RESEARCH ARTICLE OPEN ACCESS

Malware Detection and Signature Generation

Prateek Nigam
Dean & Hod, Electrical And Electronics Engineering (Eee) Sarvepalli Radhakrishnan University-Bhopal

ABSTRACT
Now a day, the malware detection is needful to enhance the performance of the systems and omit the effect of malware to system. The conventional signature-based detection of malware did not detect a major of new variants. This paper presented a hybrid technique for automatic malware signature generation and classification. The hybrid method is named as a ANFIS-SSA approach. Using this observation, we present a hybrid method for detection of malware using the correlation between the semantics of the malware and its API calls. Here, develops a base signature for a whole malware class more than for a solitary specimen of malware. The signature can able of find out even advanced variants and unknown which related to that class. Here, demonstrates our method on some well-known malware classes and presented that any advanced variants classes is detected from the base signature.
Keywords: Malware detection, signature generation, malicious

I. INTRODUCTION

The most famous PC assault is malware that comprise of seventeen classes, for example, infections, worms, Trojan horse, spyware and furthermore different malicious software. Malware is a program with pernicious aim intended to harm the PC on which it executes or the system over which it imparts [1-10]. Albeit a wide range of malware has their particular target, the primary design is to break the PC activity. Thus, the security component should be actualized so as to ensure all code and information against change, substitution or sub-formed. Present day PC and correspondence frameworks are exceptionally helpless to different sorts of assault [11-20]. A typical method for propelling these assaults is by methods for malicious software (malware, for example, worms, infections, and Trojan horse, which, when spread, can make serious harm private clients, business organizations, and governments [21-24].

The ongoing development in fast Internet associations gives a stage to making and quickly spreading the new malware. A few examination strategies for recognizing malware have been proposed [25-34]. They are named to whether they are static or dynamic. In dynamic analysis (otherwise called social based investigation), identification depends on data gathered from the working framework at runtime (i.e., during the execution of the program, for example, system calls, network access and records, and memory alterations [35-50]. In static analysis, the location depends on data removed expressly or verifiably from the executable twofold/source code. The fundamental bit of leeway of static examination is in giving fast order. Since antivirus sellers are confronting every day a mind-boggling measure of suspect documents for review, rapid detection is basic [51].

Static examination arrangements are fundamentally actualized utilizing two techniques: signature-based and heuristic-based. Mark put together strategies depend with respect to the recognizable proof of novel strings in the binary code [52]. The heuristic strategies depend on rules, which are either controlled by specialists or by AI systems that characterize a noxious or a kindhearted conduct so as to identify obscure malware. This exploration centers around robotizing the way toward producing marks to be introduced on such apparatuses for known malware that should be sifted by the machines [53-55]. Different methods have been proposed to determine malware marks consequently, including among others: helplessness based marks; payload-based marks; content filtering; semantic-mindful marks; The Amd calculation; Honeypot-based marks and polymorphic substance based marks [56-60]. Moreover, the deep learning is acquainted with create the programmed marks. The above strategies are not ready to create the best outcomes for programmed signature age and malware identification. To conquer the current techniques disadvantages, the proposed strategy will be structured and created in this paper

II. LITERATURE REVIEW

A wide range of strategies for malware identification and signature generation are created by the analysts. A portion of the techniques are explored here,

Dina Saif *et al.* [61] have exhibited building up an effective computational system dependent on Deep Belief Networks for malware discovery. The structure combines significant level static investigation, dynamic examination and system calls in feature extraction so as to accomplish the highest

accuracy. The assessment looks at the most commonplace AI approaches that were applied in malware recognition with the proposed system. The acquired outcomes are exhibit that Deep Belief Networks procedure can understand 99.1% accuracy with the introduced dataset. Far beyond that, here build up our total static examination container which embraces distinctive productive techniques trying to encourage and accelerate the static investigation by dealing with all the Android applications in just one stage instead of thinking about each application in turn.

