A Survey of Attack Prediction Approaches in Cyber Security

Varsha Zokarkar[1*] and Kirti Mathur[2]

[1, 2]International Institute of Professional Studies, DAVV, Indore, India

*varshatare39@gmail.com

Abstract. In the age of digitization, Cyber-attacks significantly affect the world. Lots of resources and the economy are compromised due to cyberattacks. Predictions of cyber attacks enable us to handle the attack at the appropriate time, which can save money and resources. This paper surveys the different methodologies used to predict cyberattacks. These methodologies are broadly classified into discrete and continuous models. Discrete model examples are the attack graph, Bayesian network, and Markov model, while time series are examples of a continuous model. Other methodologies used to classify and predict the attacks are machine learning, data mining, and deep learning.

Keywords: Cyber-attack prediction, DDOS (Distributed Denial of Services), Discrete Models, Bayesian Networks, Markov Model

1 Introduction

Today's world is bursting with digital information; all information is stored in digital form and is available online. From banking to grid power control, their servers are connected to the network. It provides ease and flexibility in working, but it also creates new threats, as malicious activities are possible through different types of cyber-attacks.

If a cyberattack occurs, recognizing the attacker's intentions is known as attack projection. Attack intention recognition finds out the ultimate goal of the attacker, which will be helpful in predicting his next move. Attack prediction involves recognizing the type of attack as well as when and where it will take place [1].In intrusion detection, when a specific pattern of anomalies is detected, the intrusion detection system reacts and responds to these anomalies. However, a proactive approach would identify the pattern of anomalies in the past flow of networks and, on the basis of this information, predict future attacks [2].

There are different methodologies to predict cyberattacks, like the attack graph, Bayesian network, and Markov model, which predict on the basis of low levels of alerts. To apply any of these methodologies, either expert knowledge is required to generate the attack plan or machine learning algorithms are required to train these models. Frequent training of these models is also required for each incoming alert.

Data mining and machine learning algorithms are capable of identifying specific types of anomalies. Machine learning is also used to train the model and predict the behaviour of upcoming network flows.

S. Bhalerao et al. (eds.), *Proceedings of the International Conference on Recent Advancement and Modernization in Sustainable Intelligent Technologies & Applications (RAMSITA-2025),*Advances in Intelligent Systems Research 192,
https://doi.org/10.2991/978-94-6463-716-8_75

All these methodologies cannot be useful for predicting the attack ahead of time. As packet flow in a network with reference to time can be characterized as a time series, the statistical properties of time series have been exploited to predict the cyberattack rate. Deep learning algorithms are also useful for classifying and predicting anomalies in network flow based on past raw data. The prediction of attack rates cannot specify the type of attack. We use our methodology to first identify patterns in various types of attacks, then fit those patterns into a time series model and predict the cyber-attack. Cyber-attacks are also a major concern in cloud environments, as all clients are communicating through highly loaded networks so cyber security is a major concern for them.

Preventing cyber-physical systems from cyber-attacks is also a major concern, it impacts national resources and damage will be not only limited to economic aspects but it can create huge losses and any mishap is also possible.
Apart from network flow, a cyber-attack can be predicted due to some abnormal user activity.

These are some prominent attacks in the last two years.
A DDoS attack was observed on the website of the Finnish parliament in August 2022. The government was suspicious that it might be targeted by state-sponsored hackers in Russia [3].

The insurance company CNA Financial employees can no longer access company resources because of a ransomware attack that has locked them out of their computers. The March 2021 attack also resulted in the theft of company data, which prompted CNA Financial to purportedly pay the $40 million settlement price [3].
The All-India Institute of Medical Sciences (AIIMS), New Delhi, had a cyberattack on November 22 that rendered its servers unusable. The attack affected five servers at AIIMS Delhi, and the hackers encrypted 1.3 TB of data [4].

Predictions of cyberattacks enable us to handle the attack at the appropriate time, which can save money and resources. This paper surveys the different methodologies related to prediction of cyberattacks. These methodologies are broadly classified into discrete and continuous models. Discrete model examples are the attack graph, Bayesian network, and Markov model, while time series are examples of a continuous model. Other methodologies are Data Mining, Machine Learning, and Deep Learning, which can be used to identify the attack type and predict cyberattacks.

