Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 4, April -2017

SECURITY OPTIMIZATION OF DYNAMIC NETWORK WITH OPTIMAL DEFENSE STRATEGY AND INTRUSION DETECTION

M.S.Muthuselvam[1]
PG Scholar
Department of Computer Science and Engineering
Coimbatore Institute of Technology
Coimbatore, India

A.N.Senthilvel[2]
Assistant Professor, Senior Grade
Department of Computer Science and Engineering
Coimbatore Institute of Technology
Coimbatore, India

Abstract *– Network security has become more important to personal computer users, organizations and the armed forces. With the beginning of the internet security became a major concern and the history of security permits a better understanding of the emergence of security technology. Acquiring the networks of large organizations is technically challenging due to the multipart configurations and constraints. A network administrator needs to identify vulnerable configurations, as well as tools for hardening the networks. Unauthorized intruder or attacker into a computer system or network is one of the most serious threats to computer security. Many of them try to access the resources of an unauthorized person to win their business. The proposed methods identifies the attack hosts with the help of two models (i) success predictable model attain the expected chance vulnerability attacks in a network, and block the repeated IP address with the help of intrusion detection (ii) security enhancement model implement the optimal defense strategies with a method of secured login system by three matching pattern is used identify the intruder and hackers for wired devices and wireless connections. This will help to secure data in large organizations*

Keywords *- Intrusion detection, large organizations, vulnerability, Network security, optimal defense strategy.*

I. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. The Network administrators need to analysis and response to newly discovered vulnerabilities with security policy and modifications of network configuration to utilizing defensive security for complex networks to minimize the risk from external attacks.

Existing work utilizes attack graphs for analyzing the security risks by quantified graphs analysis using a range of techniques, such as Bayesian belief propagation basic laws of possibility and vertex ranking algorithms .These models lack an organized and scalable performance of optimized network configurations. Existing attack graph quantification models assume a network with known and fixed configurations in terms of the connectivity, availability, and policies of the network services and components disregard the dynamic of modern network. Moreover, with the exception of few attempts precise techniques for risk fall have not been reported.

As an application that predicts the security risk as the attack graph for an expected chance of successful attacks. The proposed system of the two models that denoted to as a (i) Success Predictable Model (SPM), Security Enhancement Model (SEM) has more than four different layers such as confidential, sensitive, private and public. The layers featured with a goal to finding the possible layer is vulnerable and check the maximum attack capabilities by considering dynamic network features and the check the availability vulnerable attack of mobile devices in the dynamic network.

The new contribution can achieve the goal for a large organizations level in which the networks can be positioning for four different layers. It can be categories with these layers named confidential, sensitive, private and public. The layers can be executed in hierarchical order. The functions implemented by these layers (i) the layers can be upload any type of file and stored in a file server. (ii) The layers categories for accessing the other layer data is vulnerable, so it predict the expected chance of successful attack and to develop an attack graph for the vulnerable host with the affected layer and file type.(iii) The system can find the vulnerable host and block the repeated IP address and the file. (iv)The value to check the complex network features of huge organizations and the check availability of portable devices in the network

The Network administrator needed to enquiry and comeback to recently exposed weaknesses with security strategy and alterations of network configurations. The optimal network proposed an application realize a method called, secured login system which lies under the security enhancement model. The system implements three different login matching patterns like color matching, key stroke and it includes the password. These three prevent the highly security level of users login.it helps

to reduce the attack goals from any unauthorized user from both inside and outside organization via wired and wireless devices.

This paper is organized as follows. Section II, briefly summarizes the related work. Section III, provides the description of the System overview. Section IV, describes the Methodology in detail. Section V, presents the Experimental results and analysis. Conclusions and future work are given in Section VI. The Final part is References.

