IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

*Research paper*  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12,Dec 2022

# A New Approach in Neural Networks for Cyber Security

**Raghvendra Singh[1], Ramakant Soni[2], Pushpendra Kumar[3], Archana Shukla[4*], Poonam Yadav[5]**

[1]School of Sciences, UP Rajarshi Tandon Open University, Prayagraj

[2]Computer Science and Engineering Department, B K Birla Institute of Engineering & Technology, Pilani

[3]Department of Mathematics, Shri Khushal Das University, Pilibangan, Hanumangarh

[4]Department of Mathematics, Nehru Gram Bharati (deemed to be) University, Prayagraj

[5]Research Scholar, Bhagwant University Ajmer

**Email:** 10singh.raghvendra@gmail.com; ramakant.soni@bkbiet.ac.in; pushpendrasaini22@gmail.com; archanashuklaald@gmail.com

Corresponding author*

**Abstract:** In this paper deals with the Internet Security, today's IT leaders face numerous problems and quick developments. They must safeguard corporate, consumer, citizen, member, and employee data while fending off cyber-attacks. Intrusion Detection System (IDS) is a mature technology architecture that is primarily designed to safeguard the network from external cyber-attacks. With the growth of the Internet and the evolution of cyber-attacks, it is more vital than ever to build new cyber security tools, especially for Internet of Things (IoT) networks. This study presents a thorough examination of the use of deep learning (DL) technologies in cyber security. After that, we show how learning differs from deep learning. Furthermore, a description of current cyber-attacks in IoT and other networks, as well as the efficacy of DL approaches for managing these attacks, is offered. In addition, investigations highlighting the DL approach, cyber security applications, and dataset sources are described in this study. According to our findings, the restricted Boltzmann machine (RBM) achieves a classification accuracy of 99.72 percent when applied to a bespoke dataset, while the long short-term memory (LSTM) achieves a classification accuracy of 99.80 percent for the KDD Cup 99 data set. Furthermore the value of cyber security for dependable and practical IoT-driven healthcare systems is discussed in this essay.

**Keywords:** Internet security, RBM, Intrusion detection system, Cyber threats,

**Introduction:** In the Organizations are finding it difficult to protect their digital assets and intellectual property. According to recent surveys, external hacking is the leading cause of data loss in the corporate world. Organizations must take reasonable precautions to prevent data loss or leakage. Unchecked IT cyber security risk factors that go unaddressed for too long which happens in practically every business are frequently the source of unanticipated cyber-attacks. Intrusion Detection Systems (IDS) are primarily used to secure corporate networks these days. To identify all attempted intrusions and safeguard the organisation from the attack, as IDS is highly recommended. Cyber security refers to the collection of techniques and technologies used to protect networks, software, and data from attacks. Cyber defence mechanisms are available at the network, data, host, and application levels. Firewalls, intrusion detection systems, intrusion prevention systems, and other cyber security measures are always active at each end to detect security breaches and thwart attacks. Nonetheless, as the number of systems connected to the Internet grows, the risk of cyber-attacks grows as well. Cyber security is becoming more critical than ever with the use of Internet of Things (IoT) networks. Many security vulnerabilities exist in

ISSN PRINT 2319 1775 Online 2320 7876

*Research paper*  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12,Dec 2022

computer networks, including IoT. Some attacks can be easily controlled because they follow a pattern. Attackers, on the other hand, are developing zero-day exploits, which launch an assault as soon as a flaw in the system is discovered. Such an attack has never been seen before, and it has the potential to harm the computer system before the problem is resolved. Furthermore, the system must be safeguarded not just from external threats, but also from internal threats, such as the exploitation of permitted access by an individual or an entity claiming to be a part of the business.

The most difficult challenge is identifying the indicators of a compromising system throughout the attack's lifecycle, which may contain relevant signs of a prospective attack in the future. However, because to the vast amounts of data generated on a constant basis by a large number of cyber-enabled gadgets, this may prove to be a challenging task. Information and event management (SIEM) is a scheme that collects a large amount of data from cyber defence systems, which can sometimes overflow the specialists in security with event warnings.

In the field of security, hybrid detection combines anomaly detection with misuse detection. This system is primarily used to reduce the rate of false-positive values associated with anonymous attacks while simultaneously increasing the rate of detection associated with recognised intrusions. Deep learning (DL) approaches have not been discussed in previous reviews, such as those in which machine learning (ML) applications for the solution of cyber-related problems were discussed, but those articles did not specifically include deep learning (DL). Some papers demonstrate how to use DL methods for cyber security purposes. However, there are several limitations to the uses of these methodologies in the field of cyber security.

