Privacy Preservative Dimensions of Machine Learning with Cypher Security Issues

[1] Prakash N, [2] Dr. Janarthanam S, [3] Dr. Shanthakumar M
1, 2Assistant Professors of Computer Science, Gobi Arts & Science College, Gobichettipalayam. Erode.
3Assistant Professor of Computer Science, Kamban College of Arts & Science, Sulur, Coimbatore.

Abstract : Machine learning is one of the most fundamental techniques in computer science and extensively applied in image processing, natural language processing, pattern recognition, cyber security and supplementary fields. Regardless of successful applications of machine learning algorithms in many circumstances, e.g., object recognition, malware detection, and intrusion detection. The globally connected systems and devices stricken by the intrusion not solely digital world as within the past however conjointly the physical world through the web of Things (IoT) and therefore the social world through present social media platforms. To tackle these issues must come up with countermeasures. In this article, the author firstly analyzes the security and reliability issues existing in computer networks, and then proposes some opinions on how to deal with the current computer network security issues, aiming to discuss this together with extensive customers to enhance the awareness of computer network security protection.

Index Terms **- Anomaly detection, Artificial intelligent, Cypher security, Machine learning, Network security, Privacy.**

I. INTRODUCTION

Recent innovative technological developments of network communications, virtualization of manufacturing processes and data analysis with Big Data analytics and cloud computing enables effective mass customization in industrial production. The goal of combining production methods with state-of-the-art ICT to create value chains to serve specific needs of consumers faces certain challenges. These challenges range from standardization of communication to legally securing the sensitive information pertaining to various factors involved [1].

In the network, there are a lot of viruses and hackers damaging network security, and some deliberate cyber-crimes impose huge threats to information security. Machine learning is one of the most popular research fields, and its effectiveness has been validated in various application scenarios, e.g., pattern recognition, network intrusion detection, autonomous driving, etc. The general approach observed towards developing ML based security applications is, training the models using labeled network traces obtained with some experimental environment, with a comprehensive set of intrusions and abnormal behavior along with the normal behavior.

The advent of huge knowledge has stirred broad interests in machine learning and privacy problems by facultative corresponding algorithms to disclose a lot of fine-grained patterns and create a lot of correct predictions. Cypher security is the set of applying security preventions to provide the integrity and availability of data [2]. As a basic technology of future intelligent society, machine learning shall unendingly expedite its theoretical study, rule style and development and security related datasets are extremely rare, mostly due to privacy issues.

II. LITERATURE REVIEW

2.1 Machine Learning

Internet of Things is a network of Internet-enabled objects like as sensors and smart devices with applications in smart homes, smart cities has intelligent transportation [3]. The interconnection of physical objects provides efficient data collection and sharing in IoT applications, although there is also underpinning security concerns the potential data or privacy leakage. Hence the area of focus to design an effective and provably secure access control schemes to protect related resources against unauthorized access or modification.

The privacy enhancing techniques concentrated on allowing multiple input parties to collaboratively train ML models without releasing their private data in its original form. This was in the main performed by utilizing cytological approaches, or differentially-private knowledge. Differential privacy is very effective in preventing membership reasoning attacks. to handle various security threats towards machine learning, several researchers devote themselves to propose some defensive techniques to safeguard learning algorithms, models and systems.

Basically, defensive techniques of machine learning consist of security assessment, countermeasures in the training phase, and countermeasures in the testing or inferring phase, data security and privacy. Furthermore, the advances of security threats and defensive techniques regarding machine learning are promoted alternatively, resulting in a more powerful and intelligent analysis.

