Advances in Cyber Security Paradigm: A Review

Shahana Gajala Qureshi[1]and Shishir Kumar Shandilya[2]

[1,2]Vellore Institute of Technology, VIT BhopalUniversity(M.P.), India

shahana.rit@gmail.com

Abstract. This review paper discusses the various defensive models and mechanisms used so far in cyber security. Cyber security is very sensitive issue, where technologies are integrated day by day. To deal with sophisticated attackers, there is a need to develop a strong proactive defensive mechanism for fastest growing malware codes and other attacks too. In particular, digitization and information infrastructure initiated a battle for dominance in cyber space. This paper aims to highlight various challenges in cyber security, recent integrated technologies along with the recent advances in cyber security paradigm.

Keywords: Cyber Security, Cyber Crime, Malicious Code, Proactive security mechanisms, Hybrid approach, Cyber Security Decision Support (CSDS) System.

1 Introduction

The world is moving towards digitalization with rapid technological developments. Therefore data security is one of the leading challenges in front of us. Integration in technologies has made the Internet the most important infrastructure for the business development of government and private organizations [1]. While computer networks and the Internet remain an important part of organizations, they are also creatingenough opportunities for attackers. Strong Cyber Security infrastructures are required for nation's security and economic welfare byprotecting critical information. With the advancement in communication technologieslike latest tools, denser network, and high bandwidth, cyber attackers are having more possibilities to exploit and new vulnerabilities.

Data security is one of the major issues while sharing of data in different areas like banking, government department, e-commerce, communications, national defense, entertainment, finance, and private organization over cyberspace. To protect essential information, many techniques have been developed but still, the databases are prone to variety of attacks. These attacks are further classified as active attacks and passive attacks [3-4]. A strong cyber architecture can be a solution to this, which is mostly emphasizes on security features, such as cybersecurity devices like firewalls, Intrusion Detection/Protection Systems, strong passwords encryption/decryption devices,

etc. and secure communication protocols such as HTTPS, SSL, etc. However, most of the organizations face difficulties in identifying what critical assets need to be protected and how to implement appropriate cyber architecture to control, and segment the network. To avoid these difficulties, organizations need to move toCyber Security Decision Support (CSDS) systems. There are various types of security mechanisms, which are based on the various attacks [5-6]. Figure 2 depicts some of the most common cyber-attacks.The first level categorizes the types of cybersecurity, the second level corresponds to the objective related to each type and the third level in the hierarchy includes various attacks observed.

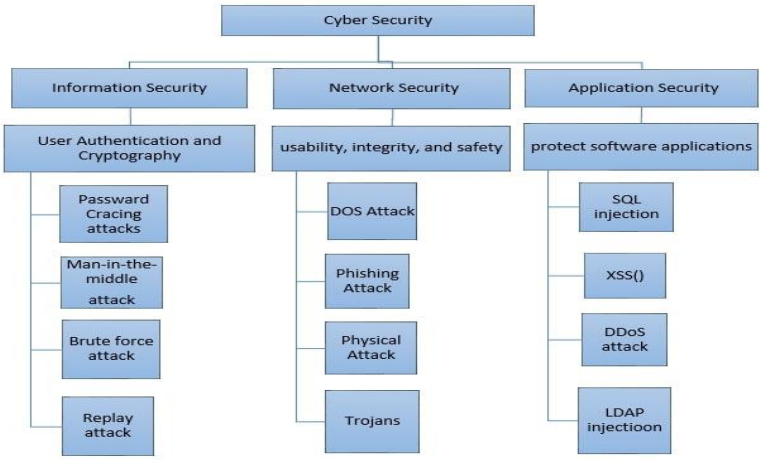

Fig.2. Classification of Cyber Security with Attacks

2 Literature Review

In the mid-1990s, cyber issues came into existence and by the end of the ’90s; official responses to dealing with these issues had also taken shape [7]. And since then, many defensive mechanisms have been developed so far to deal with cyber issues. In this paper, we have tried to throw some light on cyber-attacks and their defensive mechanisms.