II. RELATED WORK

The literature has a various number of attempts of getting an attack node by using different models, probabilistic algorithms and various tools can be used to solve this problem of security in large networks. The various analysis of security attacks in organizations to execute a proposed model to guarding against the attackers. The effort of survey produces the various results for securing data and lacks a comprehensive accurate methodology of different graph analysis tools and classification of algorithms. The major methods to follow the security in any networks are probabilistic attack graph and raking algorithms are comparing the vulnerabilities. In the subsequent, it grants a systematic comparison of our effort with the associated learning followed by a summary of the work.

A. Probabilistic Graph Analysis

Defending large enterprise networks is very difficult. A defender must be able to locate all paths into the network and prevent attackers from using them. The system builds multiple-prerequisite graphs, or MP graphs, which are faster to build and have greater expressive power than from the previous work's that Net SPA Tool access the predictive graphs [1]. MP graphs are able to model portable credentials, such as passwords, which an attacker can use from anywhere to compromise a target In addition to network-specific data, the system requires additional knowledge about vulnerabilities. Nessus can identify the hosts, interfaces, and ports on a network, pin pointing where vulnerabilities are. Attack graphs are a useful tool in the arsenal of network defenders. Vulnerability scanners such as Nessus report large severity in isolation [2]. The strength in [3] converses an understanding of the metric and an experimental to compute the metric. In this paper [4], suggest a risk controlling framework using Bayesian networks that enable a system administrator to quantify the chances of network compromise at various levels. In this identical of work, the approaches provide a success predictable model that generalizes the method by catching the insecurity in attacker's choices.

B. Ranking

The dependency of a ranking method by resources of state listing attack graphs [5]. The knowledge of PageRank is realistic to state listing attack graphs with a revised analysis of the ranking. Attack graphs built on ideal checking have been proposed in [6] reinforcing an intrusion attack in a finite state model. Authors in [6] do not suggest a complete attack graph ranking method. The indication of PageRank is realistic to state listing the attack graphs with a improved clarification of the ranking algorithm. Attack graphs created on model testing have been suggested in [6] formalizing an interruption attack in a finite state model. By means of an alternative, a system to calculate nominal critical attack effects based on user-specified metrics has been introduced. Asset Rank [7] was planned to rank any dependence attack graph using a chance of walk model. Asset Rank is a justification of PageRank enlargement it to handle both conjunctive and disjunctive nodes. Asset Rank is maintained by an essential probabilistic clarification based on a random analysis walk for the both nodes.

C. Security Improvement

Enumerated attack graphs or comparable formalism are mainly useful when applied as a basis for refining the security of a network. The authors in [4], [8] proposed solutions for the security hardening problem as a multi unbiased optimization difficulty. The main advantage of the work compared to the use of genetic algorithms in [8] is that formulate the security hardening problem as a general mathematical programming problem that is directly developed according to an attack graph. The accurate software design problem offered in this paper can be expanded to reflect a variety of constraints to converse as a forthcoming direction. Moreover, the problem of the work differs in the research goal as that focus on reducing the achievement rates of attackers, whereas the work in [8] is on optimizing costs (similar to [9]) and reducing damages. Noel and Jajodia offered a greedy solution for the problematic of the best placement of IDS sensors in a network using attack graphs [9]. The clarification that finds a minimal number of sensors that can cover all critical attack paths. Wang et al. recommended a method for outcome the (early) conditions that need to be removed to improve network security [10]. Both these solutions target at rearranging the networks to increase security. In contrast, the total effort that provides network hardening solutions beyond network reorganization. These models support the computation of optimal network security defense approaches.

III. SYSTEM OVERVIEW

A network is definite as a two or more computing devices connected together for allocating resources efficiently. Additionally, fixing two or more networks organized is known as internetworking. As an outcome, the Internet is just an internetwork – a group of interconnected networks. For setting up its internal network, an organization has several possibilities. It can use a wired network or a wireless network to connect all workplaces. Currently, organizations are mostly using a grouping of both wired and wireless networks.