A Multi-Level Deep Learning System (MLDLS) [62] those sorts out various deep learning models utilizing the tree structure. Each model in the tree structure of MLDLS was not based in general dataset. Rather, every deep learning model spotlights on learning a particular information circulation for a specific gathering of malware and all deep learning models in the tree cooperate to settle on an ultimate conclusion. Thusly, the learning viability of every deep learning model worked for one bunch can be improved. Trial results demonstrate that framework performs superior to the conventional methodology. To safeguard against an expanding number of advanced malware assaults, deep learning based Malware Detection Systems (MDSs) have turned into an indispensable segment of our financial and national security. Customarily, analysts construct the single deep learning model utilizing the whole dataset. In any case, the single profound learning model may not deal with the undeniably mind boggling malware information appropriations successfully. Since various example subspaces speaking to a gathering of comparative malware may have remarkable information conveyance. So as to further improve the presentation of deep learning based MDSs.

Yuan Xue *et al.* [63] have created root privilege management agency named Root Agency, which receives a digital signature scheme to ensure the selective root-privilege-granting chances of confirmed applications. Root Agency verifies an application by checking whether it holds the mark produced by the secret key, and awards the root privilege when a marked application presents the solicitation. In addition, it checks the application's uprightness to keep it from repackaging. Hence, the clients were not engaged with decision making while defying root requests. The plan guarantees the security of established Android gadgets, and upgrades the security of portable terminal gadgets. This reduces the risk to cloud foundation from root-misused Android gadgets. What's more, a model was executed to assess its viability, proficiency, and overhead. The trial results demonstrate that Root Agency was generally good and its exhibition overhead was sensible.

III. AUTOMATIC SIGNATURE GENERATION

The word malware is a portmanteau of "malicious software" and means programming intended to invade or harm a PC framework, without the proprietor's assent. Malware is an aggregate name for adware, spyware, Trojan horses, worms, viruses and their preferences. Usually the word" viruses" is utilized to depict all the above mentioned, despite the fact that genuine infections make out an entirely modest number of the current malware [16]. The need to group malignant projects as per a bound together terminology is about as old as PC infections themselves. Clearly this isn't a simple work with numerous classes covering or being firmly related. Now and again specialists additionally differ on the arrangement, even inside CARO (Computer Antivirus Researchers Organization). The a portion of the viruses are viruses, zoo viruses, Hoaxes, Root kits, key loggers, downloader's, spyware, exploits, Trojan Horses (trojans), worms and so on. The detail depiction of the a portion of the infections are displayed underneath,

- **Viruses:** a PC Virus is code that recursively recreates a conceivably advanced duplicate of itself. Viruses taint a host record or framework territory, or they essentially change a reference to such articles to take control and afterward increase again to shape new generations.
- **Worms** are ordinarily independent applications without a host program. They fundamentally duplicate on systems, for the most part with no assistance from a client. Be that as it may, a few worms additionally spread as a record infector virus and contaminate host programs, which is the reason they are frequently named a unique subclass of viruses.
- **Trojan Horses (trojans)** depict themselves as an option that is other than what they are at the purpose of execution. In spite of the fact that it might promote its action in the wake of propelling, this data isn't evident to the client in advance. A Trojan neither imitates nor duplicates itself, yet purposes harm or bargains the security of the PC.
- **Exploits** are projects or procedures that exploit defenselessness in programming. Endeavors can be utilized for breaking security or generally assaulting hosts over the system.
- **Spyware** are programs that can examine frameworks or screen movement and pass this data on to the aggressor. Regular data that might be effectively or latently assembled is passwords, sign in subtleties, account numbers,

individual data, singular records or other individual archives

The diverse malwares identification is basic to improve the presentation of the PC and evade the effect of the framework by malware. Throughout the years malware essayists have been cunning in developing their manifestations. Malware have advanced as to replication and spreading instruments, just as strategies used to avoid examination or potentially discovery. Such procedures incorporate enemy of troubleshooting, encryption, utilizing exe-packers, entry point obscuring and so forth. Despite the fact it has been demonstrated that there is no calculation that can flawlessly distinguish all future viruses in finite time. It is critical to take note of that not all methods can be applied to all malware and this ought to likewise not be required. Because one strategy can't be utilized all the time doesn't mean it is totally incapable. It is sufficient to have a wide range of procedures, one of which will be a decent answer for square, recognize or sterilize a specific malware.