In 2008 Moradian E. et al. [8] proposed a meta-agents approach in web services. For a business system, web services have always been a subject of concern. The approach was specifically proposed to monitor the threats and attacks in web services. They proposed meta-agents over software agents in a multi-agent system to prevent possible attacks on web services. In meta-agents, an agent was used to monitor software agent activities and accordingly work was directed to software agents. By using this approach, unexpected event were also handled. Bedi P. et al. in 2009 [9] proposed a system based on multi-agent system planning for threat avoidance (MASPTA) where the system works in a multi-agent environment and uses a goal-oriented action planning (GOAP) strategy with the threat modeling process. In their proposed system, the agents played an important role to avoid threats. In particular, the main aim of

thisapproach was to protect web-based systems by avoiding identified threats. The system used to treat modeling concepts to identify the threats first and after that, an attack tree was created by using Hierarchical Task Network (HTN) technique. Along with this, Goal Oriented Action Planning (GOAP) was used to generate an action plan which avoids threats. Whereas Saurabh A. et al. [10] considered the problem of security-constrained optimal control for discrete-time. In particular, they focused on a class of denial-of-service (DoS) attack models and were aimed to minimize the objective function of the problem by finding an optimal feedback controller subject to safety and power constraints. To solve this problem they presented a semi-definite programming based solution.

Nassar M. et.al in 2010[11] proposed a framework for monitoring SIP (Session Initiation Protocol - RFC 3261) enterprises networks. They proposed an approach Anomaly detection provided security to SIP enterprises networks at three levels; 1) Traffic on network, 2) the server logs and 3) enterprises billing records. This Anomaly detection was based on two factors: feature extraction and one-class Support Vector Machines (SVM). They also proposed methods for anomaly/attack type classification and attack source identification. Fu-Hau H. et al.in 2011 [12] proposed a BrowserGuard, to protect a browser against drive-bydownload attacks. In this type of attack, attackers can download any code on a victim's host as well as can execute it also. BrowserGuard used to monitor the download scenario of every loaded file on the web browser. To implement BrowserGuard on IE 7.0, they used the BHO (browser helper object) mechanism of the window. Their experiment result showed less than 2.5% of low performance and in their experiment, they did not use false positives and false negatives for the web pages.

In 2012, Gandotra V. et al. [13] presented a Three Phased Threat-Oriented Security model based on the concept of proactive threat management. In this model, they provided security for both known and unknown threat, which was not possible in the traditional method. By this model, in the first phase; they applied both threat modeling processes and research honey tokens together to identify unknown threats and in the second phase; using a multi-agent system, concern and necessary security measures had reduced the dangers. Basically, this model was used in the risk analysis segment of the spiral model to enhance security. This model leads the traditional technique, where they provide security only against the identified threats. Whereas Roy A. et al. [14] proposed a novel attack tree (AT): attack countermeasure trees (ACT) that took into account both attacks and countermeasures as detection mechanisms and mitigation techniques respectively. This proposed model allows one to perform security on the basis of qualitative and probabilistic analysis. Their proposed model outperforms as compare to other existing analytical model-based security optimization strategies. In 2013, Almasizadeh J. et al. [15] proposed a State-Based-Stochastic model which uses Semi-Markov-Chain to generate a security matrix. Through this matrix, the degree of system security was counted. The degree indicated the level of security on the system. In particular, the proposed model was described as the attacker's activity, as well as the system's reactions over time by using probability distribution function.

In 2014 [16], Dewar presented a paper intending to define cybersecurity terminologies. Along with this, three approaches were proposed: 1) Active Cyber Defense (ACD): It was designed to predict proactive measures to identify malicious codes. 2) Fortified Cyber Defense (FCD): it was designed to provide security by constructing secure communication and information networks. 3) Resilient Cyber Defense (RCD): This approach was designed to focus on decisive infrastructure and services which provided continue network communication and services. Peri Net Machine is a tool of graphical and digital modeling along with a strong mathematical basis and graphical modeling capability. In the same year [17] researchers, Xinlei Li and Di Li found that traditional machines are not capable enough in detection capability in the synthetic model, andone cannot use all Peri Net Machines to describe attack behavior and if the machine is having a machine element simply it causes errors. Hence, to overcome failures in traditional machines, they proposed a Network Attack model based on Colored Petri Net. This model supported both synthesis operation and colored synthetic operation along with this model ensured synthetic model reserves original detection capability.The same year, an Intelligent approach against injection (e.g. SQL, XSS) and Trojan attacks happened in web applications had been proposed by Razzaq A. et al. [18]. They modeled security framework using the ontology approach. This was very promising to detect zero-day vulnerabilities. Especially, this model captured the context; detect HHP protocol attacks, focused only on specific requests and responses where malicious attacks were possible. This model also took into consideration important content of attacks, source, target, vulnerabilities, technologies used by attackers and controls for mitigation.