**Review of Literature:** Karan and Varinderjit have been working on a review article on security vulnerabilities in virtual private networks (VANETs). They have examined the increased interest in virtual private networks (VANETs) in their article, but they have also raised a number of security problems. Many of these security vulnerabilities were prevalent in wireless ad-hoc networks at one time or another. However, the novelty of moving objects communicating with one another in VANETs creates a new set of outside attack challenges that must be addressed. These computers in the networks are subjected to a variety of attacks on a daily basis, and their work provides a complete description of the types of attackers and attacks that they encounter. As previously stated, the methodologies established for network security in MANETs are no longer relevant for VANETs due to the severe mobility limits that these networks face. The metrics of jittering, packet losses, delay, and throughput have, in an interesting twist, been elevated to the status of service parameters. The hierarchy of networks, starting with wireless networks and progressing through mobile networks and finally MANETs and VANETs, has been clearly laid out. The Driver-Vehicle Model (DVM) and the Traffic-Flow Model (TFM). In their work, they have discussed communication and application models in detail. In addition, six different types of security requirements and five different types of security difficulties have been described. A collection and presentation of issues related to broadcast tampering, including denial of service and key and certificate replication attacks as well as key and certificate spoofing and tunnelling concerns have been assembled and presented in their respective works. The solution to the security difficulties and obstacles mentioned above has been presented as keeping an authenticator on the central server, authenticating in groups, and developing a plausible protocol for functioning outside of the range of the network. The study was published in the fourth volume of the International Journal of C.S.E. in 2016.

Scientists Robshaw and Lisa Yin, who were working on cryptosystems that implemented security through elliptic curve algorithms, made scientific recommendations to improve public key crypto systems. They began by reviewing the fundamental history of the public use of cryptographic technology. They studied the similarities between RSA and the elliptic curve, as well as the academic applications of both techniques. Aside from that, this study includes details on the design of elliptic curve DSA and Curve Encryption for academic purposes, as well as a discussion on practical future advancements. The practical security difficulties with elliptic curve discrete algorithms, which were previously thought to be difficult to breach, have also been addressed. The implementation and performance analysis were given in a straightforward and easy-to-understand academic manner. Additionally, the paper includes a comparison table between ECDSA, RSA, and discrete logarithmic systems in terms of their performance on the parameters of encryption, decryption, signature, and verification. Following that, the practical

ISSN PRINT 2319 1775 Online 2320 7876

*Research paper*  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12,Dec 2022

challenges associated with adopting the aforementioned standards were discussed, with the conclusion recommending business applications. At the end of the study, they leave the topic of whether the elliptic curve cryptosystem is more secure than many other security techniques open for discussion.

In 2019, M.S. Sheikh, J. Liang, and W. Wang completed a thorough assessment of security services, attacks, and applications for VANETs, which was published in IEEE Spectrum. In their presentation, they provided a comprehensive description of the VANET architecture as well as the communication standards, features, and security protocols that are employed in VANETs. In this work, they also discuss numerous attacks on the availability, secrecy, authentication, data integrity, and non-repudiation of a system's information. They also talked about other types of assaults, such as malware, jamming, eavesdropping, Sybil, replay, message tempering, social attacks, and so forth. Additionally, they provided a brief overview of the authentication systems used in VANETs, such as ID-based signature, group signature, and certificate signature, as well as asymmetric cryptography, ID-based cryptography, and symmetric cryptography, among others. Hung Yu Chien, an IEEE member, has been working on alternative Digital Signature techniques that do not rely on hash or message redundancy in any way. The purpose of this study was to protect against Forgery Attacks, which were proposed by Chang and Chang's while working on digital signatures and were successfully implemented. During that time, the work piqued the curiosity of all security designers, who focused their efforts mostly on hash functions that were conventionally available to protect systems from outside attacks. Hung's paper also included examples of assaults that were in use in 2006, as well as examples of security systems that were vulnerable to a significant degree. The paper presented message redundancy and one-way hashing, as well as a full description of Chang and Chang's signature scheme, which defined the distinct phases of signature generation, verification, and forgery attacks in greater detail than previous work.