2 Literature Survey

In the digital era, cyber threats can impact any country's economy, security, and political situation. Foreign countries, organized hackers, terrorists, sabotage groups, and Internal dissatisfaction factors are sources of these cyber threats [5].There are following two ways by which a target can be attacked [6]:

Direct attacks - In this attack, the attacker perceives and recognizes the vulnerabilities of the specific network and using this information tries to control the access of critical

systems or critical information of the specific network. This information can be used by attacker for indirect attacks, for example, exploitation of web vulnerabilities.
Indirect attacks - Attackers exercise multiple layers of attacks to efficaciously achieve the final stage, for example, phishing.

The most important cyber-attacks are:

- Denial of Service (DOS) – In this attack authorized user could not connect to the server, The Attacker flooded messages to that server and utilized all its resources, so the server was not able to serve the authorized user. Attackers can also flood these messages not only from a single source but from a large distributed system (DDOS) which stops all authorized communication [7].
- Logic Bomb – In a logic bomb programmer embeds the code into the program, when a specific event has occurred, it automatically performs destructive actions.
- Sniffers – These are the programs that dig out important information like passwords by observing each packet of the data stream.
- Trojan Horse – destructive code is embedded in helpful programs, which is user is willing to execute.
- Virus – A virus is a corrupt system file, which commonly requires programs, a copy of it inserted into it, and when it is loaded into the memory it corrupts other files. In a virus, human interaction is required to spread it.
- Worms – It is an autonomous program by copies itself computer by computer in a network.
- Botnet – A network is infected by remote-controlled systems, which are used to distribute malware, spam, coordinated attacks and steal messages. Botnets are secretly installed in targeted computers and remotely control malicious activities. It is also known as an electronic soldier.
- Ransomware – It is malicious malware due to which accessing your important PDF, excel file, word file etc. becomes impossible and attacker demands ransom against this attack [8].

Cyberattack projection is to identify the attack patterns and their intentions, but cyber prediction is an early warning system. There have been several approaches used to predict cyberattacks.

2.1 Attack Graph

The attack graph is one approach to predicting the attack. The attack graph consists of states and their associative transition path. Some states are initial states and some are successful states. When an attack occurs, it identifies the initial states and finds out that, is it moving toward a successful state. If it is moving towards a successful state, it warns about the attack.

Kotenko et al. [9] presented a framework to calculate Cyber-Attack Modeling and Impact Assessment Component (CAMIAC) where attack graphs are generated by experts, security metrics are computed in real-time mode, and the attack graph analyses the malefactor and detects the scenario of the current attack in real-time.

Author uses NVD (National Vulnerability Database) for the calculation of CAMIAC. Ghasemigol et al. [10] proposed a forecast attack graph to deal with uncertainty and exchange information on alerts and responses at the time of the attack. A forecast attack graph mainly constitutes an uncertainty-aware attack graph associated with probabilities to deal with the uncertainty of an event, hyper alerts graph in which on the basis of information exchange of intrusion alerts e-correlator information is used to get global IDS alerts, multi-level response graph to response to the attack so that damage should be minimized and dependency graph to show the impact of attack on services. The forecast attack graph model considerably reduces the number of nodes and edges which improves the time complexity with respect to the attack graph. The same author proposed a multi-level response model to provide a high-level view of intrusion responses [11]. This model generates response cost estimates on the basis of intrusion detection alerts, possible attacks, possible damage by attack, and response impact.

N. Polatidis et al. [12,13] proposed an attack graph using a recommender system to predict cyberattacks. In this paper attack graph is generated by using the data source of maritime supply chain infrastructure. The proposed system uses attack graph discovery procedures to recognize attack paths and foresee attacks. The recommendation system collaborative filtering method uses attack path, affected assets, and vulnerabilities as input and predict attacks. The recommender system uses a multilayer collaborative filtering method to improve performance [14].

The attack Graph model (Fig. 1) predicts with low-level alerts but conditional probabilities are not introduced so prediction accuracy is low. Secondly, this model needs expert knowledge to design an attack graph and with time training is required to update it.