A. Network Security

In this present-day communication, organizations greatly depend on computer networks to share information throughout the organization in a well-organized and dynamic manner. Organizational computer networks are currently suitable for a large and pervasive. Assuming that each staff member has a dedicated workstation, a large scale company would have few thousands workstations and many server on the network. The synchronous network that contains of shifts does not defense data and consequently the data are not vulnerable by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet. It is to be expected that these workstations may not be centrally managed, nor would they have edge protection. They may have a variation of operating systems, hardware, software, and protocols, with different level of cyber consciousness among users.

At this moment visualize, these thousands of workstations on company network are directly connected to the Internet. This sort of unsafe network becomes a goal for an attack which holds valuable information. The foremost goals of network security are Confidentiality, Integrity, and Availability. These three maintenances of Network Security are often signified as CIA triangle.

The function of confidentiality is to protect treasurable business data from unauthorized persons. Confidentiality part of network security makes sure that the data is offered only to the intended and authorized persons, Integrity this goal incomes maintaining and promising the accuracy and uniformity of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons. Availability is the function of availability in network security is to make sure that the data, network resources are persistently available to the sincere users, when they require it.

B. Vulnerabilities & Attacks

The common vulnerability that exists in both wired and wireless networks is an unauthorized access to a network. An attacker can connect his device to a network though unsecure hub/switch port. In this concern, wireless network are considered less secure than wired network, because wireless network can be certainly retrieved without any physical connection. After accessing, an attacker can exploit this vulnerability to launch attacks such as:

a. Sniffing the packet data to steal valuable information.
b. Denial of service to genuine users on a network by saturating the network medium with fake packets.
c. Spoofing physical identities (MAC) of legitimate hosts and then stealing data or further launching a man-in-the-middle attack.
d. Trojans perform to be benign platforms to the user, but will essentially have some malicious purpose. Trojans typically carry some burden such as viruses.

To inhibit all the above attacks different prevention methods and systems can be used. The difficult of the approaches can be resolved by intrusion detection with optimal defense strategy in proposed system.

C. Intrusion Detection

An Intrusion Detection is a method used for monitoring the network and protecting it from the intruder. By the rapid growth in the internet based expertise new application zones for computer network have emerged the fields like business, financial, industry, security and healthcare divisions that the LAN and WAN applications have improved. All of these application sectors made the network of an attractive target for the mismanagement and a vast vulnerability for the different organization the goal of intrusion detection is to monitor the network resources to detect unusual behaviour and misuse in network. There are two types of an intrusion detection method such as Host-Based ID, Network-Based ID. Host based ID observe the indication of intrusion in the home-group system. For enquiry they use host organization logging and other information. HID are used efficiently for considering the network attacks, for example, it can sometimes tell exactly what the attacker did, which directives he used, what files he opened, rather than just a unclear complaint. The advantage of the HID is

validating the chance of success attack in that network. Network based ID systems collect information from the network itself rather than from each separate host. Network Node ID agents are deployed on every host within the network being protected with this security.

D. Optimal Security Defense Strategy

The proposed system of Security Enhancement Model (SEM) achieves the technique of optimal security to inhibit and reduce the attackers or intruders are entering into the network. The secured login system is the optimal defense strategy of entire network with the help of three matching types of security which are corresponding to the arrangement of the individuals. The arrangements are listed that follows: key stroke, color matching and the secure password. The key stroke make the users can execute the pass rate that are easily reminds there achieve a secure level of confusing the attackers. Another arrangement named as a color matching, this leads to create a three different color matching with the key stroke pass rate and secure password. These all three arrangements are to optimize the security of users and to reduce the attack of data or any individual information.

IV. METHODOLOGY

The methodology of the proposed system is followed by the wide-ranging research goal of emerging optimized network security circumstances. The level of efforts preceding the difficult of attainment a hard impose of a more predictable network strategy, moreover security defense approaches with the goal of reducing the chance of a successful large-scale attack in dynamically varying and multi-part network architecture. The proposed system performs the new procedure which monitors two models. There is a requirement for a highly consistent and precisely rigorous platform to bearing an effective security reinforcing analyses.

