includes Trojan horses, spyware, ransomware, adware, and computer infections. It also includes hybrid threats. The sophistication of recent ransomware assaults has increased thanks to the use of artificial intelligence and targeted spear phishing emails. [4]. In this instance, section 1 of the

paper examines the introduction, whereas section 2 examines the relevant literature. Section 3 provides an explanation of the planned work, Section 4 presents the work's outcomes, and Section 5 concludes the project.

2. Literature Review

An intrusion detection system (IDS) keeps an eye on Internet traffic to spot anomalous activity. When it finds such activity, it sends out alerts. It is a piece of software that monitors a computer or network for unauthorised activity or violations of policies. Usually, a Security Information and Event Management system (SIEM) is used to gather information remotely or to report any harmful activity or violation to an administrator [3]. In order to distinguish between harmful activity and false alarms, a SIEM architecture combines multisource outputs and applies alert filtering techniques [5]. Intrusion systems keep an eye on networks for potentially harmful activities, but they are frequently false alarms. Thus, organisations must enhance their IDS after installing them. This guarantees that the intrusion systems may be appropriately configured to recognise typical network traffic in relation to malicious activity. Prevention systems against dangerous activity frequently monitor network packets that infiltrate the device in order to detect malicious behaviour and promptly deliver warning signals. The IDS paradigm was initially presented in 1987 [14] as a monitoring system that identifies questionable activity when it is noticed. Based on these signals, a security operations centre (SOC) analyst or incident response team may look into the issue and take the necessary steps to address the threat [7]. The creation of harmful software, or malware, is a major issue for the design of intrusion detection systems. The complexity of malicious attacks has increased, and the largest obstacle is locating unknown and cryptic malware since its authors utilise various evasion techniques to hide data so that intrusion detection systems cannot identify it. IDS is designed to identify different kinds of malware as soon as feasible, something that a traditional firewall is unable to do. The increasing quantity of computer malware has made the development of improved intrusion detection systems vital. The last couple decades have seen the adoption of machine learning for intrusion detection, and a current comprehensive taxonomy and overview of IDS-related research are required [9]. Many comparable research studies employing the DARPA'99 and KDD datasets have been conducted to validate the creation of IDSs; however, the question of which data mining technique would be more useful has not yet been definitively answered. [8].

3. Methodology

Since intrusion detection systems (IDS) are seen to be among the most important instruments for monitoring harmful activity in cyber security against different threats like DDoS, malware, and spoofing, Figure 1 depicts the architecture of the suggested model. For security purposes, the suggested architecture aids in the detection of threats or attacks that can jeopardise the network's availability, integrity, or privacy. In the architecture, a large number of user devices are linked to the data management system. The server analyses all data sent by user devices using a pre-built database to verify user activity on the inside. On the second hand, online activity via cloud environments—sometimes referred to as outside firewalls—is also taken into account. IDS's monitor is in charge of identifying harmful activity for both types of networks based on train structure by utilising machine learning or artificial intelligence concepts. [13].

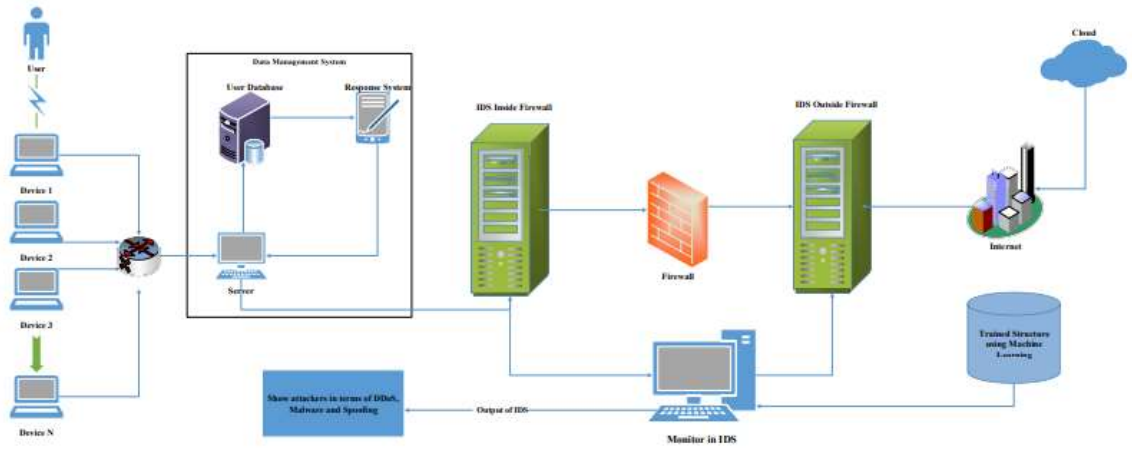

Figure 1. Schematic Diagram of proposed framework

The algorithms for Partcle Swarm Optimisation [10] are employed to ascertain the relative importance of the qualities. Radial-based function networks can be used to locally represent an N-dimensional space. It is executed by the control zone, which is confined by baseline functions. The requirements for this baseline function are calculated by

$$\varphi_j(x) = \exp\left(\frac{\|x-\mu_j\|^2}{2\sigma^2{}_j}\right) \qquad (1)$$