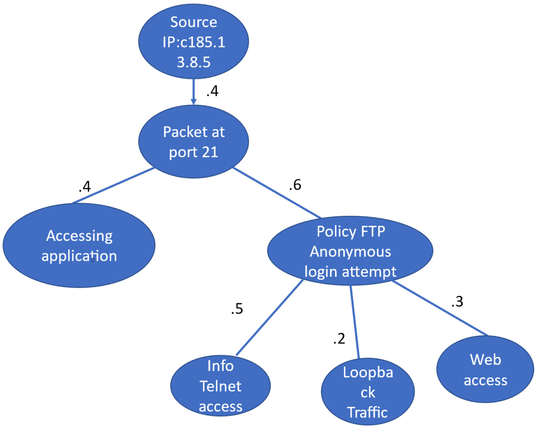
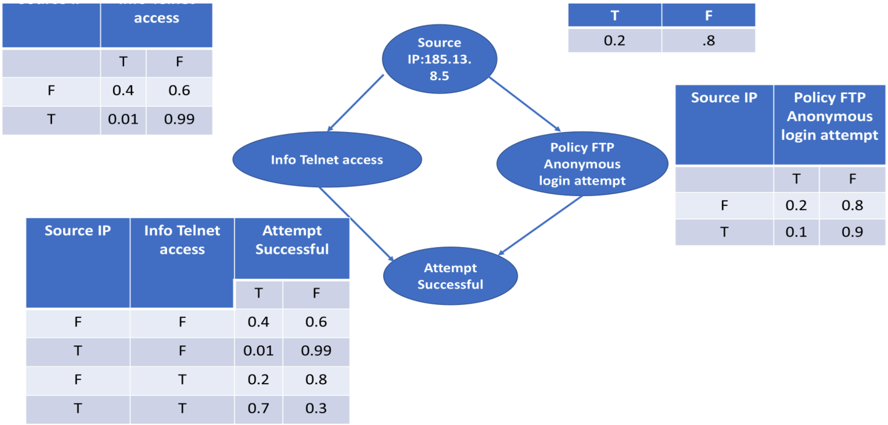


Fig. 1. Uncertainty Attack Graph

2.2 Bayesian Network

Another approach is Bayesian networks (Fig. 2) there are variables and their conditional probabilities are associated with each node. The Bayesian network is a directed acyclic graph, where each node accompanying with a set of variables and the nodes are connected by direct edges. Each variable has a conditional probability table associated with parents P1, P2, and Pn.Qin and Lee [15] presented a methodology to generate alerts of forthcoming attacks based on already-defined attack plans. Initial states indicate the low-level alerts, afterward, a probabilistic interpretation is directed to evaluate the possibilities of the next attack step. The drawbacks of their work is that it requires a comprehensive library of attack plans and that should be updated frequently. If for any specific alert, no plan is available in the library, the proposed model unable to detect the attack, and also misleading plan cannot infer the actual goal of the attacker. Ramaki et al. [16] proposed a real-time alert correlation and prediction framework based on an early warning system to predict multi-step attacks. It works in online and offline mode. In the offline mode, early phases a Bayesian attack graph is constructed from low-level alerts. After that in the online mode, the most probable next step of the attacker is predicted according to the Bayesian attack graph. Framework is tested on DARPA data set and observed 95% accuracy of results.The drawback of the attack graph and Bayesian network model is that building them requires expert knowledge, although they can be trained using machine learning algorithms.



	access	
	T	F
F	0.4	0.6
T	0.01	0.99

T	F
0.2	.8

Source IP	Policy FTP Anonymous login attempt	
	T	F
F	0.2	0.8
T	0.1	0.9

Source IP	Info Telnet access	Attempt Successful	
		T	F
F	F	0.4	0.6
T	F	0.01	0.99
F	T	0.2	0.8
T	T	0.7	0.3

Fig. 2. The Bayesian Network

A. Qkutan et al. [17] proposed a Bayesian network that makes decisions based on unrelated signals captured on the network to predict cyberattacks. The author considered four unconventional signals and trained the Bayesian network for each for DOS, defacement, malicious email or URL, and any other type of attack and predicted the attack.Huang et al. [18] proposed a Bayesian network framework (Fig. 2) to predict cyberattacks on industrial cyber-physical systems and developed an application. Accuracy is better than an attack graph but expert knowledge is required at the initial stage and after that frequent training is required.

2.3 Hidden Markov Model

There is a presence of unobservable states and transitions, then an attack graph and a Bayesian network are unable to identify the attack. In this situation, the Hidden Markov Model removes the dependency on complete information for processing and identifying intrusion detection and attack prediction. This enables successful intrusion detection and prediction of attack is possible even if some steps are missed or cannot be interpreted completely. Hidden Markov Model (HMM), the Variable Length Markov Model (VLMM), and the Variable Order Markov Model (VOMM) are different variants that are used for attack prediction.