IoT (Internet of Things) can be seen as a new instrument in the era of technology enhancement. 2015 was the year, where industries were progressively enabling IoT in their organizations. Neisse R. et al. [19] proposed Model-Based Security Toolkits for IoT devices. This toolkit was constituted in a management framework to support both specification and efficient evaluation of security policies of user data protection. This framework addressed two major problems: i) validity of security and privacy of user's data towards IoT. ii) Maintaining trust between IoT technology and individuals. Through a case study in a Smart City scenario, they successfully evaluated its feasibility, performance and concluded that their proposed model successfully gained trust in IoT transactions.

In 2016 Varshney G. et al. [20] proposed Phishing Detection System: Lightweight Phish Detector (LPD). The basic principle of LPD was to discover the right set of features associated with authentic web pages, through popular engines. LPD used two features to check the authenticity of the web page: 1) URL's Domain Name and 2) title of the page. They compared the current search engines that supported anti-phishing approaches and others who used chromes, Firefox, Internet Explorer-like popular search engines and got 92.4% to 100% true negative varying rate and 99.5% true positive rate and concluded that the proposed scheme was accurate enough. In the same year, Deore1 D. et al. [21] presented a survey of different automated software used to protect data. To protect data from the virtual machines, they used different distributed cybersecurity automation framework. In their proposed work, they explained the various techniques used to develop software like: user virtualization, event

log analysis, one-time password, and malicious attack detection along with this some privacy protection was also explored in their proposed work.

Meszaros J. et al. [22] same year proposed a new framework for online services security risk management. This framework was used by both service providers and service consumers. They also performed a case study for the validation of the framework. Threat model and a Risk model were the two key components of the proposed framework. These two models provided a specific feature for online services. Mainly in their proposed work their entire focused was on services used in the public internet environment. With the aim of automated management to detect and prevent potential problems such as identifying traffic behavior patterns, Gilberto F. et al. [23] proposed two anomaly detection mechanisms. These proposed mechanisms were based on statistical procedure principle Principal Component Analysis, Ant Colony Optimization metaheuristic and Dynamic Time Warping methods and the major contribution of the proposed method were in pattern recognition and anomaly detection. SeyedMojtaba H.B. et al. [24] proposed an intrusion detection framework. This framework was based on multiple criteria linear programming (MCLP) and support vector machines (SVM), and tome-varying chaos particle swarm optimization (TVCPSO). The proposed method performed welled in terms of having a high detection rate and a low false alarm rate.

In 2017 Park J. et al. [25] addressed the accessibility issues for the enterprise management system who were providing remote access to their users. They proposed an Invi-server system that addressed this issue. It was designed to protect the secrete server from unauthorized access by keeping IP and MAC addresses that remain invisible from external scanning. They suggested that this Invi-server system could be used to reduce the attacker's surface. They also implemented the prototype of Invi-server which significantly reduced attack surface without affecting the performance of the network. Wagner N. et al. [26] in 2018 proposed an Automatic method for generating segmentation architectures. These segmentation architectures were optimized for security, cost and mission performance. They proposed the concept of network segmentation as a mitigation technique to protect the computer network by partitioning it into multiple segments. It was a hybrid approach that combined Nature Inspired optimization along with cyber risk modeling and simulation. The prototype systems were used to implement the method and demonstrated a network environment under cyber-attacks through a case study. In 2019 Badsha S. et al. [27] proposed a Privacy Preserving Protocol. They addressed that organizations that used this protocol can freely share their private information in encrypted form with anyone and they could know about the future prediction by learning the information without disclosing any information to anyone. They also addressed that through a properly developed decision tree, organizations can predict whether the email received is spam or not.