In the end, Hung stressed the importance of new cryptographic protocols and the necessity of developing new protocols in order to address cryptographic difficulties. The work has been published in Communication Letters of the IEEE, volume ten, serial five, summer 2006, and is available online. [36] Kritika and Prabhat from the Indian Institute of Technology Bhopal researched different cryptographic methods that are utilised in different vehicular ad-hoc networks for safe communication among different nodes. This comparative research was published in the IJIRCCE's volume four, issue eight, which was published in the month of August 2016. It was published in the month of August 2016. The authors began their research with an interest in driverless vehicles as a starting point. They took into consideration the information supplied and received by roadside units and vehicles travelling in front of us, following us, and arriving from the opposite direction. There were three types of probable attacks to consider. One comes from vehicles travelling in the same direction as the first, the second comes from vehicles moving in the opposite direction, and the third comes from outside assailants who were keeping an eye on these vehicles. Using classic cryptographic methods implemented in MANETs and VANETs, the authors have demonstrated the security and dependability of all of the schemes, and they have identified the techniques that provide privacy and security for automobiles. The pairing in constant numbers, as well as multi point computations, had also been worked on, and their results were independent of the amount of text packets used. In the final section, the findings of eight distinct encryption strategies were provided, along with the IEEE protocols that were used to implement them. Based on the results, the decryption pattern of RSA was recommended as the best, while ECC, ECDSA, and RSA were all good and easy to mimic alternatives.

Sandhya and Rakesh also worked on securing message communication, and their work was published in the International Journal of Information Technology and Knowledge Management in the second part of 2010. The authors investigated the role played by Digital Signatures and attribute-based cryptography in the advancement of science. The investigation into radio interfaces for on-board equipment was the first step in the process. The focus was on the fact that no roadside unit is capable of gathering private information about automobiles. The work was particularly concerned with the connection between digital signature algorithms and attribute-based cryptography approaches. Probably the most interesting aspect of this paper is that the authors have provided specifics on the hardware that is utilised in VANETs, such as event data recorders, Temper Proof devices, and the implementation of public key infrastructure. In addition, the Electronic License Plates were adopted and made

ISSN PRINT 2319 1775 Online 2320 7876

*Research paper*  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12,Dec 2022

available to other researchers. Identity-based encryption systems, their operation, and an attribute-based encryption scheme with key pair and cypher text policies were all discussed in depth throughout the presentation. Several attribute-based cryptographic techniques for message authentication were evaluated and compared on the basis of their Dynamicity, i.e. whether the characteristics are dynamic in nature or not, as stated in the papers in question. The researchers talked about the future prospects of various cryptographic algorithms and how they might be improved.

A new survey conducted by Vinh and Ana of France, which was published in 2014. The effort involved the investigation of attacks and their corresponding countermeasures in connection with 23 different automotive adhoc networks. The study was conducted only for the purpose of demonstrating that VANETs are an easy target for attackers and that such attack can result in network corruption. The research revealed the fundamental on-site structure of VANETs, as well as the types of emergencies that must be dealt with. The attack targeted all of the major research publishers, including Elsevier, Wiley, ACM, Springer, and others, and collected a massive data set of attack data for the years 2011-13. In their work, they discussed malicious, rational, active and passive, local, extended, and monitoring attacks, among other things. Following that, the security requirements of VANETs were investigated, with the integrity, availability, privacy, trace-ability, revocability, and confidentiality issues all being considered in detail. Bogus information, Bush telegraph, imitation attack, and masquerades have all been discussed in detail. A detailed explanation of the damage caused by GPS spoofing, disguised cars, illusion attacks; ID disclosures; and tunnel attacks was provided, along with appropriate numbers. A list of the top twelve attacks, as well as the type of attacker, the security codes that were violated during these assaults, and the class of attacks, is included in the last section of the report. Overall, the study can be given as a foundation for any field researcher interested in the subject matter.

Manish, Nanhay, and Ram Shrinagar of the AIACTR in New Delhi have also begun work on security issues, challenges, and solutions in the context of the organization's mission. Their work did not reach the same level of completion as Vinh and Ana's, but they diverged in the opposite direction, focusing on a variety of assaults such as Ariadne, ndm, sead authenticated routing, and so on, with corresponding remedies being proposed. In 2013, the International Journal of New Science and Technology (IJNSA) published their study. A specific short-range communication system running at 5.9 GHz and based on IEEE 802.11 has also been proposed by the researchers. The protocols for car-to-car communication and network-on-wheels communication, as well as the availability of spectrum, have been discussed. A comparison has been made between VANETs' technological hurdles and MANETs' technical challenges in terms of restrictions, tolerance issues, and key distributions. Suggestions have also been offered regarding various security concerns. A study about fuzzy theory, optimization techniques, supply chain management and inventory management discussion by (43-75).