A wide range of methods are created by the specialists yet it not ready to deliver the best answer for stay away from the malware in the framework. Here, signature based malware detection is presented in this paper. Signature based recognition is one of the static investigation strategies that regularly utilized on business antimalware programming. The static investigation strategy would look over the program code for detection reason and some of the time called output strings. This system utilizes it portrayal of the malicious code to conclude that is malware of not through program examination. Regularly, each malware spoke to by at least one mark designs which are novel to portray it. At the point when a program is executed, hostile to malware programming will look through bytes of information stream. A large number of signatures will be place on database and filtering procedure will search for every signature to contrast and the program code that execute. Scanning calculation will be utilized to contrast substance of program code and the signature on database. In this structure, signature-based strategy will actualize as the main guard from malware assault that will taint PC activity. This method was picked in light of the fact that this sort of procedure has been compelling in recognizing understood malware. So as to improve the effectiveness of PC activity, this system was proposed in this structure. The definite proposed technique architecture is introduced in the beneath segment.

IV. PROPOSED ARCHITECTURE

In this section, first, we briefly outline our approach for malware signature generation and classification. Next, we describe our program behavior model used for signature generation and the statistical comparison technique. Then, we present our malware detection algorithm using our program behavior model [17]. Finally, we describe our prototype implementation in detail and show a sample signature of a malware extracted using our approach. The proposed model is presented in the figure 1.

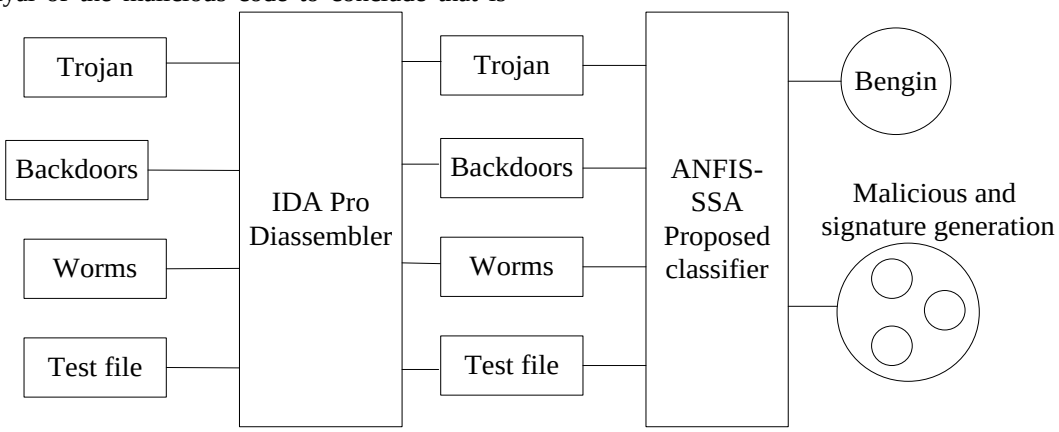

Figure 1: Architecture of the proposed method.

We make signatures dependent on the attributes of a whole malware class as opposed to a solitary example of malware. Malware classes are characterized dependent on comparative conduct. The conduct of a malware class can be determined dependent on the application program interface (API) calls that the individuals from the malware calls use. For example, an infection attempting to look for executable records will commonly utilize API calls, for example, KERNEL32.DLL, FindClose, FindNextFileA and FindFirstFileA. The conduct of looking through records is caught by the utilization of these API calls. As opposed to considering all API calls, we consider just basic API

calls. Basic API calls incorporate all API calls that can prompt security bargain, for example, considers that change the manner in which the working framework carries on or those utilized for correspondence, for example, WinSock, File I/O API, File I/O API Registry API and so on.