The Figure (1) represented the flow diagram of the system architecture to achieve the goal to reduce the attackers in complex network organizations. The Success Predictable model (SPM) and Security Enhancement Model (SEM) are the two important models to analysis the performance and the level of vulnerability attack in complex networks. To secure the hardening of huge network complications and to reduce the attackers is the main objective of the proposed system executed by this methodology.

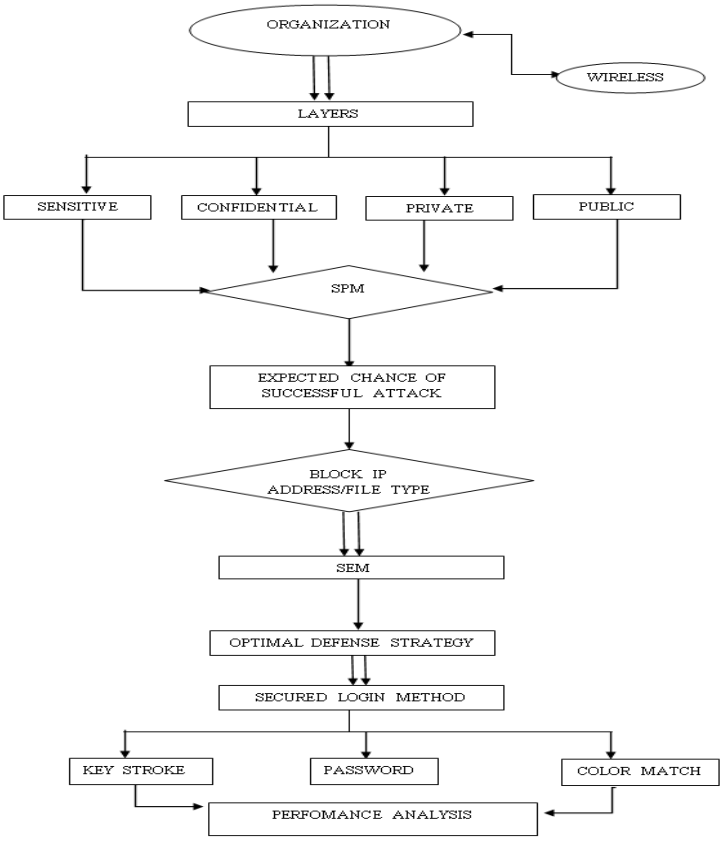


Figure-1 Flow Diagram of Proposed System

The technique understands the huge organizations and to develop four different types of layers named as sensitive, confidential, private and public. The figure (1) represent the flow diagram above layers is performing individual users and data's can be stored in file server. The organization can normalize by the administrator. The admin manage all the details of every user and permit to access their individual users. These different layers are categorizing the levels of their induviduals.The main process of the technique is to complete with the help of two most important models which define as a security optimized range of complex architecture in huge organizations. The proposed models are described as bellow.

A. Success Predictable Model

In this section describes the proposed system of the first model Success Predictable Model (SPM) to figure out the expected chance of successful attacks on a network with respect to the corresponding ultimate four layers of multi-part organization. The layers which are having a more information of data's that are organize and secured by administrator. The success predictable model complete by the process that confidential layer has permitted to access the private and public files but for sensitive files the attackers can't access, because the layers are performed by hierarchical level to reduce the attack levels. The attackers or intruder may access the sensitive file.
The SPM model signifies to identify the vulnerability of an attack node in a large network. The analysis of vulnerability attack can be represented by graphical method with the help of repeated attacks on the layers of multi-part organization. To overcome these successful attacks, this model proposed to block the particular and repeated IP address in those layers.