3 Recent Scenario in Cyber Security

Enoch S. et.al [28] proposed a Temporal Hieratical Attack Representation Model to evaluate the effectiveness of security metrics. They categorized the network into two categories (e.g., first changes in hosts and second in the edge). They used Attack Graphs and Attack Trees Graphical Security Models for dynamic networks for the systematical analysis of security posture by using a security matrix. Most of the time these models were lacking to capture dynamic network (changes in topology, firewalls, etc). There proposed Temporal Hieratical Attack Representation Model has overcome these problems by systematically capturing and analyzing the changes of security in the network. Semerci M.et al. proposed an Intelligent Cyber Security System against Distributed Denial of Service (DDoS) Attacks in communication Networks [29]. The proposed model was consists of two components: A monitor to detect DDoS attacks and a discriminator to detect unwanted users in the system. They deployed their proposed model over a Simulated telephone network evaluated the performance of the model by a high throughput simulation environment. The proposed system detected the attack as well as identifies the attackers, but particularly the proposed model was focused on DDoS attack.
Hajisalem V. et al. [30] proposed a hybrid classification Intrusion Detection System. The proposed system was based on the Artificial Bee Colony Algorithm (ABC) and Artificial Fish Colony (AFC) algorithms. They used Fuzzy C-Means Clustering (FCM) to divide the training data set and Feature selection (CFS) techniques to remove irrelevant features in the data set. If any single deviation was found system considered it as an attack. Whereas the normal IDS system used two techniques for the same: pattern matching and statistical anomaly. There proposed method outperformed as compared to the normal IDS system and achieved a 99% detection rate and 0.01% false-positive rate.Li Y. et al. [31] proposed a framework to facilitate the design of Self-Destructing Wireless Sensors that ensured the security and performance of the wireless sensors. In a proposed framework, a cryptographic self-destructing mechanism was used that enabled autonomous self-destruction in wireless sensors. Self-destructing wireless sensors required the ability to determine that, whether the sensor is lost and if yes then timely the sensitive information should destroy. The proposed framework was capable enough on performing quantitative analysis on the security and performance of wireless sensors.

4 The Challenges of Cyber Security

To develop strong security mechanism which meets all modern requirements is a very complex task. Following are some reasons behind it,

- There are many security mechanisms that are designed so far, but how logically we could select and use the appropriate security mechanism(s) is a subject of concern.

- While designing security mechanisms, potential attacks are always a matter of concern but still in many cases, attacks are designed by looking at problems in present system, therefore an unexpected weakness in the mechanism is possible.
- The dynamic nature of the network system constitutes another challenge to network security, where devices, IMP's, and security elements like firewall, topologies keep changing dynamically.
- Continuously monitor and maintain integrity in security over time is also one of the major issues in overloaded environment.
- Many organizations are facing accessibility issues in providing remote access to their users, because once the network server is connected with the Internet, any host on the Internet can access the server and steal the user's private information.
- Security Validation of IoT devices and maintaining the privacy of user's data while keeping trust among users is very challenging.
- Many organizations are looking to move their most of the data to 'the cloud', which has created a new opportunity for the attackers.

5 Research Gap

Cyber Security in the modern network is difficult to assess because they are dynamic in a configuration such as changes in topology, firewalls, routers, etc. We cannot deny that in existing infrastructure, there are numerous limitations (such as lacking self-awareness, absence of self-organizing mechanism and feedback mechanisms, no ability to diagnose miss-configuration). Many traditional techniques such as data encryption techniques, authenticate mechanisms, firewalls are applied to protect computers and networks. Moreover, Graphical security models such as Attack Graphs and Attack Trees are widely used to systematically analyze the security posture. The basic problem with these models is that they are unable to capture dynamic changes in terms of host and edges in networks. Many other models were applied as a solution to handle dynamic changes at hosts and edges level but not at configurationally. Intrusion detection systems and Intrusion pretension systems are well-known security instruments to the network layer to identifies and block malicious activities if firewalls fail to provide securities but they fail to identify unknown malicious activities. In recent years, to optimize the performance of intrusion detection systems various nature-inspired meta-heuristic techniques such as Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO), and Artificial Bee Colony were applied. But they also failed to provide complete security because of their predictable nature somewhere.

The current cyber security architectures are static therefore usually it is controlled by humans such as systems properties and systems behavior being highly dependent upon human administration to be programmed and told how and what can done. This extensively influences the decision-making procedure and perhaps is the major drawback in the automation of such systems. Therefore, the current architecturesare neither reliable nor robust in nature hence with this no-adaptive behavior, unable to learn or have limited learning capability makes them unsuitable to adapt unexpected situations

in dynamic environment. Therefore, it is important to propose and experiment self-organized and resilient cyber architecture.