Signature Generation

Subsequent to arranging and making nearby duplicates of the malware tests the scan engine is kept running over them to part the examples into block files. The block files speak to the segments of the documents the scanner regard prone to contain malignant code. It is from these block files that a mark at that point is produced [18]. To conceivably produce generic signatures the documents are contrasted with discover normal code. The block files are opened with an interior instrument that demonstrates a hexadecimal portrayal of the machine code and features regular code fragments between the open files. Which block from an example to contrast and which square from another must be picked carefully. Ordinarily the size of the first records together with the size of the produced block files can be useful in discovering which blocks may contain basic code. For a malware where just a couple of tests exist or where all variations are about indistinguishable discovering normal code should be possible before long. Be that as it may, it isn't hard observing that when numerous examples exist and they share almost no practically speaking this can be monotonous work to do physically. In the worst outcome imaginable every single imaginable pair of records must be analyzed just to discover that no likenesses exist.

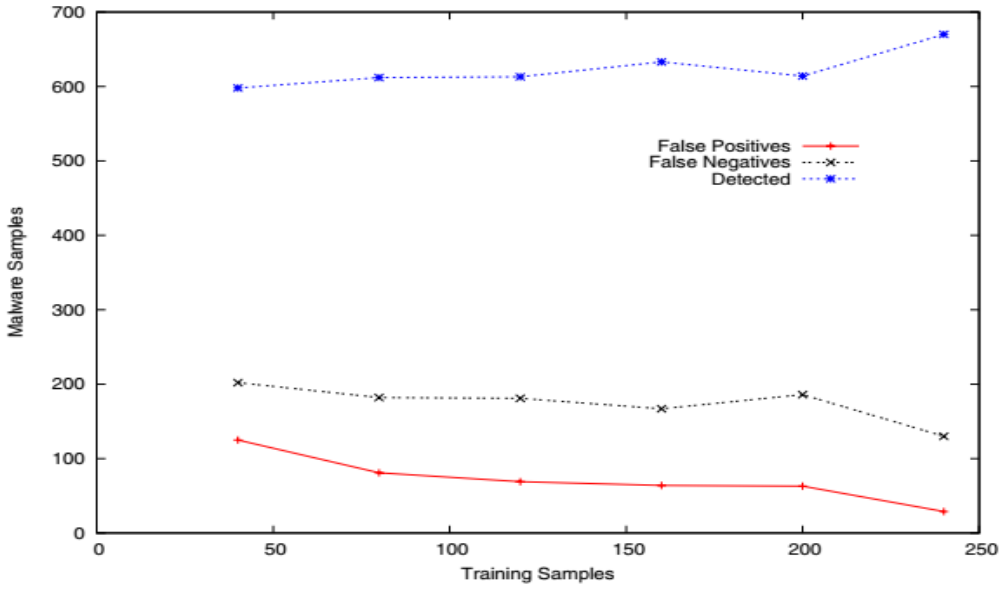

Figure 2: Number of training samples with false positive, false negative values

We found that few benign projects share conduct (for example, looking through records, replicating documents to network drives and so on.) with certain noxious projects. The watched false positive rate is because of such common conduct. The outcomes demonstrate that even without the base signature, our procedure had the option to identify another malware utilizing the mark developed from wide malware classes with sensible exactness. Once the new malware is identified, its base signature can without much of a stretch be developed to recognize its future variations. The proposed technique is contrasted and the current strategies, for example, SAFE.

Table 1: Comparison analysis of the proposed method

Malware	API call extractor/Annotator		Detector	
	SAFE	proposed	SAFE	proposed
Hare	9.142	1.665	1.604	0.0282
F0sf0r0	4.900	1.781	0.923	0.0256
Zombie-6.b	4.600	1.718	1.149	0.0314
Chernobyl	1.444	2.172	0.535	0.0138

We tested the time it requires to order a given record as malicious or benign. We consider the time adopted by our strategy to extricate the API calls and to arrange it as malicious or benign. We contrast our methodology with SAFE. SAFE makes a deliberation example of the pernicious code and changes over it into an inward portrayal. Given a test program, it makes a control stream chart (CFG) of the test program, and checks whether the interior portrayal of malevolent code is available in the CFG. SAFE has been tried uniquely on a not many malware tests. Table 3 looks at the time adopted by our strategy with that of SAFE for four examples of malware. Plainly, our methodology is a lot quicker than SAFE.