**Artificial Neural Network in Network Security:** The artificial neural network is becoming increasingly essential in the field of network administration. The majority of the research in the field of intrusion detection systems makes heavy use of artificial intelligence techniques in order to create, deploy, and improve security monitoring systems. According to studies, current anomaly detection intrusion detection systems (IDS) are unable to achieve an adequate detection rate while also producing a low number of false alarms. Here, the advantages and disadvantages of commercial and research tools, as well as a new method to improve false alarm detection in intrusion detection systems (IDS) by employing a neural network approach are discussed. The main differences between ML and DL are as follows:

**a)** The performance of DL models is not significantly better than the performance of classical ML models for small-scale data volumes, as shown in Figure 1. The reason for this is that deep learning models require a significant amount of data in order to interpret the data completely. Traditional machine learning algorithms, on the other hand, rely on well-established rules.

**b)** It is possible to consider the graphics processing unit (GPU) to be crucial hardware for correctly training the deep learning models. Because DL models necessitate a large number of matrix operations, the GPU

ISSN PRINT 2319 1775 Online 2320 7876

*Research paper*  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12,Dec 2022

is primarily used to optimise matrix procedures. Traditional machine learning algorithms, on the other hand, do not typically necessitate the use of high-performance machines equipped with GPUs.

**c)** In feature processing, the method of inputting domain knowledge into a feature extractor in order to reduce the complexity of data is referred to as feature extraction. Due to the fact that patterns are typically produced during feature processing, ML and DL algorithms perform significantly better. This stage, on the other hand, is time-consuming, and specific knowledge is required in this situation. The quality of the features (pixel values, textures, forms, and positions, among other things) extracted is critical to the performance of most machine learning models.

The attempt to infer high-level characteristics from personal data in an open manner is a significant difference between classic machine learning and deep learning methods. As a result, DL reduces the amount of time spent designing by focusing on extracting features for each problem. d) Execution time: Due to the large number of parameters in a DL model, a significant amount of execution time is required to train it. The training phase is likewise more time-consuming. On the contrary, training a machine learning model takes only a few seconds to a few hours of execution time (as opposed to days or weeks). The time required during the testing stage, on the other hand, is the polar opposite. When compared to some ML models, DL models require significantly less testing time.

**Recurrent Neural Network:** RNN (recurrent neural network) is a subset of neural networks that is connected between nodes and forms a directed graph. It is at this point that the network is in its internal state. It enables the demonstration of dynamic sequential behaviour. They handle arbitrary sequences of input using their internal memory, and the signal goes both forward and backward through the network as a result of the network's creation of loops.

RNNs are typically more difficult to train than other types of neural networks since the gradients have vanished. However, as a result of advancements in architecture and training, a variety of RNNs have emerged. This model is easier to train than the previous one. It was Hochreiter and Schmidhuber in 1997 that introduced the long short-term memory (LSTM), which was an upgraded version of the RNN system. LSTM is bringing about a sea change in speech recognition, and it has set a new standard for several older models in some speech applications by breaking records. It is introduced in order to address the short-term memory problem of RNNs. The LSTM units are connected to the scenario in the temporal stage that follows. A memory cell is a structure of the units that store information and are used to accumulate information.

**Convolution Neural Network:** A convolution neural network (CNN) is a type of deep neural network that processes and analyses visual imagery input. It is a component of deep neural networks. If a colourful or greyscale image is used as an input, the image will be saved as pixels, similar to a 2D array, as shown below. Additionally, CNNs are used for the management of audio spectrograms with 2D arrays, which is another application. The CNN model, on the other hand, is composed of three types of layers: classification layers, pooling layers, and convolution layers, to name a few. Figure 4 depicts a cartoon representation of CNN.

**Generative Adversarial Networks:** GANs are used in unsupervised machine learning, in which two neural networks compete against one another in a game of zero-sum to see who can outperform the other. Good fellow's work serves as an introduction to it. The block diagram of GAN is depicted in Figure 5. By utilising input data, the generator generates output data that has characteristics that are comparable to those of real-time data. The discriminator then analyses the real data to determine if the input is genuine or fictitious.

**Recursive Neural Network (RNN):** Recursive neural networks are neural networks that connect a number of weights in a recursive manner. It accepts a variety of inputs. At initially, the major two inputs are treated as if they were a single entity in the model. The output of a node is therefore considered to be an input for the node that follows it. This type of model is used in many applications such as natural language processing and image segmentation.