Where $\mu_{\ j}$ reference vector and σ_j *is the* circumstances of the influence field

Each RBFN unit that can be expressed mathematically as a function of a radial basis

$$\varphi_j(x) = \varphi(\|x - x_j\|) \qquad j = 1,2,\dots N \qquad (2)$$

Where N represents the dimension of the preparation model and $(\|x - x_j\|)$is the Euclidean norm of the vector $(x - x_j)$. The J[th] input data point x_j determines the RBF center, and the pattern vector x is added to the input layer. Gaussian function is used in the hidden layer of the network as the radial basis function in which each computing unit is located.

$$\varphi_j(x) = \varphi(x - x_j) = \exp\left(-\frac{1}{2\sigma_j^2}\|x - x_{\ j}\|^2\right) \qquad j = 1,2,\dots N \qquad (3)$$

Where, j is a measure of the width of the Gaussian j[th] function with $x_j$center. All the Gaussian hidden units are usually, but not always, allocated a specific width.

The RBF network structure's mathematical formation has the following mathematical form:

$$F(x) = \sum_{j=1}^{k} w_j\, \varphi(x, x_j) \qquad (4)$$

Where the input vector x is vector dimensional and every hidden unit is defined by the radial base function (x, x_j), where j=1, 2... K. The output function, which is expected to consist of a single element, is defined by the vector w of weight, whose dimensionality is also K.

4. Experimental Results

Cyber-attack detection was the aim of presenting the real-time classification experiment. We used a single Windows 7 Virtual Machine (VM) to run the suggested PSO with RBFN. In our model, the accuracy of the training and testing sets rises with epochs. The training and testing sets lose less data as the epoch gets longer. Accuracy rises and loss falls with the number of training rounds, but eventually it seems to be flat. To determine the ideal epoch value, we tried every ten epochs, ranging from 10 to 50.

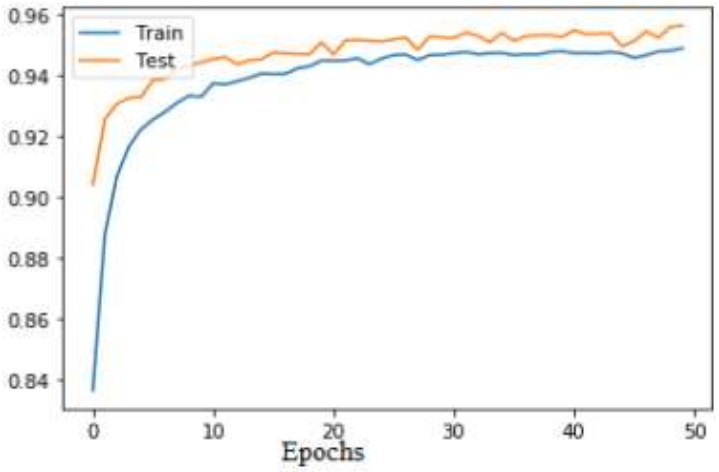

Figure 4. Accuracy of attack detection model

Table 1 displays the accuracy, precision, recall, F-Score, false alarm rate, and misclassification rate for each class as well as the performance of the suggested model on the test dataset.

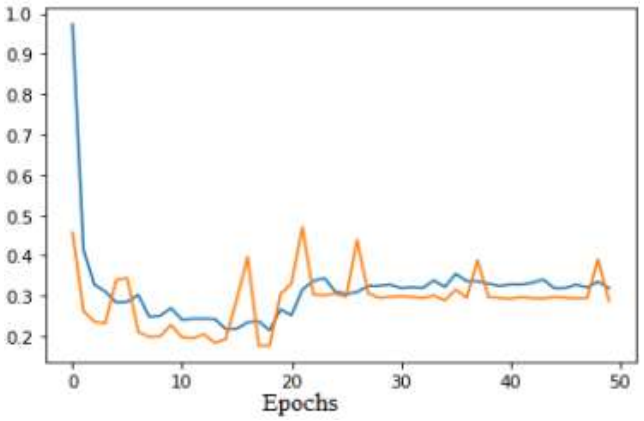

Figure 5. Loss of attack proposed model

Table 1. Performance metrics of attack prediction

Models	**Accuracy (%)**	**False alarm rate**	**Misclassification rate**	**F1-Score**	**Precision (%)**	**Recall (%)**
Normal	97.5	2.0	2.5	0.97	97	89.85
DOS	99.2	0.7	0.8	0.985	97.50	90.25
MITM	96.5	0.95	3.5	0.97	98.15	81.05
Phishing	97	1.2	3	0.985	97.50	90.25
replay	98.5	1.0	1.5	0.97	98.15	81.05

We tested the accuracy of our RBFN model with the most well-established and the newest machine learning model methods. The NIC dataset was used in the experiment to show this with outstanding precision. Table 2 displays the proposed model next to the conventional model.