2.2 Analysis Techniques

Multivariate data analysis techniques [2] such as multivariate correlation analysis, covariance and maximum likelihood ratio are used for network anomaly detection [4]. Recently, some surveys on the security perspective of artificial intelligence and machine learning have been presented [1] [5]. For the security issues of artificial intelligence especially the supervised and reinforcement learning algorithms [6]. On the opposite hand, Paltzer et al. reviewed existing works regarding security problems and

corresponding defensive ways within the life cycle of a machine learning-based system from coaching to logical thinking [7]. Completely different from previous surveys and reviews, this survey targets a comprehensive literature review concerning security threats and defensive techniques throughout coaching and testing or inferring of machine learning from an information driven read. Particularly, it emphasizes the data distribution drifting caused by adversarial samples and sensitive information violation problems in statistical machine learning algorithms.

For instance Lei et al. projected AN attack strategy approach victimization spoofing and electronic jamming so as to interfere with the most range of signal channels. The approach used distributed power usage on each spoofing and electronic jamming attacks by applying dynamic programming and was evaluated by subsequent experiments. However, this approach is most applicable to the facility grid infrastructure. The authors of a previous paper official. [18] Projected a dynamic energy-aware cloudlet-based mobile cloud computing model (DECM) that focuses on finding extra energy consumptions throughout wireless communication in a very grid atmosphere.

Agrawal et al. propose an answer for vary queries on numerical knowledge that permits convenient categorization. Their resolution is made on AN encryption that preserves the order of the numerical knowledge in every column. *Consequently, if a database intruder observes the encrypted data, he learns the order of all cells in every column, which is a significant amount of information. They give no rigorous analysis quantifying the information leak of their solution.*

A follow-up by Chang and Mitzenmacher [9] has interesting analysis but their solution is restricted to searching for a keyword chosen from a pre-determined set. Boneh et al. present a searchable public key scheme [6]; the scenario they considered is analogous to that of [8] but uses public-key encryption rather than symmetric-key encryption. In the same scenario, demonstrates a method for secure indexes using Bloom filters [15]. These solutions are possibly useful in searching for keywords in a file; however, it is unclear how to apply them to the problem of efficiently querying encrypted relational databases.

III. DIMENSIONS OF INTERACTIONS

In this section the operationalization takes the least amount of time for addressing legal and policy issues takes more time, at least several Hardware, e.g., new processor architectures, typically takes more to materialize.

3.1 Building trust through accountability

Cyber security systems may seem a highly technical topic best left to a small group of expert computer scientists. However, the most formidable challenges for the future of ML are likely to be social in nature. While ML promises to improve security by automating some aspects of defense, caution is needed for the creation, deployment, and use of these systems. Unless developed and used very carefully, ML may irretrievably damage national security, economic stability, and other social structures, safety nets of legal and ethical constraints are needed. Building a world—a social, ethical, and legal context that is ready for the incorporation of ML matters as much as the creation of the technical systems themselves.

In 2016, the Mirai botnet publicized the arrival of a brand new class of attack: distributed denial of service (DDoS) attacks meted out by botnets consisting entirely of vulnerable IoT shopper devices. Despite these devices having comparatively very little computing power, Mirai yet succeeded in DDoS to a number of the best-defended websites on the net [3]. A strong legal response will be needed to rebuild public trust in ML. Up to now, however, courts and regulators in most countries are slow to assess legal liability for damage arising from code malfunction. This reticence will need to change in the context of ML.

3.2 Technical Human Factors

The selection of knowledge sets will probably suffer from style of sampling errors and biases. every work sample will have a selected degree of sampling error, and this error desires analysis and revelation to avoid creating a false sense of confidence throughout a express work methodology. Fully different work methodologies will vary in success primarily based, in part, on the extent of this sampling error. Builders of ML systems should also disclose the extent of any affirmative steps they have taken to avoid sampling bias in selection. In other words, they should articulate why they are confident that the sample used for training data is accurately representative of the entire population of real-world deployment situations that the ML system is likely to encounter.

ML coaching failure occurred in March 2016 once Microsoft introduced Tai, associate "AI chatbot" on Twitter. among in the future, Twitter users "taught" Tai to spout racist and Nazi information [13], a extremely undesirable outcome from Microsoft's perspective. most significantly, like each rigorous scientific method, the activity and choice processes with reference to coaching knowledge ought to be replicable by freelance third parties.