ISSN PRINT 2319 1775 Online 2320 7876

*Research paper*  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12,Dec 2022

**Comparison between Shallow Learning and DL:** This section presents a quick comparison of deep learning algorithms and shallow learning algorithms, respectively. DL is composed of numerous layers. Apart from that, in Deep Learning, a deep network contains multiple hidden layers, whereas shallow neural networks normally have only one hidden layer. Apart from the fact that the neuron layers are linked together by adaptive weights, the neighbour network layers are also frequently linked together. Shallow network design, on the other hand, can be divided into two types: supervised and unsupervised. In supervised learning, the labels are kept secret until the work is learned. Furthermore, feature extraction is accomplished on an individual basis.

Because of the various hidden layers present in this type of DL model, it is able to extract higher-level features from the raw input data. It is necessary to distinguish between the input layer and the output layer on multiple levels; the output layer is regarded to be of higher level, whereas the input layer is considered to be of lower level. Higher-level concepts are defined as a result of the definition of lower-level concepts. Despite the fact that feature extraction may be accomplished from the first few levels of a DL network. Unsupervised, hybrid, and supervised DL architectures are the three types of DL architectures. Because shallow neural networks include only one hidden layer, advanced feature extraction must be performed individually in order to avoid overfitting the network. Deep networks, on the other hand, are capable of learning. However, even with high processing power, numerous GPUs are required for deep learning approaches, and training DL models takes an inordinate amount of time.

**Conclusion:** It has been determined that neural networks perform well in three cyber security use cases: Android malware categorization, incident detection, and fraud detection, according to this article. Additional classical machine learning classifiers are employed in conjunction with this one. No matter what the situation is, the performance of NNs is superior to that of the standard machine learning classifier. The same architecture, on the other hand, is able to outperform the other conventional machine learning classifier across the board in all use scenarios. In order to improve the reported outcomes of NNs, it is necessary to promote training or to stack a few extra layers on top of the already existing designs. This will continue to be a direction for future development in the same way that it has been. We can see from those trials that a neural network that has been created and trained is capable of correctly classifying individual data packets. Also, we can claim that a higher number of neurons in the hidden layer has an impact on the sorting quality of the neural network; nonetheless, it appears that the number of 40 neurons in the hidden layer is the optimal amount in this case. This is a really complicated issue, and there is still a great deal of work to be done. Only a small portion of the larger problem has been addressed by this study. We will be able to solve a variety of problems in the next weeks. Propose, for example, a neural network that is substantially larger and is capable of classifying incoming packets into more than one category. Afterwards, we can build on the model by incorporating other NN that would look through the data stream for other anomalies. We may probably alter this model to employ a different form of neural network, such as a type of the Kohonen network, to achieve the desired results.

**References:**


1. Bharati, S.; Podder, P.; Mondal, M.; Robel, M. and Alam, R.; Threats and countermeasures of cyber security in direct and remote vehicle communication systems. Journal of Information Assurance & Security. 2020, 15(4), 153-164. 2020.
2. N. Vanets, “A Survey of Security Services , Attacks ,” 2019
3. Berman, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L. A Survey of Deep Learning Methods for Cyber Security. Information 2019, 10, 122.
4. Torres, J.M.; Comesaña, C.I.; García-Nieto, P.J. Machine learning techniques applied to cybersecurity. Int. J. Mach. Learn. Cybern. 2019, 1–14.
5. D. A. Hahn, A. Munir, and V. Behzadan, “Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges,” IEEE Intell. Transp. Syst. Mag., no. May 2019, pp. 2–17, 2019.
6. H. Talbot and R. Beare, “Mathematical Morphology,” Mathematical Morphology, 2019. [Online]. Available: https://homepages.inf.ed.ac.uk/rbf/HIPR2/matmorph.htm.

 