V. CONCLUSION

This paper proposes a hybrid approach for automatic generation of signatures for malware executable of all sizes with an aim to be utilized by rapid malware sifting gadgets. We consider the way that huge executables are involved generous measures of code that begins from the fundamental standard improvement stages and is therefore duplicated crosswise over different cases of both benign and malware created by these stages. So as to limit the danger of false positive characterization of favorable executables as malware, we propose and assess a strategy to dispose of signature up-and-comers that contain such duplicated lumps of code. The primary advantage of the proposed strategy is that it empowers examination at the binary level and doesn't require a semantic interpretation of code into capacity blocks utilizing systems, for example, code markers, dismantling, state-machines and so forth. This advantage implies that the procedure is conventional and isn't influenced by changes in CPU or presentation of new improvement stages. By and by, undertakings which might want acknowledge Auto-Sign in creating signatures for high-throughput arrange security machines need to pursue an increasingly thorough and orderly strategy for structure their CFL vault. Thinking about the worldwide assortment of advancement stages and the portability of dangers encouraged by the Internet, guaranteeing the outside legitimacy of this examination depends significantly on arriving at a minimum amount of CFL records which speaks to inexhaustible improvement stages. Besides, it frequently doesn't get the job done for a signature to be accessible sent signature must be overseen, dispersed and stayed up with the latest by security executives.

REFERENCE

[1] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, Dac Nhuong Le, Smart Surveillance Robot for the Real Time Monitoring and Control System in Environment and Industrial Applications, Advances in Intelligent System and Computing, pp 229-243, Springer

[2] Ezhilarasu, P., & Krishnaraj, N. (2015). Applications of Finite Automata in Lexical Analysis and as a Ticket Vending Machine–A Review. Int. J. Comput. Sci. Eng. Technol, 6(05), 267-270.

[3] Agrawal, U., Arora, J., Singh, R., Gupta, D., Khanna, A., & Khamparia, A. (2020). Hybrid Wolf-Bat Algorithm for Optimization of Connection Weights in Multi-layer Perceptron. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 16(1s), 1-20.

[4] Prasanna, S., & Ezhilmaran, D. (2016). Association rule mining using enhanced apriori with modified GA for stock prediction. International Journal of Data Mining, Modelling and Management, 8(2), 195-207.

[5] Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. IEEE Access, 8, 107112-107123.

[6] Shankar, K., Zhang, Y., Liu, Y., Wu, L., & Chen, C. H. (2020). Hyperparameter tuning deep learning for diabetic retinopathy fundus image classification. IEEE Access, 8, 118164-118173.

[7] Joshi, G. P., Perumal, E., Shankar, K., Tariq, U., Ahmad, T., & Ibrahim, A. (2020). Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. Electronics, 9(9), 1358.

[8] Saračević, M. H., Adamović, S. Z., Miškovic, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., & Shankar, K. (2020). Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures. IEEE Transactions on Reliability.

[9] Namasudra, S., & Roy, P. (2017). Time saving protocol for data accessing in cloud computing. IET Communications, 11(10), 1558-1565.

[10] Elsir, A., Elsier, O., Abdurrahman, A., & Mubarakali, A. (2019). Privacy Preservation in Big Data with Data Scalability and Efficiency Using Efficient and Secure Data Balanced Scheduling Algorithm.

[11] Ezhilarasu, P., Krishnaraj, N., & Babu, S. V. (2015). Applications of finite automata in text search-a review. International Journal of

Science, Engineering and Computer Technology, 5(5), 116.

[12] Huyen, D.T.T., Binh, N.T., Tuan, T.M., Nguyen, G.N, Dey, N., Son, L.H, Analyzing trends in hospital-cost payments of patients using ARIMA and GIS: Case study at the Hanoi Medical University Hospital, Vietnam, Journal of Medical Imaging and Health Informatics, 7(2), pp. 421-429.