Replicable activity processes, at the side of what social scientists decision "interrater reliability" checks, build confidence and trust. It is through this level of rigor, planning, and transparency that builders can re assure both users and policy makers, their systems are well built to the extent, possible protected against malfunctioning in catastrophic ways.

3.3 Data and Information Frontiers

In 2014, the International Data Corporation reported that the amount of data was doubling every year and would reach 44 zeta bytes (44×10^{21} bytes) by 2020 [18]. This data includes from individuals, devices, technical networks, social networks, and various applications. As security AML requires large and diverse data sets for effective training and the networks that the ML will be

applied to produce significant amounts of real-time data, it is clear that data represent a critical dimension. To be effective, security ML algorithms must be trained on large, diverse training data sets. As such, the effectiveness of the algorithms is directly proportional to the amount and quality of the information. Whereas massive coaching knowledge sets area unit usually on the market, one challenge is that the completeness of the information. Existing devices associate degreed networks weren't originally designed with instrumentation and activity as an integral feature.

Relevancy and integrity area unit extra factors related to knowledge. Whereas simulated knowledge sets area unit convenient to come up with, they're usually artificial as a result of they are doing not properly encapsulate reality and also the human dimension of adversarial actions. in addition, to be effective, knowledge sets should be regularly updated in order that they embrace the foremost recent evolution of threat results. Knowledge that doesn't embrace the foremost recent attack knowledge cannot be effective against those attacks. Data integrity affects both the effectiveness of and confidence in ML. Data assortment techniques, by their terribly nature; usually embody unintended human and technical biases. Understanding, documenting, and sharing those biases are important to ensure ML effectiveness and operation. Data integrity also affects human confidence in ML. If the ML training data set is incomplete, includes questionable biases, or is, in general, not fully understood, then confidence in the entire system is diminished [14]. Preprocessing of the data prior to use for training can also alter data integrity and reduce confidence.

Because data in the cyber security domain continue to grow at an increasing rate, it is important to consider alternative algorithmic approaches those abstract threat anomalies from the data level to higher-level ensemble indicators [10]. Characterizing common attack patterns will allow ML models to focus on features that predict outcomes. Additionally, rare threat events, whereas probably devastating are typically underrepresented during a probabilistic model that encompasses all threats. As a result, there is a need within the ML development community to devise a feature-engineering approach.

3.4 Cypher Security and Hardware for ML

The network is not any longer outlined by the equipment at intervals the physical protection of buildings and campuses. Today, the network consists of human users connected by mobile devices anyplace within the world and autonomous devices broadcasting sensing element info from remote locations. therefore Hardware is Associate in Nursing integral a part of this resolution in 3 ways. the primary is by integration security into hardware device styles [11]. The second is by making hardware network architectures that may showing intelligence monitor the network's security state. The third is by making hardware that permits AI/ML systems to unravel a lot of advanced issues by eliminating existing cypher barriers.

As a result of IoT and mobile devices typically lack the procedure power required to run advanced security computer code, security should be embedded at intervals the hardware of the devices themselves. The devices should become the line of defense, or they'll be wont to alter attacks. This was shown within the October 2016 DDoS attack [21], [22] during many DVRs and webcams were reborn into botnets by the Mirai malware so wont to launch never-ending and big stream of traffic that resulted in motility down Netflix and different major websites. Within the extremely competitive, cheap surroundings of the IoT, it's arduous to convert device makers to commit style time and resources to implementing these options. Customers wished to be assured that the devices they bought wouldn't be a danger to their homes and families. All that they had to try to was rummage around for the "UL" seal. This, additionally to product safety standards wrong fully obligatory by acceptable restrictive bodies, forced makers to feature safety options to their product to sell them. An identical UL-like seal for security is required. Sadly, despite having been mentioned for years and a few recent efforts being created, the thought has ne'er been enforced at scale. We'd like to treat cyber incidents in an exceedingly manner kind of like ancient safety incidents.