7. W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," Symmetry (Basel), vol. 11, no. 2, p. 141, 2019.
8. M. Joshi, B. Mazumdar, and S. Dey, "Security Vulnerabilities Against Fingerprint Biometric System," pp. 1–27, 2018.
9. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access 2018, 6, 35365– 35381.
10. T. Rathimala, R. Francis, and M. Kamarasan, "Application of Neural Network Based Data Security in to LFC of a Two Area Power System," vol. 7, no. 2, pp. 19–23, 2018.
11. R. Al-Mutiri, M. Al-Rodhaan, and Y. Tian, "Improving vehicular authentication in VANET using cryptography," Int. J. Commun. Networks Inf. Secur., vol. 10, no. 1, pp. 248–255, 2018.
12. J. Hertz, A. Krogh, R. G. Palmer, J. Hertz, A. Krogh, and R. G. Palmer, "The Hopfield Model," Introd. to Theory Neural Comput., pp. 11–41, 2018.
13. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.; Du, X.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. arXiv 2018, arXiv:1807.11023.
14. X. Wang, S. Li, S. Zhao, Z. Xia, and L. Bai, "A vehicular ad hoc network privacy protection scheme without a trusted third party," Int. J. Distrib. Sens. Networks, vol. 13, no. 12, 2017.
15. C. N. Modi and K. Acha. Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: A comprehensive review. J. Supercomput., vol. 73, no. 3, pp. 1192-1234, 2017.
16. M. Kumar and K. S. Vaisla, "To study of various security attacks against Biometric template in a generic Biometric Recognition System," Proc. Second Int. Conf. Res. Intell. Comput. Eng., vol. 10, pp. 235–240, 2017.
17. Yu, Y.; Long, J.; Cai, Z. Network intrusion detection through stacking dilated convolutional auto encoders. Secur. Commun. Netw. 2017, 2017, 4184196.
18. Zhu, D.; Jin, H.; Yang, Y.; Wu, D.; Chen, W. Deep Flow: Deep learning-based malware detection by mining Android application for abnormal usage of sensitive data. In Proceedings of the 2017 IEEE Symposium Computers and Communications (ISCC), Heraklion, Greece, 3–6 July 2017; pp. 438–443.
19. E. Viegas, A. O. Santin, A. França, R. Jasinski, V. A. Pedroni, and L. S. Oliveira. Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems," IEEE Trans. Comput., vol. 66, no. 1, pp. 163-177, Jan. 2017.
20. Y.-H. Jo, S.-Y. Jeon, J.-H. Im, and M.-K. Lee, "Security Analysis and Improvement of Fingerprint Authentication for Smartphones," Mob. Inf. Syst., vol. 2016, no. Krait 400, pp. 1–11, 2016.
21. R. Hunt, J. Kalas, P. Lowe, and A. Stewart, "Biometric Security," pp. 1–11, 2016.
22. Naveen and K. R. Reddy, "A Review : Elliptical Curve Cryptography in Wireless Ad-hoc Networks," pp. 1786–1789, 2016.
23. S. P. Jashnani Kritika, "Comparison of Different Cryptography Approach for Secure Communication in Vehicular AD-Hoc Network," Int. J. Innov. Res. Comput. Commun. Eng., vol. 4, no. 8, pp. 14919–14923, 2016.
24. Kolosnjaji, B.; Zarras, A.; Webster, G.; Eckert, C. Deep learning for classification of malware system call sequences. In Proceedings of the Australasian Joint Conf. on Artificial Intelligence, Hobart, Australia, 5–8 December 2016; pp. 137– 149.
25. Tobiyama, S.; Yamaguchi, Y.; Shimada, H.; Ikuse, T.; Yagi, T. Malware detection with deep neural network using process behavior. In Proceedings of the IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; Volume 2, pp. 577–582.
26. Yuan, Z.; Lu, Y.; Xue, Y. Droiddetector: Android malware characterization and detection using deep learning. Tsinghua Sci. Technol. 2016, 21, 114–123.
27. Hardy, W.; Chen, L.; Hou, S.; Ye, Y.; Li, X. DL4MD: A deep learning framework for intelligent malware detection. In Proceedings of the International Conference Data Mining (ICDM), Barcelona, Spain, 12–15 December 2016; p. 61.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12,Dec 2022


**28.** Buczak, L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security. IEEE Commun. Surv. Tutor. 2016, 18, 1153–1176.

**29.** V. Singh and K. Mahajan, "VANET and its Security Issues- A Review," no. 10, 2016.

**30.** M. N. Rajkumar, M. Nithya, and P. Hemalatha, "OVERVIEW OF VANET WITH ITS FEATURES AND SECURITY ATTACKS," Int. Res. J. Eng. Technol., vol. 03, no. 01, pp. 137–142, 2016.

**31.** K. Zaidi and M. Rajarajan, "Vehicular internet: Security & privacy challenges and opportunities," Futur. Internet, vol. 7, no. 3, pp. 257–275, 2015.

**32.** N. P. K. S and P. K. S, "Comparative Study on Security Protocols for VANET " s," vol. 4, no. 9, pp. 3004–3006, 2015.

**33.** S. V. S. Muzumdar Ketki S., "Signature recognition and verification using ANN," Proceeding Third …, vol. 3, no. 6, pp. 66–76, 2015.

**34.** L. Guan, J. Lin, B. Luo, J. Jing, and J. Wang, "Protecting Private Keys against Memory Disclosure Attacks using Hardware Transactional Memory," pp. 3–19, 2015.