[13] Prasanna, S., & Maran, E. (2015). Stock Market Prediction Using Clustering with Meta-Heuristic Approaches. Gazi University Journal of Science, 28(3).

[14] Pustokhina, I. V., Pustokhin, D. A., Rodrigues, J. J., Gupta, D., Khanna, A., Shankar, K., ... & Joshi, G. P. (2020). Automatic Vehicle License Plate Recognition using Optimal K-Means with Convolutional Neural Network for Intelligent Transportation Systems. IEEE Access.

[15] Namasudra, S. (2018). Cloud computing: A new era. Journal of Fundamental and Applied Sciences, 10(2).

[16] Uthayakumar, J., Elhoseny, M., & Shankar, K. (2020). Highly Reliable and Low-Complexity Image Compression Scheme Using Neighborhood Correlation Sequence Algorithm in WSN. IEEE Transactions on Reliability.

[17] Deepalakshmi, P., & Shankar, K. (2020). Role and Impacts of Ant Colony Optimization in Job Shop Scheduling Problems: A Detailed Analysis. Evolutionary Computation in Scheduling, 11-35.

[18] Ashwin, M., Kamalraj, S., & Azath, M. (2019). Multi objective trust optimization for efficient communication in wireless M learning applications. Cluster Computing, 22(5), 10687-10695.

[19] Ezhilarasu, P., & Krishnaraj, N. (2015). Double Substring based Classification for Nondeterministic Finite Automata. Indian Journal Of Science And Technology, 8, 26.

[20] Amira S. Ashour, Samsad Beagum, Nilanjan Dey, Ahmed S. Ashour, Dimitra Sifaki Pistolla, Gia Nhu Nguyen, Dac-Nhuong Le, Fuqian Shi (2018), Light Microscopy Image De-noising using Optimized LPA-ICI Filter, Neural Computing and Applications, Vol.29(12), pp 1517–1533, Springer, ISSN: 0941-0643.

[21] Prasanna, S., Govinda, K., & Kumaran, U. S. (2012). An Evaluation study of Oral Cancer Detection using Data Mining Classification Techniques. International Journal of Advanced Research in Computer Science, 3(1).

[22] Sankhwar, S., Gupta, D., Ramya, K. C., Rani, S. S., Shankar, K., & Lakshmanaprabu, S. K. (2020). Improved grey wolf optimization-based feature subset selection with fuzzy neural classifier for financial crisis prediction. Soft Computing, 24(1), 101-110.

[23] Namasudra, S., & Deka, G. C. (2018). Introduction of DNA computing in cryptography. In Advances of DNA computing in cryptography (pp. 1-18). Chapman and Hall/CRC.

[24] Mubarakali, A., Srinivasan, K., Mukhalid, R., Jaganathan, S. C., & Marina, N. (2020). Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems. Computational Intelligence.

[25] Le Nguyen Bao, Dac-Nhuong Le, Gia Nhu Nguyen, Vikrant Bhateja, Suresh Chandra Satapathy (2017), Optimizing Feature Selection in Video-based Recognition using Max-Min Ant System for the Online Video Contextual Advertisement User-Oriented System, Journal of Computational Science, Elsevier ISSN: 1877-7503. Vol.21, pp.361-370.

[26] Ezhilarasu, P., Thirunavukkarasu, E., Karuppusami, G., & Krishnaraj, N. (2015). Single substring based classification for nondeterministic finite automata. International Journal on Applications in Information and Communication Engineering, 1(10), 29-31.

[27] Bhateja, V., Gautam, A., Tiwari, A., Nhu, N.G., Le, D.-N, Haralick features-based classification of mammograms using SVM, Advances in Intelligent Systems and Computing, Volume 672, 2018, Pages 787-795.

[28] Latha, A., Prasanna, S., Hemalatha, S., & Sivakumar, B. (2019). A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks. Cognitive Systems Research, 56, 14-22.

[29] Krishnaraj, N., Elhoseny, M., Lydia, E. L., Shankar, K., & ALDabbas, O. (2020). An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment. Software: Practice and Experience.