Shin et al. [19] proposed a method to identify multistep attacks to gain control of multiple hosts. The author proposed real-time intrusion prediction, which uses HMMs. Zhang et al. [20] proposed the Baum-Welch algorithm to train HMM and forecast the sequence of attacks by the Vitrebi algorithm. It improves the performance of detection and prediction of multistep attacks by trained HMM over untrained HMM. Abraham and Nair [21] proposed a Markov model-based cybersecurity framework for exploitability analysis. Common Vulnerability Scoring System (CVSS) data is calculated to dig out vulnerabilities and predict cyberattacks. Bar et al. [22] proposed a model of attack propagation [23] based on the Markov chain using honeypot data. The proposed model predicts which next honeypot will most likely be attacked and other features are left out for future work. Pilar et al. [24] proposed a novel method to predict multi-step attacks on the base of HMM using intrusion detection system alerts. Supervised and unsupervised machine learning algorithms are used to train the model, and the Viterbi algorithm and forward–backward algorithm is used to predict the sequence of multi-step attacks. The hidden Markov model (Fig. 3) is able to extract the hidden state of attack which is not possible in an attack graph and Bayesian network but still training is required to train the model.

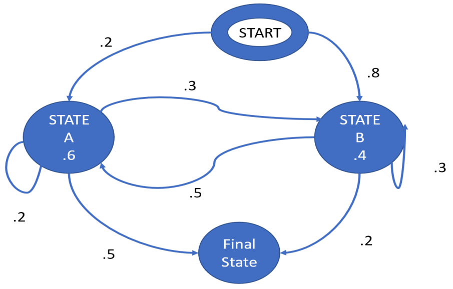


Fig. 3. Hidden Markov Model

2.3 Game Theory

The game theory is an interaction between the attacker and the defender. Game theory methods primarily aim to find the best strategy to defend the most frequent attack detected in historical data. It is useful in identifying especially the prediction of advanced attackers' activity. Lisy et al. [25] proposed a zero-sum game in a scenario of deficient information to find out the attacker's strategy in a situation where the attacker tries to deceive the defender about his goal. Pibil et al.[56] developed a theoretical game model which deliberately creates delay and wastes the resources of the attacker, M. Abdlhamed et al. [26] proposed an intrusion prediction model for the cloud computing environment if the situation is fitted into the theoretical game theory model then prediction has been done by, otherwise prediction has been done based on statistical behavior. Game Theory is a complex procedure, it predicts about next move of the attacker and on that basis, it takes security measures.

2.4 Time Series

Continuous packet flow information with respect to time is a time series consisting of many statistical properties. A collection of data points of features with reference to the time is a time series. A time series is constructed from past data of observed features of a particular activity with time. The network parameters at the time of attacker's activity or network compromising situation state is captured with respect to time and constructs a time series. There are a number of approaches in time series analysis that can be useful in predicting the time series. Park et al. [27] proposed a mechanism for prediction on the basis of randomness in network traffic. The forecast is based on time series analysis and linear regression. Werner et al. [28] used an autoregressive integrated moving average (ARIMA) time series to predict the probable number of attacks the next day. Zhan et al. [29] associated long-term and short-term prediction of cyberattacks using time series with long-range dependency and extreme values by the Fractional Autoregressive Integrated Moving Average (ARIMA) + Generalized Autoregressive Conditional Heteroskedasticity (GARCH) model and achieved an hour-ahead prediction accuracy of 87.9%. Time ahead prediction is possible through a time series model and training is also not required but it is necessary to extract the exact features of time series.

2.5 Machine Learning, Data Mining and Ensemble Model

Different machine learning algorithms are used to train the models in the attack graph and Markov model. Apart from this, data mining is useful for mining the rules for classifying unlabeled data (unsupervised learning). This feature can be used to classify and recognize different anomaly patterns. In machine learning, by training the model, we can predict the cyberattack. The limitation of these is that time-ahead prediction is not possible.

Uwagbole et al. (2017) [30] proposed a mechanism to predict SQL injection attacks based on machine learning. SVM (Support Vector Machine) is used to classify web requests arrived at server so that pattern has been identified for SQL injection attacks and can be projected before a web page starts performing a malicious database query.

Kim and Park [31] used data mining to build an attack graph for attack prediction. Soska and Christin [32] used a decision tree algorithm to automatically detect vulnerable websites before they turned malicious. Traffic statistics, file system structure, and website content were used to create an ensemble of decision trees.