**35.** D. H. Shah and T. V Shah, "Signature Recognition and Verification : The Most Acceptable Biometrics for Security," vol. 4, no. 8, pp. 30–36, 2015.

**36.** R. Shaikh and D. Deotale, "A Survey on VANET Security using ECC ," vol. 4, no. 6, 2015.

**37.** R. K. Pooja and U. K. N. Kalyane, "VANET BASED SECURE AND EFFICIENT TRANSPORTATION SYSTEM," pp. 2319–2322, 2015.

**38.** Y. Liu, L. Wang, and H.-H. Chen, "Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks," IEEE Trans. Veh. Technol., vol. 64, no. 8, pp. 3697– 171 3710, 2015.

**39.** Y. Zhang, C. Zhaofeng, X. Hui, and T. Wei, "Fingerprints On Mobile Devices: Abusing and Leaking," p. 11, 2015.

**40.** S. C. Satapathy, A. Govardhan, K. S. Raju, and J. K. Mandal, "Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 2," Adv. Intell. Syst. Comput., vol. 338, pp. I–IV, 2015.

**41.** Addressing Cyber security vulnerabilities, Omar Y Sharkasi, ISACA Journal volume 5, 2015.

**42.** A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne. Evaluating computer intrusion detection systems: A survey of common practices. ACM Comput. Surv., vol. 48, no. 1, pp. 1-41, 2015.

**43.** A K Malik, Dipak Chakraborty, Satish Kumar. Quadratic Demand based Inventory Model with Shortages and Two Storage Capacities System. Research J. Engineering and Tech. 2017; 8(3): 213-218.

**44.** Gupta, K. K., Sharma, A., Singh, P. R., Malik, A. K. Optimal ordering policy for stock-dependent demand inventory model with non-instantaneous deteriorating items. International Journal of Soft Computing and Engineering, 2013; 3(1): 279-281.

**45.** Kumar, S., Chakraborty, D., Malik, A. K. A Two Warehouse Inventory Model with Stock-Dependent Demand and variable deterioration rate. International Journal of Future Revolution in Computer Science & Communication Engineering, 2017; 3(9): 20-24.

**46.** Kumar, S., Malik, A. K., Sharma, A., Yadav, S. K., Singh, Y. An inventory model with linear holding cost and stock-dependent demand for non-instantaneous deteriorating items. In AIP Conference Proceedings, 2016; 1715(1): 020058.

**47.** Kumar, S., Soni, R., Malik, A. K. Variable demand rate and sales revenue cost inventory model for non-instantaneous decaying items with maximum life time. International Journal of Engineering & Science Research, 2019; 9(2): 52-57.

**48.** Malik, A. K. and Singh, Y. A fuzzy mixture two warehouse inventory model with linear demand. International Journal of Application or Innovation in Engineering and Management, 2013; 2(2): 180-186.

**49.** Malik, A. K. and Singh, Y. An inventory model for deteriorating items with soft computing techniques and variable demand. International Journal of Soft Computing and Engineering, 2011; 1(5): 317-321.

**50.** Malik, A. K., Chakraborty, D., Bansal, K. K., Kumar, S. Inventory Model with Quadratic Demand under the Two Warehouse Management System. International Journal of Engineering and Technology, 2017; 9(3): 2299-2303.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12,Dec 2022


**51.** Malik, A. K., Mathur, P., Kumar, S. Analysis of an inventory model with both the time dependent holding and sales revenue cost. In IOP Conference Series: Materials Science and Engineering, 2019: 594(1): 012043.

**52.** Malik, A. K., Sharma, M., Tyagi, T., Kumar, S., Naik, P. J., & Kumar, P. (2022). Effect of Uncertainty in Optimal Inventory Policy for Manufacturing Products. International Journal of Intelligent Systems and Applications in Engineering, 10(1s), 102-110.

**53.** Malik, A. K., Shekhar, C., Vashisth, V., Chaudhary, A. K., Singh, S. R. Sensitivity analysis of an inventory model with non-instantaneous and time-varying deteriorating Items. In AIP Conference Proceedings, 2016; 1715(1): 020059.

**54.** Malik, A. K., Singh, S. R., Gupta, C. B. An inventory model for deteriorating items under FIFO dispatching policy with two warehouse and time dependent demand. Ganita Sandesh, 2008; 22(1), 47-62.

**55.** Malik, A. K., Singh, Y., Gupta, S. K. A fuzzy based two warehouses inventory model for deteriorating items. International Journal of Soft Computing and Engineering, 2012; 2(2), 188-192.