Today's laptop design was designed to try and do advanced calculations on comparatively little amounts of information. This design isn't suited to the kind of computations performed by trendy mil systems. mil algorithms notice clusters info or associations to attach determined information along then offer context for the observations. This context permits the machine to grasp the perceived world and build selections regarding the way to answer what the system is observant [16]. To accomplish this, mil algorithms method an oversized quantity of information and perform comparatively easy operations (e.g., matrix multiplications) on those information. This can be a essentially totally different process paradigm from what's common nowadays. owing to this disconnect, mil needs an oversized quantity of computing hardware to try and do the coaching, thereby precluding the time period threat assessment and response needed by cyber security for brand new threats.

To solve this downside, pc architects got to basically amendment their approach to computing. We'd like to require a lot of data-centric approach, specializing in however information flow through a processor and a less processor-centric approach focuses on however computations are done. This effort ought to be principally business targeted, with the govt taking part in a supporting role in encouraging the event of those systems. To modify milliliter systems to construct an in depth model of a situation, developers are challenged to quickly perceive traditional and threatening eventualities and their associated feature area at a high level.

Typical cyber security information sets are very massive, networks for information delivery and therefore the process of milliliter models should be capable of with efficiency handling staggering amounts of numerous information. The deficiency of such networks nowadays could be a major hindrance to progress within the field. Achieving such networks for period analytics needs even a lot of careful code style and algorithms.

IV. DEFENSIVE TECHNIQUES

In the previous decades, existing works essentially centered on the fundamental ideas and models of security dangers against machine learning. Lowd et al. Proposed the idea of ill-disposed learning in 2005 [13], and Barreno et al. expressly researched the security of machine learning in 2006, including the scientific classification of assaults against machine learning frameworks and the ill-disposed models [14]. To address assorted security dangers towards machine learning, numerous specialists dedicate themselves to propose some cautious methods to ensure learning calculations, models and frameworks. Fundamentally, protective procedures

of machine learning comprise of security appraisal, countermeasures in the preparation stage, and countermeasures in the testing or inducing stage, information security and protection.

Because of the restrictions of human's intellectual methodologies, the imperfections in framework plan and designing practice are unavoidable, which shapes organize asset vulnerabilities. The center of system assault and barrier is centered on the use of system asset defenselessness [17]. The run of the mill hostile and guarded modes are presented in this area. In view of the root wellspring of the lopsided circumstance the protective sides are broke down. As broadly acknowledged digital slaughter chain is a multistage section type nosy model proposed by Lockheed Martin participation [3] depicts the regular meddling personal conduct standard with two phases. Left-of-abuse is to accumulate data and build ambush weapons store. Aggressors investigate and bolt focused on framework amid surveillance. Additionally, as indicated by the investigated system highlights, assailants define assault apparatuses and strategies. Right-of-abuse of digital execute affix is principally to do assault conduct and broaden the harm scope. At that point, the wanted conditions of focused frameworks can be accomplished. Moreover, aggressors abuse comparable vulnerabilities to upgrade the hostile viability. From the attitude of defenders, existing defensive methods can be mainly divided into block embedded defense and structure remodeling defense. For instance, access control adds access control policy as the blocking rule to prevent unauthorized access. After that, attackers cannot access system to induce the sensitive info they require [19].

As a result, sensitive information in a system can be protected. Regardless of the universality of this kind of method, absolute obstruction, it becomes more and more difficult for the appearance of side channel attackers. Besides, the conflict and space for storing explosion of policy sets emerge with the rise of the amount of rules added. As for structure reworking defense methodology, it mainly copes with the inherent flaw of targeted systems. Structure reworking methodology makes network resource vulnerabilities unusable by inserting plug-ins and mend. For instance, upgrading system security can fix some vulnerability in the system. Attackers cannot launch attacks without exploiting corresponding vulnerabilities.