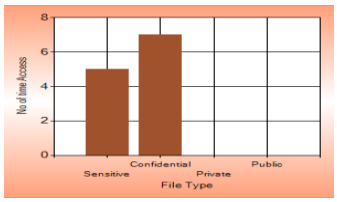


Figure-2 Expected Chance of Successful Attack

The figure (2) represent the excepted chance of successful attack is happen at that node. The intrusion detection algorithm helps to detect the vulnerability and block the repeated IP address and also the file type of vulnerable layer. The intrusion detection algorithm is mainly used for monitoring the network and protecting it from the intruder. The algorithm can differentiate by two types, Host ID and Network ID.The SPM succeeds both the IDs which allow the known packets and reduce the vulnerability attacks. The progression of IDA follows:

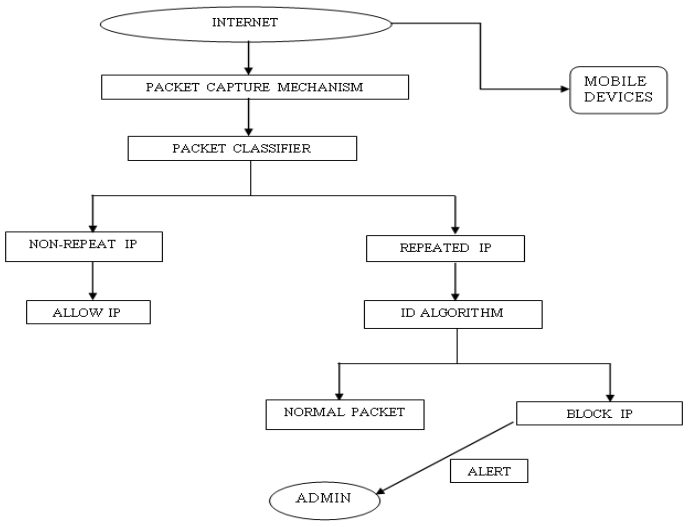


Figure-3 Intrusion Detection Mechanism

The main achievement of the goal is to find an expected chance of successful attack in complex organization. The analysis of vulnerable attacks in a network that inhibits by figure (3) represented ID mechanism realizes their functions.

To improve the security level of network and to reduce the attackers with the help of improvement model such as Security Enhancement Model (SEM) is to analysis by three matching pattern goals. The optimal defense strategy is the major functions with the process of three matching pattern under the method called as a secured login system. This method can reduce the attackers in the networks.

B. Security Enhancement Model

To achieve the main research goal of reducing expected chance of success in an attack, and to improving the overall security of the network, that fact out the essential characteristics of this difficult as an optimization security for every individuals with the help of Success Predictable Model (SPM). In Security Enhancement Model (SEM) complete the process of specific security of every individual in a multi-part network organization by using secured login system with the help of figure(4) representing the three matching patterns.

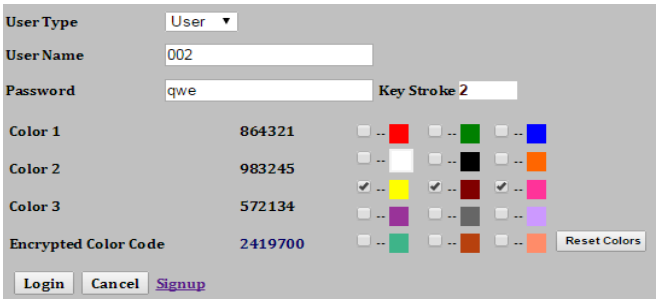


Figure-4 Three Matching Pattern

a. Key *Stroke*

The current access systems prompt users to validate themselves with a username and password pair. The underlying assumption is that each individual presents a unique typing pattern when using the keyboard to enter words that the user is familiar with, for example, passwords and user or account names. The keystroke patterns might derived in the method of the timing delays between successive key pairs, duration though pressing a key, or even the pressure applied on distinct keys on the keyboard and it is hard to collect intruder or hackers when the key stroke progresses.