**56.** Malik, A. K., Vedi, P., and Kumar, S. An inventory model with time varying demand for non-instantaneous deteriorating items with maximum life time. International Journal of Applied Engineering Research, 2018; 13(9): 7162-7167.

**57.** Malik, A.K. and Garg, H. An Improved Fuzzy Inventory Model Under Two Warehouses. Journal of Artificial Intelligence and Systems, 2021; 3, 115–129. https://doi.org/10.33969/AIS.2021.31008.

**58.** Malik, A.K. and Sharma, A. An Inventory Model for Deteriorating Items with Multi-Variate Demand and Partial Backlogging Under Inflation, International Journal of Mathematical Sciences, 2011; 10(3-4): 315-321.

**59.** Malik, A.K., Singh, A., Jit, S., Garg. C.P. "Supply Chain Management: An Overview". International Journal of Logistics and Supply Chain Management, 2010; 2(2): 97-101.

**60.** Satish Kumar, Yashveer Singh, A. K. Malik. An Inventory Model for both Variable Holding and Sales Revenue Cost. Asian J. Management; 2017; 8(4):1111-1114.

**61.** Sharma, A., Gupta, K. K., Malik, A. K. Non-Instantaneous Deterioration Inventory Model with inflation and stock-dependent demand. International Journal of Computer Applications, 2013; 67(25): 6-9.

**62.** Singh, S. R. and Malik, A. K. Effect of inflation on two warehouse production inventory systems with exponential demand and variable deterioration. International Journal of Mathematical and Applications, 2008; 2(1-2): 141-149.

**63.** Singh, S. R. and Malik, A. K. Inventory system for decaying items with variable holding cost and two shops, International Journal of Mathematical Sciences, 2010; 9(3-4): 489-511.

**64.** Singh, S. R. and Malik, A. K. Two warehouses model with inflation induced demand under the credit period. International Journal of Applied Mathematical Analysis and Applications, 2009; 4(1): 59-70.

**65.** Singh, S. R., Malik, A. K. An Inventory Model with Stock-Dependent Demand with Two Storages Capacity for Non-Instantaneous Deteriorating Items. International Journal of Mathematical Sciences and Applications, 2011; 1(3): 1255-1259.

**66.** Singh, S. R., Malik, A. K., & Gupta, S. K. Two Warehouses Inventory Model for Non-Instantaneous Deteriorating Items with Stock-Dependent Demand. International Transactions in Applied Sciences, 2011; 3(4): 911-920.

**67.** Singh, Y., Arya, K., Malik, A. K. Inventory control with soft computing techniques. International Journal of Innovative Technology and Exploring Engineering, 2014; 3(8): 80-82.

**68.** Singh, Y., Malik, A. K., Kumar, S., An inflation induced stock-dependent demand inventory model with permissible delay in payment. International Journal of Computer Applications, 2014; 96(25): 14-18.

**69.** Tyagi, T., Kumar, S., Malik, A. K., & Vashisth, V. (2022). A novel neuro-optimization technique for inventory models in manufacturing sectors. Journal of Computational and Cognitive Engineering.

**70.** Tyagi, T., Kumar, S., Naik, P. J., Kumar, P., & Malik, A. K. (2022). Analysis of Optimization Techniques in Inventory and Supply Chain Management for Manufacturing Sectors. Journal of Positive School Psychology, 6(2), 5498-5505.

ISSN PRINT 2319 1775 Online 2320 7876
*Research paper*  UGC CARE Listed ( Group -I) Journal Volume 11, Iss 12,Dec 2022

**71.** Vashisth, V., Tomar, A., Chandra, S., Malik, A. K. A trade credit inventory model with multivariate demand for non-instantaneous decaying products. Indian Journal of Science and Technology, 2016; 9(15): 1-6.

**72.** Vashisth, V., Tomar, A., Soni, R., Malik, A. K. An inventory model for maximum life time products under the Price and Stock Dependent Demand Rate. International Journal of Computer Applications, 2015; 132(15): 32-36.

**73.** Verma, P., Chaturvedi, B. K., & Malik, A. K. (2022). Comprehensive Analysis and Review of Particle Swarm Optimization Techniques and Inventory System, International Journal on Future Revolution in Computer Science & Communication Engineering, 8(3), 111-115.

**74.** Yadav, S.R. and Malik, A.K. Operations Research, Oxford University Press, New Delhi, 2014.

**75.** Yadav, V., Chaturvedi, B. K., & Malik, A. K. (2022). Advantages of fuzzy techniques and applications in inventory control. International Journal on Recent Trends in Life Science and Mathematics, 9(3), 09-13.