From the viewpoint of protectors, existing cautious techniques can be chiefly separated into square implanted barrier and structure renovating guard. For example, get to control includes get to control strategy as the blocking standard to avoid unapproved get to. From that point onward, aggressors can't get to framework to get the delicate data they need. Thus, delicate data in a framework can be secured. Despite the all-inclusiveness of this sort of strategy, outright impediment, it turns out to be increasingly troublesome for the presence of side channel aggressors. Also, the contention and storage room blast of strategy sets rise with the expansion of the quantity of standards included [18,19]. Concerning structure rebuilding safeguard technique, it for the most part adapts to the characteristic imperfection of focused frameworks. Structure renovating technique makes arrange asset vulnerabilities unusable by embedding modules and fixing. For example, updating framework security can settle some weakness in the framework. Aggressors can't dispatch assaults without misusing relating vulnerabilities.

The homogeneity of system components gives the living space to assailants to extend the harm scope. Aggressors can compromise the whole system framework by just discovering one blemish. Besides, the regular weakness can be abused in various frameworks in numerous assaults. Then again, safeguards need to apply diverse cautious means exhaustively in order to accomplish antivirus and fixing vulnerabilities. In addition [17], with the end goal to enhance the security of focused frameworks, safeguards need to moderate all vulnerabilities. Subsequently, the normally successful assault implies and the thorough cautious methodology prompts the cost preferred standpoint of assailants.

As the system framework will in general be joined, robotized, keen, and confused, the sharp differentiation between assailants embracing straightforward techniques, little apparatuses, and different vulnerabilities to dispatch viable interruption with protectors actualizing complex methodologies, facilitated instruments, and complete organization further disturbs the asymmetry circumstance of the cautious side. Moving target safeguard [12] empowers us to make, investigate, assess, and send instruments and techniques that are various and that persistently move and change after some time to expand multifaceted nature and cost for aggressors, limit the presentation of vulnerabilities and open doors for assault, and increment framework versatility.

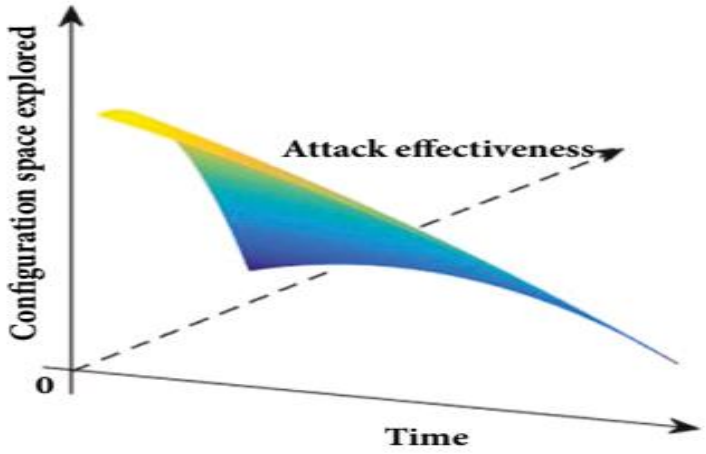

Figure 1. The trend of attack over time under moving target defense mechanism

In the meantime, the abused vulnerabilities and assault way developed additionally increment persistently. In addition, with the homogeneity of system components, aggressors can abuse comparable vulnerabilities and develop secondary passages to expand the harm scope.

As needs be, the data asymmetry of assailants and safeguards turns out to be less and less. Besides, despite the fact that assailants can misuse vulnerabilities and develop assault way effectively, assault time will be compacted with the time-fluctuating of the framework. In this manner, the time hole among aggressors and safeguards is getting littler and littler. Finally, regardless of whether aggressors can actualize meddling activities effectively, they are difficult to accomplish high advantage with minimal effort due to the assorted variety of framework shown in figure 2. By brushing the consequence of master involvement with that of machine learning [11], it guarantees the precision of technique age and the adequacy of component usage. The architecture transits from proactive defense architecture to reactive defense architecture. Furthermore, it gradually develops into architecture with availability. In order to balance the pro activeness and pertinence during defense, defense architecture with inevitability combines the advantage of proactive defense and reactive defense. It adopts predefined transformation therefore on succeed defense while not detection. In the method of defense implementation, architecture with availability analyzes the state of the targeted system in real-time and formulates more targeted defensive strategy by adopting strategy generation, mechanism deployment, and effectiveness evaluation. Consequently, it improves the self-adaptive defense. Besides, as the application scenarios tends to be distributed in deployment, complex of targeted system structure, and complicated in operation and maintenance, command and control are also gradually transformed from manual or automatic way singly into the combination of expert experience and automation, thus improving the efficiency of defense deployment. According to the composition of the architecture, this section summarizes three key parts, which are strategy formulation, transformation mechanism, and effectiveness evaluation is to generate the optimal defense strategy that meets the expected safety goals when analyzing existing network conditions and potential security threats.