6 Conclusion and Future Scope

As the useof integrated technologies has increased, cyber security has receivedthe paramount importance. Static mechanisms are vulnerable to many attacks because of their predictable nature such as centralized control, limited learning capabilities and inability to handle new cases in a frequently changing environment. These features present new challenges, as achieving security is more difficult in dynamic mechanisms.After studyingexisting research work, it is observed to have an automated architecture with proactive defense mechanism. A Hybrid approach could be a solution in the area of cyber security decision support (CSDS) that leverage data-driven methods to generate optimal/near-optimal security decisions in dynamic network conditions.

References

1. Sharma R.: Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research,3(6), 1-4 (2012).
2. Kulkarni S. Urolagin S.: Review of Attacks on Databases and Database Security Techniques. International Journal of Emerging Technology and Advanced Engineering, 2(11), 253-263 (2012).
3. Emil Burtescu: Database Security-attack and control method's. Journal of Applied Quantitative Methods, 4(4), 449-454 (2009).
4. DeorelD. Waghmmare V.:A Literature Review of Cyber Security Automation for Controlling Distributed Data. International Journal of Innovative Research in Computer and Communication Engineering, 4(2), 2013-2016 (2016).
5. Ghate S. Agrawal P.: A Literature Review on Cyber Security in Indian Context. Journal of Computer& Information Technology, 8(5), 30-36 (2017).
6. Homer J. Zhang S. Schmidt D. et al.: Aggregating Vulnerability Metrics in Enterprise Networks using Attack Graphs. Journal of Computer Security, 21(4), 561–597 (2013).
7. Michael Warner:Cybersecurity: A Pre-history, Intelligence and National Security, 27(5), 781-799 (2012).
8. Moradian E., Hakansson A.: Approach to Solving Security Problems Using Meta-Agents in Multi Agent System. In: Nguyen N.T., Jo G.S., Howlett R.J., Jain L.C. (eds) Agent and Multi-Agent Systems: Technologies and Applications. KES-AMSTA. Lecture Notes in Computer Science, vol. 4953, pp. 122-131. Springer, Berlin, Heidelberg (2008)
9. Bedi P., Gandotra V., Singhal A. et al.:Avoiding Threats Using Multi Agent System Planning for Web Based Systems. In: Nguyen N.T., Kowalczyk R., Chen SM. (eds) Computational Collective Intelligence. Semantic Web, Social Networks and Multiagent Systems. ICCCI. Lecture Notes in Computer Science, vol. 5796, pp. 709-719. Springer, Berlin, Heidelberg (2009).
10. Amin S., Cárdenas A., &Sastry S.: Safe and Secure Networked Control Systems under Denial-of-Service Attacks. Lecture Notes in Computer Science, 31–45.Doi:10.1007/978-3-642-00602-9_3 (2009).