[30] Namasudra, S., Roy, P., Vijayakumar, P., Audithan, S., & Balusamy, B. (2017). Time efficient secure DNA based access control model for cloud computing environment. Future Generation Computer Systems, 73, 90-105.

[31] Lakshmanaprabu, S. K., Shankar, K., Rani, S. S., Abdulhay, E., Arunkumar, N., Ramirez, G., & Uthayakumar, J. (2019). An effect of big data technology with ant colony optimization based routing in vehicular ad hoc networks: Towards smart cities. Journal of cleaner production, 217, 584-593.

[32] Namasudra, S., & Deka, G. C. (Eds.). (2018). Advances of DNA computing in cryptography. CRC Press.

[33] Mubarakali, A., Ashwin, M., Mavaluru, D., & Kumar, A. D. (2020). Design an attribute based health record protection algorithm for healthcare services in cloud environment. Multimedia Tools and Applications, 79(5), 3943-3956.

[34] Dey, N., Ashour, A.S., Chakraborty, S., Le, D.-N., Nguyen, G.N, Healthy and unhealthy rat hippocampus cells classification: A neural based automated system for Alzheimer disease classification, Journal of Advanced Microscopy Research, 11(1), pp. 1-10

[35] Krishnaraj, N., Ezhilarasu, P., & Gao, X. Z. Hybrid Soft Computing Approach for Prediction of Cancer in Colon Using Microarray Gene Data. Current Signal Transduction Therapy, 11(2).

[36] Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. (2020). The revolution of blockchain: State-of-the-art and research challenges. Archives of Computational Methods in Engineering.

[37] Goel, N., Grover, B., Gupta, D., Khanna, A., & Sharma, M. (2020). Modified Grasshopper Optimization Algorithm for detection of Autism Spectrum Disorder. Physical Communication, 101115.

[38] Prasanna, S., Narayan, S., NallaKaruppan, M. K., Anilkumar, C., & Ramasubbareddy, S. (2019). Iterative Approach for Frequent Set Mining Using Hadoop Over Cloud Environment. In Smart Intelligent Computing and Applications (pp. 399-405). Springer, Singapore.

[39] Le, D.-N.a, Kumar, R.b, Nguyen, G.N., Chatterjee, J.M.d, Cloud Computing and Virtualization,
DOI: 10.1002/9781119488149, Wiley.

[40] Raj, R. J. S., Shobana, S. J., Pustokhina, I. V., Pustokhin, D. A., Gupta, D., & Shankar, K. (2020). Optimal Feature Selection-Based Medical Image Classification Using Deep Learning Model in Internet of Medical Things. IEEE Access, 8, 58006-58017.

[41] Namasudra, S., & Deka, G. C. (2018). Taxonomy of DNA-based security models. In Advances of DNA Computing in Cryptography (pp. 37-52). Chapman and Hall/CRC.

[42] Mubarakali, A., Ramakrishnan, J., Mavaluru, D., Elsir, A., Elsier, O., & Wakil, K. (2019). A new efficient design for random access memory based on quantum dot cellular automata nanotechnology. Nano Communication Networks, 21, 100252.

[43] Ramakrishnan, J., Mavaluru, D., Sakthivel, R. S., Alqahtani, A. S., Mubarakali, A., & Retnadhas, M. (2020). Brain–computer interface for amyotrophic lateral sclerosis patients using deep learning network. NEURAL COMPUTING & APPLICATIONS.

[44] Van, V.N., Chi, L.M., Long, N.Q., Nguyen, G.N., Le, D.-N, A performance analysis of openstack open-source solution for IaaS cloud computing, Advances in Intelligent Systems and Computing, 380, pp. 141-150.

[45] Sinha, A., Shrivastava, G., Kumar, P., & Gupta, D. (2020). A community-based hierarchical user authentication scheme for Industry 4.0. Software: Practice and Experience.

[46] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. Computer Communications, 151, 539-547.

[47] Mubarakali, A., Durai, A. D., Alshehri, M., AlFarraj, O., Ramakrishnan, J., & Mavaluru, D. (2020). Fog-Based Delay-Sensitive Data Transmission Algorithm for Data Forwarding and Storage in Cloud Environment for Multimedia Applications. Big Data.