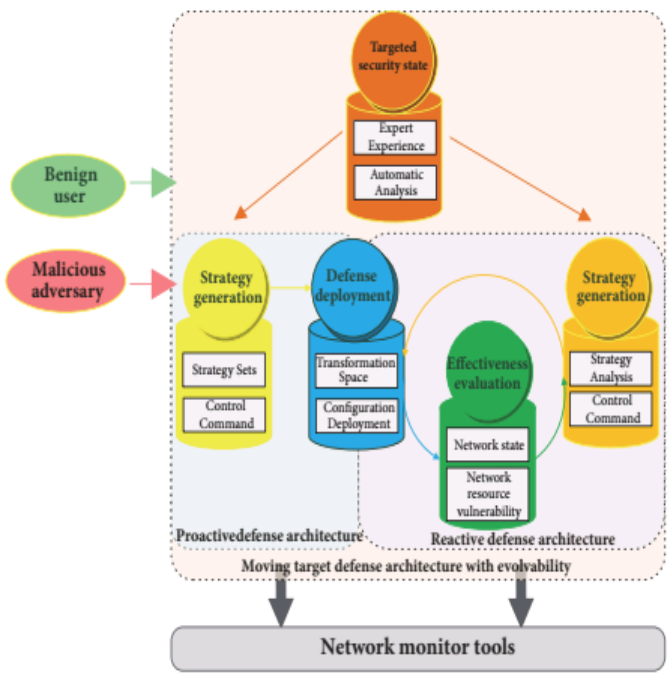

Figure.2. Different Moving defensive architecture

4.1 Strategy Formulation Based on Game Theory

Game Theory [5] is a kind of strategic selection method to achieve maximum benefit of each rational player in the pattern of mutual interest. The equilibrium of game is that the steady state of rational players once no player will increase their own profit by dynamical their strategy unilaterally. Dependency and non-cooperative options in network confrontation are extremely compatible with the feature of theory of games, thus making the optimal strategy selection based on game theory becoming one of the hotpots to study. This model formulates defensive strategy by analyzing the exaggerated performance overhead of targeted system and therefore the impact on the attack implementation. Carter et al. [9] proposed leader follower game model so as to describe the self-learning features of attackers under incomplete information condition. By analyzing the transformation impact on attackers and system performance consumption below static attack and self-adaptive attack conditions, severally, it shows that maximizing platform distinction will increase the aptitude of resisting attacks effectively.

4.2 Strategy Formulation Based on Machine Learning Control Theory

Machine learning control theory [12] is a new discipline formed by the intersection of machine learning and control theory. Control theory is used in control system [13], in which controller with corrective function is adopted to control process variables to ensure the correctness of system operating. Machine learning [14] uses statistics and optimization methods to efficiently and accurately analyze the complex environment. Therefore, combining machine learning and management theory will solve the management improvement drawback within the complicated system. Rowe et al. [13] proposed diversity transformation approach

based on control theory. Security state assessment rule is adapted to research network security state initially. As a result, it determines triggering time. In the in the meantime, defense cost in different defense strategies is evaluated by quantifying implementation overhead. Therefore, it selects defensive strategy by guaranteeing each defensive effectiveness and low overhead. Adams et al. [23] compare open-loop with closed-loop defense systems; it verifies that the compensation feature of closed-loop system can reduce the input interference effectively. Besides, it shows that the multi elements uncertainty will make the growth of complexity following necessary difference law.