b. *Color Matching*

The Security procedure of another pattern is color matching. The different colors are organized in a matrix representation with unique color ids to identify the individuals in a complex organization. This can be used by the users can access their ids. The color pattern may vary from different users, so the color key values help to secure the information's of induviduals.The improvement of secure login system help to manage their data and to reduce the vulnerability attacks in a network.

c. *Secure Password*

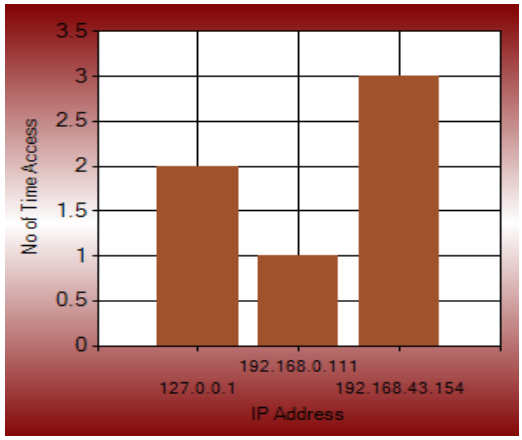
Alternative arrangement of security enhancement model allows a secure password to enquire their ids the pattern of the password to be unique performance of all the keyboard keys which functions like uppercase, lower case numerical values and symbols. The above methods are already used pattern for different organizations and individuals. By the help of above two patterns the security of user's login method is hardly confidential and secured.

EMPLOYEES ATTACKERS LIST:

username	password	attackdate	attacktime	ip	matchpercent	
emp01	45678	2/2/2017	4:59 PM	127.0.0.2	80	Delete
emp002	12345	3/28/2017	12:22 PM	127.0.0.1	0	Delete
emp002	123	3/28/2017	1:22 PM	127.0.0.1	66	Delete
001	12345`	3/28/2017	2:02 PM	2001:0:9d38:6abd:4d7:3648:62cc:f696	0	Delete
002	12345	4/1/2017	11:10 AM	2001:0:9d38:90d7:1880:146e:ce31:69b	80	Delete
EMP022	1233	4/1/2017	2:20 PM	127.0.0.1	0	Delete
m137	ma	4/4/2017	2:39 PM	2001:0:9d38:6abd:341b:2e2d:231e:72e6	0	Delete

Figure-5 Users Intruders

The entire three patterns achieve their functions and this optimal security defense strategy mainly executes the result of figure (5) representing the intruders or hackers are accessing their ids without knowing by individuals. The result showed with the help of secured login system.



IP	No of Time Access
127.0.0.1	2
192.168.0.111	1
192.168.43.154	3

Figure-6 Accessed IP Address

The Figure(6) represented the performance of the secured login system also display the repeated IP address access by the hacker or intruder and send a warning message to administrator which block the users affected data for a certain period that follows the large organizations performed by this proposed by Security Enhancement Model (SEM). Finally the optimal security executes a performance analysis by calculating the performance of the two models handling in the multi-part network.

V. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the practical evaluation of the work. The two models performs with the methods by figure (2) and figure (5) represented by the performance of these models. By these two models the proposed system achieves the goal to reduce the attackers in the large network in huge organizations. The figure (7) representing the matching percentage of original pattern of individuals by using the secured login system of analysing the intruders or hackers in our organization.

Tried Date	Accessed Date	Accessed Filename	Accessed IP	Member	Username
4/1/2017	3/24/2017	flower1	127.0.0.1	Hacker	001
4/1/2017	4/1/2017	muthu	127.0.0.1	Intruder	EMP022
4/1/2017	12/1/2017	flower	192.168.0.1	Hacker	EMP022
4/1/2017	12/1/2017	muthu	192.168.0.1	Intruder	EMP022
4/4/2017	4/4/2017	flower	127.0.0.1	Hacker	m137
4/4/2017	4/4/2017	calendar	127.0.0.1	Hacker	m137

Figure-7 Display of Attacker List

Depends upon the attacker list the result can be calculating with the performance analysis of the proposed model figure (8) representing the performance time for the optimal strategy of the Security Enhancement Model.