Abel et al. [33] proposed the majority voting (MV) algorithm, which is a combination of logistic regression, decision tree, and SVM to predict malware attacks in a cyber supply chain background. MV performance is equal to the decision tree algorithm, but not much has been achieved. Jaganathan et al. [34] proposed an artificial neural network (ANN) based model for security breach prediction. In this model, the author proposed that biometric features are trained by ANN and stored in the database. When an unauthorized user attempts to get control, it blocks the user. If the user is remote controlled then additional layers are used to identify. The model generates a hash function to access the system. Florina et al. [35] proposed a method based on forecasting and prediction based on three models: clustering, time series analysis, and a genetic algorithm to predict medium- to long-term predictions. Abdulkadir et al. [36] compared eight machine algorithms to predict cyberattacks and found that SVM is most successful in identifying attacks with an accuracy percentage of 95.02%. Husak et al. [37] apply sequential rule mining on large data of security alerts of the SABU platform and determine stable rules, which are useful for predicting the attack. Kriaa et al. [38] generated a knowledge graph using the MITRE ATT&CK framework and then defined rules to query the knowledge graph to find out the evidence of the attack. A knowledge graph convolution network is used to predict the attack.

2.6 Deep Learning Model

Deep learning is very effective at time series estimation. Xing et al. [39] used a deep learning framework for predicting cyberattack rates. A bidirectional recurrent neural network with long and short-term memory accommodates statistical properties exhibited by the cyber-attack rate. The projected model shows higher prediction accuracy than the FARIMA+GARCH and ARIMA models. Mohammad et al. [40] proposed a Gated Recurrent Unit-based deep learning model, which learns future attack dependency on past attack alert sequences. The model is experimented on the Warden alert platform. Most of the predictions (76.31%) belong to good class i.e. error < 0.2 and very few predictions (3.95%) are poor prediction i.e. error > 0.5. Anderson et al. [41] proposed a Cooperative System to Predict DDoS system (COOPRED DDoS) to predict DDoS attacks. The system consists of two software instances: Agent and Intelligent Centre. The agent collects network data from different nodes of the subnet then the system applies an Early Warning System, a statistical process to identify the attack. In the intelligence center, they applied machine learning and deep learning algorithms. The variation in accuracy is from 99.60% to 99.87%. Lin et al. [42] proposed a new iterative adversarial retraining approach to increase the robustness of deep neural networks to detect adversarial attacks by accuracy of 99% on standard test set, specifically, fast gradient sign attacks, Carlini and Wagner (C&W) attacks, Projected Gradient Descent (PGD) attacks, and DeepFool attack. Nusrat et al. [43] forecasts the frequency of cyber-attack using convolution neural network and recurrent neural network with 15% improvement in accuracy.

Husák et al. [44] discussed various facets of cyber defence, further, they chose three methodologies to illustrate with examples and discuss their limitations and research challenges. In the first methodology, data mining is used to dig out frequent attack scenarios and project the attack. An experiment found that the next action of the attacker was projected with 65% accuracy on live data but the projections turned out to be in a few seconds or to be in several hours advance. Methodology is useful in listing out black list of malicious sources but the drawback is that very short time is available to mitigate the attack. In the second methodology machine learning algorithms are used to estimate the probability of malicious IP addresses in a given time window historical data based on network reputation score to predict malicious sources and blacklist them but the drawback is there is no information about the type of attack. In the third methodology time series is used to forecast the attack. In this methodology, high prediction accuracy has been detected but the only prediction of the number of attacks is possible other information about the attack is not available. For experimentation data source SABU, a platform of intrusion detection alerts is used. Programmable networks such as software-defined networks (SDN) are more exposed to attacks like DoS, Man in the Middle, and Zero-day attacks. Ahmed et al [45] Proposed a design open flow model, Markov-based graph model, with a known DoS attack as a node and the relationship between them is edges. The author uses the K-NN classifier to identify k similar flows to identify attack signature and coherent events.

Network situation prediction is the most important aspect in network security so that network administrators can take proper remedial action to mitigate the attack. Guan-yu et al. [46] proposed a forecasting model for network security situations. The proposed model forecasts the network security situation based on a hidden belief rule base when the inputs are multi-dimensional, initial values are provided by the experts, then further it is trained by revised covariance matrix adaption evaluation strategy (CMA-ES) algorithm to improve the forecasting significantly. Manickam et al. [47] proposed an improved adaptive grey Verhulst model for predicting network security situations using the Kerlman filtering algorithm to enhance the prediction. Ghun-yu et al. [48] proposed a cloud belief rule base (CBRB) model that contains the randomness and fizziness of the cloud to decide the parameters then CMA-ES is used to forecast network situation scenarios. Hu et al. [49] proposed hierarchical network security situation prediction on the basis of a belief rule base, which not only predicts the attack but also identifies the source of the attack.