Strategy formulation achieves evolution by comprehensively analyzing network standing changes and offensive and defensive dynamic sequences. Consequently, multi objective reinforcement learning algorithm is designed to obtain the optimal security strategy so as to minimize attack surface and maximize configuration diversity. For the high computational complexity of optimal strategy generation, by analyzing the defensive computational complexity in known special parameter domain and the entire parameter domain, it shows optimal defensive strategy in familiar special parameter domain convergences in polynomial complexness and defensive strategy formulation in remaining parameter domain convergences in an exponential complexness.

4.3 Strategy Formulation Based on Evolution Theory.

Evolution theory [20] is a set of theories that explain the developmental variation among biological generations by genetic and observable phenomena. On the one hand, the unit of evolution is cluster, and genetic diversity is an important factor in evolution. On the opposite hand, natural selection is the major contributor to evolution. It affects the phenotype of species in its environment. Since a number of functional equivalence isomer constitutes the network executor of the components can be considered as different genomes on chromosomes. At constant time, offensive and defensive behaviors lead to the constant change of network environment.

Crouse etal. [14] Proposed strategy generation method to improve the diversity of genetic algorithm. It quantifies the load of configuration parameter cluster consistent with the influence on system security and victimization closing date. Eventually, the variety of configuration parameter is improved by change body pool, and the parameter group with the highest weight is selected as the optimal strategy. It consists of configuration house exploration module supported organic process algorithmic rule, transformation implementation module, and evaluation module based on expert experience. Two types of organic process algorithms square measure accustomed explore the set of configuration parameters achieving constant operate and therefore the same security goal, respectively. Consequently, the resilience of targeted system is enhanced by choosing optimum strategy. Winter rose et al. [15] proposed strategy selection method for diversified platform with time-varying. Malicious someone evolution technique is analyzed supported European nation genetic algorithmic rule. As a result, investment bias measuring is adopted to live the complexness and advantage of defense.

V. CONCLUSION

Analyzing existing defense strategy formulation studies, it can be concluded as follows: strategy formulation based on game theory formalizes objective opposition, the dependency among players, and the non-cooperativeness during network confrontation process as game models. As a result, the previous deciding is achieved on the idea of analyzing offensive and defensive confrontation things. Strategy formulation supported theory of games becomes the thought technique in strategy generation. Furthermore, on the one hand, so as to boost the accuracy of network system awareness, machine learning management theory is adopted. On the opposite hand, evolution theory can be used so as to achieve targeted network system deduction. The connected theory study and key techniques square measure summarized. Finally, challenges and future directions during this field square measure mentioned to supply a reference for additional analysis and further research.

REFERENCES

[1] A. Shameli Sendi, Y. Jarraya, M. Pourzandi, and M. Cheriet, Efficient provisioning of security service function chaining using network security defense patterns,IEEE Transactions on Services Computing, pp. 1-1, 2017.
[2] C. Lei, D.-h. Ma, H.-q. Zhang, and L.-m. Wang, "Moving target network defense efectiveness evaluation based on change-point detection," Mathematical Problems in Engineering, vol. 2016, 11 pages, 2016.
[3] Cheng Lei , Hong-Qi Zhang, Jing-Lei Tan, Yu-Chen Zhang, and Xiao-Hu Liu , Moving Target Defense Techniques: A Survey Hindawi Security and Communication Networks, Volume 2018, 25 pages.
[4] D. M. Adams, D. S. Hitefeld, and B. Hoy, "Application of cybernetics and control theory for a new paradigm in cybersecurity," Cryptography and Security, 2013.
[5] E. Alpaydin, Introduction to Machine Learning, MIT press, 2014.
[6] H. Maleki, S. Valizadeh, W. Koch et al., Markov modeling of moving target defense games, Journal of Cryptology, Pp. 47–83, 2016.
[7] H. Zhou, C. Wu, M. Jiang et al., Evolving defense mechanism for future network security, IEEE Communications Magazine, Vol. 53, No. 4, pp. 45–51, 2015.
[8] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Adversary-aware IP address randomization for proactive agility against sophisticated attackers," in Proceedings of the 34th IEEE AnnualConference on Computer Communications and Networks, IEEE INFOCOM Hong Kong, Pp. 738–746, , May 2015.
[9] J. Rowe, N. K. Levitt, and T. Demir, Artifcial diversity as maneuvers in a control theoretic moving target defense, in Proceedings of the National Symposium on Moving Target Research, 2012.
[10] L. M. Winter rose and K. M. Carter, Strategic evolution of adversaries against temporal platform diversity active cyber defenses, in Proceedings of the Symposium on Agent Directed Simulation, 9 pages, 2014.