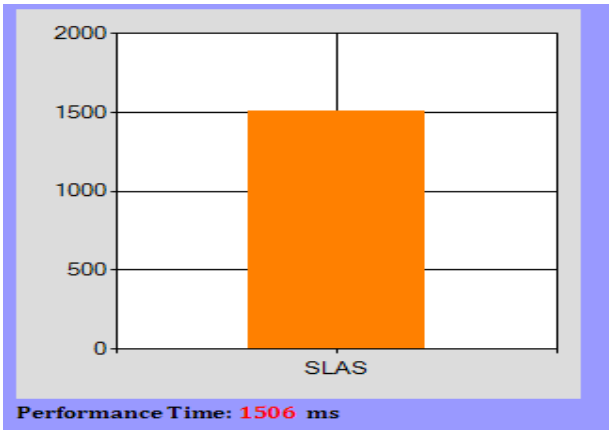


Figure-8 Performance Analysis of SEM Model

The Performance time of the proposed system can be performed with secured login system and the algorithm for this method. This can be checked the last login date and IP address and the accessed file. Therefore the system perform to reduce the vulnerability attacks in any network will follow by this models.

VI.CONCLUSION AND FUTURE WORK

In this work we dignified, executed, and assessed a new file organizations of four different layers for evaluating the security threats in multi-part networks. The originality of work is the capability to realize the expected chance of successful attack in the existence of uncertainties around the arrangement of a dynamic network and directions of probable attacks and to reduce this attack by the security enhancement model For future work, we plan to exploit and extend our success predictable model and the performance analysis of optimal security of defense strategy of secured login system to solve more complex network security optimization difficulties. Further we performed the result of the both wired and wireless devices.

REFERENCES

[1] K. Ingols, R. Lippmann, and K. Piwowarski, "Practical attack graph generation for network defense," in Proc. Compute. Security Appl. Conf., 2015, pp. 121–130.
[2] S. Jajodia, S. Noel, and B. O'Berry, "Topological analysis of network attack vulnerability," in Managing Cyber Threats: Issues, Approaches and Challenges, V. Kumar, J. Srivastava, and A. Lazarevic, Eds. Norwell, MA,USA: Kluwer,2013, Ch. 5.
[3] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, "An attack graph-based probabilistic security metric," in Proc. 22nd Annu.IFIP WG 11.3 Working Conf. Data Appl. Security, 2008, pp. 283–296.
[4] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using Bayesian attack graphs," IEEE Trans. Dependable Secure Compute., vol. 9, no. 1, pp. 61–74, Jan. 2012.
[5] V. Mehta, C. Bartzis, H. Zhu, E. Clarke, and J. Wing, "Ranking attack graphs," in Recent Advances in Intrusion Detection, vol. 4219.New York, NY, USA: Springer Berlin, 2011, pp. 127–144.
[6] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing. (2002).Automated generation and analysis of attack graphs, in Proc.IEEE Symp. Security Privacy.
[7] R. E. Sawilla and X. Ou, "Identifying critical attack assets independency attack graphs," in Proc. 13th Eur. Symp. Res. Computer Security: Compute. Security, 2008, pp. 18–34.
[8] R. Dewri, N. Poolsappasit, I. Ray, and D. Whitley, "Optimal security hardening using multi-objective optimization on attack tree models of networks," in Proc. 14th ACM Conf. Compute. Commun.Security, 2014, pp. 204–213.
[9] M. Albanese, S. Jajodia, and S. Noel, "Time-efficient and cost-effective network hardening using attack graphs," in Proc.42ndAnnu.IEEE/IFIPInt.Conf.DependableSyst.Netw.,Jun.2012,pp.1–12.
[10] L. Wang, S. Noel, and S. Jajodia, "Minimum-cost network hardening using attack graphs," Compute. Common. vol.29, no.18, pp.3812–3824, Nov.2012.