Table 2. Performance metrics with conventional models

Models	Accuracy (%)	Time complexity
Conventional Algorithm		
MLP	90	5 min
SVM	90.7	2 min
Ensemble method	92	2 min
XG-Boost	93	1.9 min
Proposed- PSO with RBFN		
Normal	97.5	10 sec
DOS	99.2	5 sec
MITM	96.5	7 sec
Phishing	97	2 sec
replay	98.5	2 sec

In order to show the viability and potential of utilising machine learning skills for attack prediction and RBFN for attack detection through data analytics and deep learning, we conducted an experiment.

5. Conclusions

Cybersecurity is currently the most susceptible field. Cyberattacks on wide-area networks, such as denial-of-service attacks and malware, have increased in frequency and impact on critical packets. Although there are now a lot of machine learning-based cyber security apps available to thwart assaults, hackers still manage to get past security measures and reduce the effectiveness of the system. Almost all information, including financial and personal data, is available online, thus safeguarding users against harmful activity is essential. Many studies have previously been conducted to mitigate the negative effects of these attacks, but as these threats evolve, so do the algorithms that are now in place to prevent intrusions. The purpose of this research is to investigate the nature of current assaults by using deep learning to extract important aspects and to suggest an improved strategy to lessen the impact of cyberattacks in wide area networks.

Reference

[1] Durneva, Polina, Karlene Cousins, and Min Chen. "The current state of research, challenges, and future research directions of blockchain technology in patient care: Systematic review." *Journal of medical Internet research* 22, no. 7 (2020): e18619.

[2] Ullah, Ata, Muhammad Azeem, Humaira Ashraf, Abdulellah A. Alaboudi, Mamoona Humayun, and Nadeem Z. Jhanjhi. "Secure healthcare data aggregation and transmission in IoT—A survey." IEEE Access 9 (2021): 16849-16865.

[3] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

[4] Sahi, Muneeb Ahmed, Haider Abbas, Kashif Saleem, Xiaodong Yang, Abdelouahid Derhab, Mehmet A. Orgun, Waseem Iqbal, Imran Rashid, and Asif Yaseen. "Privacy preservation in e-healthcare environments: State of the art and future directions." Ieee Access 6 (2017): 464-478.

[5] Wenhua, Zhang, Faizan Qamar, Taj-Aldeen Naser Abdali, Rosilah Hassan, Syed Talib Abbas Jafri, and Quang Ngoc Nguyen. "Blockchain technology: security issues, healthcare applications, challenges and future trends." Electronics 12, no. 3 (2023): 546.

[6] Madhavi, M., Sasirooba, T., & Kumar, G. K. (2023). Hiding Sensitive Medical Data Using Simple and Pre-Large Rain Optimization Algorithm through Data Removal for E-Health System. Journal of Internet Services and Information Security, 13, 177-192.

[7] Marques, Gonçalo, Rui Pitarma, Nuno M. Garcia, and Nuno Pombo. "Internet of things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: a review." Electronics 8, no. 10 (2019): 1081.

[8] Vaiyapuri, Thavavel, Adel Binbusayyis, and Vijayakumar Varadarajan. "Security, privacy and trust in IoMT enabled smart healthcare system: A systematic review of current and future trends." International Journal of Advanced Computer Science and Applications 12, no. 2 (2021).

[9] Cide, Felip, José Urebe, and Andrés Revera. "Exploring Monopulse Feed Antennas for Low Earth Orbit Satellite Communication: Design, Advantages, and Applications." *National Journal of Antennas and Propagation* 4.2 (2022): 20-27.

[10] Kotenko, I.V., Saenko, I., & Kushnerevich, A. (2017). Parallel big data processing system for security monitoring in Internet of Things networks. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 8(4), 60-74.

[11] Ahad, Abdul, Zahra Ali, Abdul Mateen, Mohammad Tahir, Abdul Hannan, Nuno M. Garcia, and Ivan Miguel Pires. "A comprehensive review on 5G-based smart healthcare network security: taxonomy, issues, solutions and future research directions." Array 18 (2023): 100290.

[12] Yang, Guojie, Mian Ahmad Jan, Ateeq Ur Rehman, Muhammad Babar, Mian Muhammad Aimal, and Sahil Verma. "Interoperability and data storage in internet of multimedia things: investigating current trends, research challenges and future directions." IEEE Access 8 (2020): 124382-124401.

[13] Oleksandr, K., Viktoriya, G., Nataliia, A., Liliya, F., Oleh, O., Maksym, M. (2024). Enhancing Economic Security through Digital Transformation in Investment Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability. Natural and Engineering Sciences, 9(1), 26-45.

[14] Hussien, Hassan Mansur, Sharifah Md Yasin, S. N. I. Udzir, Aws Alaa Zaidan, and Bilal Bahaa Zaidan. "A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction." Journal of medical systems 43 (2019): 1-35.

[15] Krishnamoorthy, Sreelakshmi, Amit Dua, and Shashank Gupta. "Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions." Journal of Ambient Intelligence and Humanized Computing 14, no. 1 (2023): 361-407.