[11] M. Atighetchi, B. Simidchieva, M. Carvalho, and D. Last, Experimentation support for cyber security evaluations, in Proceedings of the 11th Annual Cyber and Information Security Research Conference, CISRC 2016, April 2016.
[12] M. Carvalho, T. C. Eskridge, K. Ferguson-Walter, and N. Paltzer, MIRA: a support infrastructure for cyber command and control operations, in Proceedings of the Resilience Week, RSW 2015, pp. 102–107,August 2015.
[13] M. Conti, T. Dargahi, and A. Dehghantanha, "Cyber threat intelligence: challenges and opportunities," in Cyber Treat Intelligence of Advances in Information Security, Springer International Publishing, vol. 70, pp. 1–6, , 2018.
[14] M. Crouse, W. E. Fulp, and D. Canas, Improving the diversity defense of genetic algorithm-based moving target approaches, in Proceedings of the National Symposium on Moving Target Research, 2012.
[15] M. K. Carter, F. J. Riordan, and H. Okhravi, A game theoretic approach to strategy determination for dynamic platform defenses, in Proceedings of the First ACM Workshop on Moving Target Defense, Pp. 21–30, 2014.
[16] P. K. Manadhata, "Game theoretic approaches to attack surface shifting," in Moving Target Defense II, Advances in Information Security, Springer, New York, NY, USA, Vol. 100, pp. 1–13, 2013.
[17] R. Zheng, W. Lu, and S. Xu, Preventive and reactive cyber defense dynamics is globally stable, IEEE Trans on Network Science and Engineering, 2017.
[18] R. Zhuang, S. A. DeLoach, and X. Ou, "A model for analyzing the effect of moving target defenses on enterprise networks," in Proceedings of the 9th Annual Cyber and Information Security Research Conference (CISRC '14), pp. 73–76, April 2014.
[19] R. Zhuang, S. A. DeLoach, and X. Ou, "Towards a theory of moving target defense," in Proceedings of the 1st ACM Workshop on Moving Target Defense (MTD '14)—Co-located with 21st ACM Conference on Computer and Communications Security (CCS'14) Scottsdale, Ariz, USA,, pp. 31–40, November 2014.
[20] V. Heydari, S.-I. Kim, and S.-M. Yoo, Anti-censorship framework using mobile IPv6 based moving target defense, in Proceedings of the 11th Annual Cyber and Information Security Research Conference, USA, April 2016.
[21] X. Liang and Y. Xiao, Game theory for network security, IEEE Comm. Surveys & Tutorials, Vol. 15, No. 1, pp. 472–486, 2013.
[22] Y. Huang and A. K. Ghosh, "Introducing diversity and uncertainty to create moving attack surfaces for web services," Advances in Information Security, vol. 54 pp. 131–151,2011.
[23] Y.-B. Luo, B.-S. Wang, X.-F. Wang, and B.-F. Zhang, A keyed hashing based self-synchronization mechanism for port address hopping communication," Frontiers of Information Technology and Electronic Engineering, Vol. 18, No. 5, pp. 719–728, 2017.