Cyberattack prediction is possible based on user behavior on their social media activity. Peizhi et al. [50] proposed a transparent learning approach to analyse user behavior to predict the attack. The user's daily online activity creates a raw data set, the author applied some encoding to this and generated a user behaviour dataset. The author applied a rule mining module on the user behaviour data set and dug out the rules and a rating is allotted to each user. Whenever a new user performs some suspicious activities as per match with previous rules their rating is predicted.

Clouds have critical and complex infrastructure that is overloaded with network traffic and bottleneck conditions. Cyberattack prediction is a prime concern in the cloud environment. Mohamed et al. [51] proposed a framework for intrusion prediction in the cloud computing environment. This framework is based on a two-phase methodology based on available information. In one phase, where sufficient historical data is available, attack is predicted on the basis of profiling and risk assessment. In the second phase when there is no sufficient data available, statistical methods simple moving average or exponential smoothing are used to predict the attack.

Cyber Physical Systems(CPSs) have complex interactions between heterogeneous cyber and physical components. Identifying attacks in CPSs is not possible through an intrusion detection system. Zero-day attack does not contain any signature to identify the attack so Artificial intelligence-based systems are required to identify the attack [52]. Zhang et al. [53]proposed a multi-layer data-driven cyberattack detection system for industrial control systems. In the proposed detection model KNN, Decision Tree, Bootstrap aggregating, and Random Forest are used to detect five attacks men in the middle (MITM), DDoS, false Data injection, data exfiltration, and data tempering. Kaixing et al. [54] proposed a Bayesian network model to infer the probabilities of sensor and actuator compromises. These probabilities feed to a stochastics hybrid system to predict the risk assessment of industrial CPSs. Mariam et al. [[55] examined three cyber physical systems, a nuclear power plant, an industrial control system, and a vehicular network system, and developed an attack graph model to evaluate the cyber security threats.

3 Conclusion

In earlier stages of Cyber-attack prediction methodologies like Attack Graphs, Bayesian Networks, and Hidden Markov models either experts are required for generation or they should be trained by the machine learning algorithm. In these methodologies frequent pieces of training are required as well as feature identification is a difficult task. Time Series models are able to predict time ahead prediction of attack rate but are not able to identify the type of attack. Machine learning and data mining algorithms possible to predict the type of attacks but time-ahead prediction is not possible. In a Deep Neural network, features can be extracted by training data and prediction accuracy and time ahead prediction both are possible.

References

1. M. Husák, V. Bartos, P. Sokol c and A. , "Predictive methods in cyber defence: Current Experience and Research Challenges," Future Generation Computer Systems, Elsevier, vol. 115, 2021.
2. R. A. Ahmedian and A. R. Ebrahimi, "A survey of IT early warning systems:architectures,challenges, and solutions," Security and Communication Networks, vol. 9, no. 17, pp. 4751 - 4776, 2016.