[48] Reshmi, T. R., & Azath, M. (2020). Improved self-healing technique for 5G networks using predictive analysis. Peer-to-Peer Networking and Applications, 1-17.

[49] Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2020). Securing multimedia by using DNA based encryption in the cloud computing environment. ACM Transactions on Multimedia Computing Communications and Applications.

[50] Patro, K. K., Reddi, S. P. R., Khalelulla, S. E., Kumar, P. R., & Shankar, K. (2020). ECG data optimization for biometric human recognition using statistical distributed machine learning algorithm. The Journal of Supercomputing, 76(2), 858-875.

[51] Rajagopal, A., Joshi, G. P., Ramachandran, A., Subhalakshmi, R. T., Khari, M., Jha, S., ... & You, J. (2020). A Deep Learning Model Based on Multi-Objective Particle Swarm Optimization for Scene Classification in

Unmanned Aerial Vehicles. IEEE Access, 8, 135383-135393.

[52] Chakchai So-In, Tri Gia Nguyen, Gia Nhu Nguyen: Barrier Coverage Deployment Algorithms for Mobile Sensor Networks. Journal of Internet Technology 12/2017; 18(7):1689-1699.

[53] Mubarakali, A., Bose, S. C., Srinivasan, K., Elsir, A., & Elsier, O. (2019). Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. Journal of Ambient Intelligence and Humanized Computing, 1-9.

[54] Devaraj, A. F. S., Murugaboopathi, G., Elhoseny, M., Shankar, K., Min, K., Moon, H., & Joshi, G. P. (2020). An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme. IEEE Access, 8, 144310-144320.

[55] Mubarakali, A. (2020). Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN (SRHB) Approach. MOBILE NETWORKS & APPLICATIONS.

[56] Namasudra, S. (2019). An improved attribute-based encryption technique towards the data security in cloud computing. Concurrency and Computation: Practice and Experience, 31(3), e4364.

[57] Kathiresan, S., Sait, A. R. W., Gupta, D., Lakshmanaprabu, S. K., Khanna, A., & Pandey, H. M. (2020). Automated detection and classification of fundus diabetic retinopathy images using synergic deep learning model. Pattern Recognition Letters.

[58] Govinda, K., & Prasanna, S. (2015, February). Medical dialysis prediction using fuzzy rules. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-5). IEEE.

[59] Sujatha, R., Navaneethan, C., Kaluri, R., & Prasanna, S. (2020). Optimized Digital Transformation in Government Services with Blockchain. In Blockchain Technology and Applications (pp. 79-100). Auerbach Publications.

[60] Govinda, K., & Prasanna, S. (2015, February). A generic image cryptography based on Rubik's cube. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-4). IEEE.

[61] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, BioSenHealth 1.0: A Novel Internet of Medical Things (IoMT) Based Patient Health Monitoring System, Lecture Notes in Networks and Systems. Springer, 2019

[62] Prasanna, S., & Narayanan, V. (2017). A Novel Approach for Generation of All-Optical OFDM Using Discrete Cosine Transform Based on Optical Couplers in a Radio-Over-Fiber Link. International Journal of Advanced Research in Engineering and Technology, 8(3).

[63] Sanjeevi, P., Prasanna, S., Siva Kumar, B., Gunasekaran, G., Alagiri, I., & Vijay Anand, R. (2020). Precision agriculture and farming using Internet of Things based on wireless sensor network. Transactions on Emerging Telecommunications Technologies, e3978.

[64] Rathi, V. K., Chaudhary, V., Rajput, N. K., Ahuja, B., Jaiswal, A. K., Gupta, D., ... & Hammoudeh, M. (2020). A Blockchain-Enabled Multi Domain Edge Computing Orchestrator. IEEE Internet of Things Magazine, 3(2), 30-36.

[65] Khanna, A., Rodrigues, J. J., Gupta, N., Swaroop, A., & Gupta, D. (2020). Local mutual exclusion algorithm using fuzzy logic for Flying Ad hoc Networks. Computer Communications.