11. Nassar M., Stat R., &Festor O.: A Framework for Monitoring SIP Enterprise Networks. Fourth International Conference on Network and System Security.pp.1-8. Doi:10.1109/nss.2010.79 (2010).
12. Fu-Hau h. et al.: BrowserGuard: A Behavior-Based Solution to Drive-by-Download Attacks. IEEE journal on selected areas in communications, 29(7), 1461-1468 (2011).
13. Gandotraa V. Singhala A. Bedia P. Threat-Oriented Security Framework: A Proactive Approach in Threat Management. Elsvier-Procedia Technology, 4, 487 – 494 (2012).
14. A. Roy, D. S. Kim, K. S. Trivedi, Scalable Optimal Countermeasure Selection using Implicit Enumeration on Attack Countermeasure Trees, in: 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). (2012).
15. Almasizadeh J. Adollahi M.: A stochastic model of attack process for the evolution of Security Matrix. Elsevier- Computer Networks, 57(10), 2159-2180 (2013).
16. Dewar R: The Triptych of Cyber Security: A Classification of Active Cyber Defense In : P.Brangetto, M.Maybaum, J.Stinissen (eds.);6th International Conference on Cyber Security 2014, NATO, pp. 7-21. Tallinn (2014).
17. Xinlei Li and Di L.: A Network Attack Model based on Colored Petri Net. journal of networks, 9(7), 1883-1891 (2014).
18. Razzaq A. et al.: Ontology for Attack Detection: An Intelligent Approach to Web Application Security, Computers & Security, 45, 124-146 (2014).
19. Neisse R. et al. SecKit: A Model asked Security Tool Kits for Internet of Things. Elsevier-Computers and Security, 54, 60-76 (2015).
20. Varshney G. et al. A phish detector using lightweight search features. Computers & Security, 62, 213-228 (2016).
21. Ujjwala D. et al.: A Literature on Cyber Security Automation for controlling Distributed Data. International Journal of Innovative Research in Computer and Communication Engineering, 4(2), 2013-2016 (2016).
22. Meszaros J. et al.: Introducing OSSF: A Framework for Online Service Cybersecurity Risk Management, Computers & Security, 65, 300-313 (2016).
23. Femandes G. et al.: Network anomaly detection using IP flows with principal component analysis and ant colony optimization, J. Network. Computer. Appl. 64, 1–11 (2016).
24. Hosseini Bamakan S.M. et al.: An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization, Neurocomputing, 199, 90–102 (2016).
25. Park J. et al.: Invi-server: reducing the attack surfaces by making protected server invisible on networks. Computers & Security, 67, 89-10 (2017).
26. Wagner N. et al.: Automatic Generation of Cyber Architectures Optimized for Security, Cost, and Mission Performance: A Nature-Inspired Approach. Springer. 1-25(2018).
27. Badsha S. et al.: Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (2019).
28. Enoch S.Y. et al.: A Systematic Evaluation of Cybersecurity Metrics for Dynamic Networks. Computer Networks, 144, 216-229 (2018).
29. Semerci M. et al.: An Intelligent Cyber Security System against DDoS Attacks in SIP Networks. Computer Networks, 136, 13-154 (2018).
30. Vajiheh Hajisalem et al.: A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection, 136, 37-50 (2018).
31. Li Y. et al.: Designing self-destructing wireless sensors with security and performance assurance, 141, 44-56 (2018).

32. Ashutosh D. et al.: Exploiting Need Of Data Mining Services in Mobile Computing Environments. Computational Intelligence and Communication Networks (CICN) (2010).
33. Chaure R. et al.: Firewall anomalies detection and removal techniques – A survey. International Journal of Emerging Technologies, 1(1), pp. 71–74 (2010).
34. Ashutosh D. et al.: A comprehensive survey of grid computing mechanism in J2ME for effective mobile computing techniques. Industrial and Information Systems (ICIIS), pp.207-212 (2010).
35. Shishir K. S., S. Jain,: Opinion Extraction & Classification of Reviews from Web Documents. Advance Computing Conference IEEE International (2009).
36. Smita S., Shishir K. S., Tripta T., Atulya K N.,: Handbook of Research on Emerging Technologies for Electrical Power Planning, Analysis, and Optimization (2016).
37. Patel A., et al.: Data of semantic web as unit of knowledge. Journal of Web Engineering (2019).
38. Shandilya S.K., Shandilya S., Deep K., Nagar A.K.,: Handbook of research on soft computing and nature-inspired algorithms, IGI Global, USA (2017).
39. Shandilya S., Shandilya S.K., Thakur T.,: Prioritization of Transmission Lines in Expansion Planning Using Data Mining Techniques. Lecture Notes in Electrical Engineering, (2019).
40. Shandilya, S.K., et al.,: Internet of things security: Fundamentals. Techniques and applications, (2018).
41. Shandilya, S.K., Ae Chun, S., Shandilya, S., Weippl, E., IoT security: An introduction, River Publishers, Denmark (2018).
42. Shandilya, S.K., Sountharrajan, S., Shandilya, S., Suganya, E.: Big data analytics framework for real-time genome analysis: A comprehensive approach, Journal of Computational and Theoretical Nanoscience, 16 (8), 3419-3427 (2019).
43. Suganya, E., Sountharrajan, S., Shandilya, S.K., Karthiga, M.: Mobile cancer prophecy system to assist patients: Big data analysis and design, Journal of Computational and Theoretical Nanoscience, 16 (8), 3623-3628 (2019).
44. Shandilya, Shishir K., Wagner, Neal, Nagar, Atulya K: Advances in Cyber Security Analytics and Decision Systems, Springer, 978-3-030-19352-2, 2020