3. "https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks," Fortinets, 2023. [Online]. [Accessed 2023].
4. N.Thripathi, "https://www.forbesindia.com/article/take-one-big-story-of-the-day/cyberattacks-you-could-be-the-next-target/84223/1," 5 April 2023. [Online]. [Accessed June 2033].
5. Q. L. Youchoung Li, "A comprehensive review study of cyber attack and cyber security; Emerging trends and recent developments," Energy Reports,Elsevier, vol. 7, 2021.
6. Enbody, A. Sood and R. , Targeted Cyber Attacks, Syngress.
7. D. Kwon, H. Kim, D. An and H. Ju, "“DDoS Attack Volume Forecasting Using a Statistical Approach,”," in IFIP / IEEE symposium on Integrated Network and Service Management, 2017.
8. S. Camelia, G. Christopher, B. Joseph and G. Sharad, "“I was told to buy a software or lose my computer. I ignored it”:A study of ransomware," in USENIX Symposium on Usable Privacy and Security (SCOUPS), Santa Clara, CA, USA., 2019.
9. Konteko and A. Chechulin, "A cyber attack modeling and impact assessment framework," in 5th International Conference on Cyber Conflict(CYON2013),IEEE, June 2013.
10 M. Ghasemigol, A. Ghaemi-Bafghi and H. Takabi, "A comprehensive approach for network attack forecasting," Computers & Security,Elsevier, vol. 58, pp. 83-105, 2016.
11. M. GhasemiGol, H. Takabaj and G.-B. , "A foresight model for intrusion response management," comuters & Security,Elsevier, vol. 62, pp. 73-94, 2016.
12. N. Polatidis, E. Pimenidis, P. Pavlidis and H. Mouratic, "Recommender systems meeting security:From product recommendation to cyber attack prediction.Cham: Springer International publishing," Engineering Applications of Neural Networks,Springer, pp. 508-519, 2017.
13. N. Polatidis, E. Pemenidis and H. Mouratic, "From product recommendation to cyber attack prediction: generating attack graphs and predicting future attacks," Evolving Systems,Springer, 2018.
14. Georgiadis, N. Polatidis and C. K., "A multilevel collaaborative filtering method that improves recommendations," Expert system and Applications,Elsevier, vol. 48, pp. 100-110, 2016.
15. W. Lee and X. Qin, "Attack plan recognition and prediction using causal networks," in Computer Security Applications Conference, 2004.
16. A. A. Ramaki, M. Amini and R. E. Atani, "RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection," Computers & Security,Elsevier, vol. 49, pp. 206-219, 2015.
17. A. Okutan and S. J. Yang, "Predicting Cyber Attacks with Bayesian networks using unconventional signals," in Annual Conference on Cyber and Information Security Research CISRC,2017, ACM, 2017.
18. K. Huang, C. Zhou, Y. C. Tian, S. Yang and Y. Qin, "Assessing the physical impact of cyberattacks on industrial-physical systems," IEEE Transactions on Industrial Electronics, vol. 65, pp. 8153 - 8162, Oct2018.
19. S. Shin, S. Lee, H. Kim and S. Kim, "Advances probablistic approach for network intrusion forecasting and detection," Expert Systems with Applications, vol. 40, 2013.
20. Y. Zhang, D. Zhao and J. Liu, "The application of Baum-Welch Algorithm in multistep attack," Recent Advances in Communications and Networking, vol. 2014, 2014.
21. S. Nair and S. Abraham, "Exploitability analysis using predictive cybersecurity framework," in IEEE, Gdynia, Poland, June 2013.

22. A. Bar, L. Rokach, M. Unger and B. Shapira, “Identifying Attack Propagation Patterns in Honeypots Using Markov Chains Modeling and Complex Networks Analysis,” in IEEE, Beer Sheva, Israel, 2016.
23. "Scalable attack propagation model and algorithms for honeypot systems," in IEEE, Washicton, DC, USA, Dec 2016.
24. "Real-Time Multistep Attack Prediction Based on Hidden Markov Models," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, vol. 17, no. 1, JANUARY/FEBRUARY 2020.
25. R. P'ibil, V. Lisy, C. Kiekintyeld and B. Bo'sansk'y, Game therotical approach to adversarila plan recognization, vol. 242, ECAI, 2012, pp. 546-551.
26. M. Abdlhamed, K. Kifayat, Q. Shi and W. Hurst, "A system for intrusion prediction in cloud computing.," in ACM DIGITAL LIBRARY, Newyork , USA, 2016.
27. H. Park, D. Jung, H. Lee and H. P., "Cyber wheather forecasting: Forecasting unknown internet worms using randomness analysis," Information Security and Privacy Research, Springer , 2012.
28. J. G. werner, S. Young and k. McConky, "Time Series Forecasting of cyber attack intensity," in ACM, New York, 2017.
29. M. X. a. S. X. Z. Zhan, Z. Zhan, M. Xu and S. Xu, "Predicting cyber-attack rates with extreme values," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, 2015.
30. S. O. Uwagbole, W. J. Buchanan and L. Fan, "Applied machine learning predictive analytics to SQL Injection Attack detection and prevention," in IFIP/IEEE symposiym on Integrated Network and Service Management, Sept. 2017.
31. Y. H. Kim and W. H. Park, "A study on cyber threat prediction based on intrusion detection event for apt attack detection," Multimedia Tools and Applications, Springer, vol. 71, no. 2, Jul 2014.
32. K. Soska and N. Christin, "Autometically detecting vulnerable websites before they turn malicious," in 23rd USENIX Security Symposium, ACM, 2014.
33. A. Yeboah-otori and C. Boachie, "Malware attack predictive analytics in cyber supply chain context using machine learning," in International conference on Cyber Security & Internet of Things, Accra , Ghana, 2019.
34. J. Jagannathan and M. Y. Mohamad Parves, "Security Breach Prediction using Artificial neural network," Measurement - Sensors, ELSEVIER, vol. 24, 2022.
35. K. Florian, T. Budig, E. Goebel, T. Fischer, J. Muff and M. Wienes, "Attack Forcast and Prediction," in 28th Computer and Electronics security application(C&ESAR 21), Rendezuous, 2021.
36. A. Bilen and A. D. Ozer, "Cyber-attack method and perpetrator prediction using machine learning algorithms," PeerJ Computer Science, 2021.
37. M. Husak and J. Ka ´ spar, "Towards Predicting Cyber Attacks Using Information Exchange and Data Mining," in 14th International Wireless Communications & Mobile Computing Conference (IWCMC) , IEEE, Limassol, Cyprus, June 2018.
38. Chaabane, S. Kriaa and Yahia, "SecKG: Leveraging attack detection and prediction SecKG: Leveraging attack detection and prediction," in 12th International Conference on Information and Communication Systems (ICICS),IEEE, Valencia, Spain, 2021.
39. X. Fang, M. Xu, S. Xu and P. Zhao, "A deep learning framework for predicting cyber attack rates," EURASIP journal on Information Security , Springer, 2019.
40. M. A. Ambusaidi, X. He, P. Nanda and Z. Tan, "Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm," IEEE Transaction, vol. 65, no. 10, pp. 2986-2998, 2016.

41. A. B. d. Neira, A. M. d. Araujo and M. Nogueira, "An Intelligent System for DDoS Attack Prediction Based on Early Warning Signals.," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, vol. 20, no. 2, pp. 1254 - 1266, 2022.
42. J. Lin, L. L. Njilla and K. Xiong, "Secure machine learning against adversarial samples at test time," EURASIP Journal on Information Security, Springer, 2022.
43. Nusrat, Samia, S. Saha and A. Haque, "Predicting and mitigating cyber threates through data mininining and machine learning," Computer Communications,Elsevier, 2024.
44. M. Husák, V. Bartos, P. S. c and a. A, " Predictive methods in cyber defence: Current Experience and Research Challenges.," Future Generation Computer Systems, Elsevier, vol. 115, 2021.
45. A. Aleroud and I. Alsamadi, "Manage cyber attacks on software defined networks:An inferense-based intrusion detection approach," Journal of Network and Computer Applications, ELSEVIER, vol. 80, 2017.
46. G.-y. Hu , Z.-J. Zhou, C. Zhang and Xiao - J, "A method for predicting the network security situation based on hidden BRB model and revised CMA-ES algorithm," Applied Soft Computing, Elsevier, vol. 48, 2016.
47. Manickam, Y.-B. Leau and Selvakumar, "An Enhanced Adaptive Grey Verhulst Prediction Model for Network Security Situation," nternational Journal of Computer Science and Network Security, vol. 16, no. 5, May 2016.
48. H. WEI, G.-Y. HU, X. HAN, P. QIAO, Z. ZHOU, Z.-C. FENG and X.-J. YIN, "A New BRB Model for Cloud Security-State Prediction Based on the Large-Scale Monitoring Data," IEEE Access, vol. 6, 2017.
49. Q. Hu, C. Li, Y. Fang and Z. Wa, "Hierarchical Network Security Situation Prediction Based on Belief Rule Base," in CCRIS '20: Proceedings of the 2020 1st International Conference on Control, Robotics and Intelligent System, 2020.
50. P. Shao, J. Lu, R. K. Wong and . W. Yang, "A Transparent Learning Approach for Attack Prediction Based on User Behavior Analysis," in Information and Communications Security(ICICS 2016), Springer International Publishing, 2016.
51. Yassine, A. Mohamed and Zinedine, "Feature selection based on pairwise evalution," Intelligent Systems and Computer Vision (ISCV),IEEE, pp. 1-6, 2017.
52. "Cyber Security Based on Artificial Intelligence for Cyber-Physical System," IEEE Network, 2020.
53. F. Zhang, H. Angel Dia, E. Kodituwakku and J. W. Hines, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data," IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, vol. 15, no. 7, JULY 2019.
54. K. Huang, C. Zhou, C. Zhou, Y.-C. Tian, S. Yang and Y. Qin, "Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems," IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, vol. 65, no. 10, OCTOBER 2018.
55. M. Ibrahim, Q. Al-Hindawi, R. Elhafiz, A. Alsheikh and Omar, "Attack Graph Implementation and Visualization for Cyber Physical Systems," Process , MDPI, vol. 8, 2020.
56. R. p'ibil, V. Lisy, C. Kiekintveld and B. Bo, "Game therotical model of strategic honeypot selection in computer networks," Decision and Game Theory for security,Springer, 2012.