An Adaptive Decision-Support Model for Data Communication Network Security Risk Management

Akinyemi Bodunde Odunola
Department of Computer Science and Engineering, Obafemi Awolowo University, Ile- Ife, Nigeria

Amoo Adekemi Olawumi
Department of Computer Science and Engineering, Obafemi Awolowo University, Ile- Ife, Nigeria

Olajubu Emmanuel Ajayi
Department of Computer Scienceand Engineering, Obafemi Awolowo University, Ile- Ife, Nigeria

ABSTRACT

In this paper, the requirements and methodological issues to build a prediction model for network performances in the face of security risks was presented**.** Attempt was made to investigate risk management approaches that are most relevant to network security and to establish a formal model with a level of detail sufficient to enable realistic predictions of operational network behavior, portray security measurements and properties of the network accurately and consequently incorporate relevant objects of significance to the network security risk management. The proposed model will predetermine the effect of network security risk factors on the network Confidentiality, Integrity and Availability. This will enable early detection of network security risk problems which in turn should quickly alert the network administrator of any problem area in the network environment and make effective decision for quality of services.

General Terms

Network Security, Bayesian Network, Risk Management,

Keywords

Predictive Model, Impact, Network Security Risk Management (NSRM)

1. INTRODUCTION

The number of users using networks is increasing every day. The protection of networks is therefore more than useful, it is vital. Thus, maintaining network security is on-going, ever changing, and an increasingly complex problem. The performance management of a network is closely related to the security management of a network. The continued growth in the number of network elements, end users, interfaces, protocols and vendor makes the network vulnerable to threats and attacks, which result to security risks. Network Security risks are events that could result in the compromise of network asset, resources, rules, policy and guidelines. These compromises adversely affect the network performances by altering or tampering with the three set network security objectives i.e. Confidentiality, Integrity, and Availability (CIA) of network. Network Security Risk is the potential impact that a threat can have on the confidentiality, integrity, and availability of network systems resources and services by exploiting a vulnerability of the networks, thus inefficiencies in the performance of the network are inevitable.

A major difficulty faced by network administrators is the need to make decisions for situations where there is considerable uncertainty in understanding how the network system works and how particular management actions will influence the system. Currently, network administrators or security managers operate by instinct and experience rather than relying on objectives metrics to guide and justify their decision making. This is a subjective approach, which is liable to human error and biases. There is a need for a flexible, adaptable and affordable system to measure the security status quantitatively and reduce reliance on human element**.**

This paper attempts to address this problem by employing the concept of Bayes theorem as the decision tool to make inferences on the likelihood of occurrence and impact of the security risk factors on the network performance. The rest of this paper is arranged as follows: Section 2 discusses the related works while Section 3 presents the proposed framework while Section 4 described the expected result and the conclusions are described in Section 5.

2. RELATED WORKS

There has been quite a good amount of work regarding the state- of- the- art of network security risks management. Risk management problems in networks have been looked into analytically by reviewing the theory and practices of formal security management. Several security framework that overcomes the problems of managing security risks were proposed in literatures [1], [2], [3], [4], [5] and [6].

A modelling language for information system security risk management was designed in [7] in order to integrate security and risk management concepts in information system development methods. The researchers in [7] and [8] provide a research method to design a modelling language for Information Systems Security Risk Management (ISSRM) and give consensus and integration to address information systems security problems.

In [9], approaches and methodology for security risk management were developed. The study considered risks and its impacts on organization and how to minimize their impact on the organization. The outcome of the study provides the approaches and methods involved in the process of security risk management. Algorithmic aspects of risk management were figured out in [10]. Risk computation was used in the research to drive changes in an operating system's security configuration. This study allows risk management to occur in real time and reduces the window of exposure to attack.

Towards dealing with network security threats and vulnerabilities both qualitatively and quantitatively, systems' threats and vulnerabilities were uncovered in [11] by proposing a framework for security risk assessment. The researchers in [11] developed a qualitative framework for security risk and vulnerabilities assessment by adding new components to the processes of existing framework. The study provides comprehensive structure for security risk analysis.

Application of Artificial Intelligence (AI) tools to risk management has also been utilized by some authors. A study that deals with uncertainty in software project management was presented in [12]. The authors in [12] make use of combination of Bayesian Network and Knowledge Engineering method of Artificial Intelligence to analyze risk. The outcome of the study in [12] affirmed that one approach of risk assessment is the application of Bayesian framework.

In [13], Bayesian Networks was used for cyber security analysis in order to capture the uncertain aspects in cyber security. The cyber security uncertainty was modelled using Bayesian networks. The presented work in [13] also showed that Bayesian Network is a modeling approach that correctly captures uncertainties.

More recently, the problem of Security risk assessment and mitigation was addressed in [14] by proposing a dynamic security risk management using Bayesian Attack Graphs (BAG). The BAG was used to model vulnerability exploitations in a test network. It was shown in [14] that the attack graphs-based risk management framework using Bayesian Networks enables a system administrator to quantify the chances of network compromise at various levels and also help in risk mitigation procedure by identifying the most critical and probable attack path in the network. Conversely, the attack graphs can get complex as the network attacks sequences increases i.e. lack of scalability. It is also a scenario-based approach.

In this research, attempt will be made to develop a performance predictive model for managing security risks in a Data Communication Network that will monitor and report the security status of a network. The model will also gauge the effectiveness of security controls and manage risk, provides a basis for trend analysis, and identify specific areas for improvement. In addition, the proposed model will identify likely vulnerabilities that may exist, and tracking and analyzing security flaws that are eventually discovered. The proposed model will utilize the probability characteristics of Artificial Intelligence method known as Bayesians Network to address the challenges being faced by network administrators in using objective metrics to measure their network security and justify the performance of their network, rather than relying on their instinct or experience.

3. MODEL DESCRIPTION

Figure 1 shows the conceptual model of the decision-support system that would assist a network manager deciding between several available interventions for a security risk occurring in a data communication network. This model predicts or predetermines security risk compromises in a data communication network. The proposed predictive performance management of a network when performed periodically or on regular basis by the network administrator will monitor and diagnose the network resources and assets in order to forecast security risk compromises so that a needed planned management can be performed prior to the network failure. The regular security risk prediction will allow the state of the resources which is a function of the usage to be taken into account in the course of the management.

The model will perform continuous resource status and performance monitoring to detect possible failures proactively, and it will collect performance data and analyzes it to identify potential problems to resolve them without affecting the network end-users. It will assist the network administrator or the security manager to predict ahead of time that which cannot be known or measured now. This will lead to proper network capacity planning, which will discard as much detail as possible while still retaining the essence of the network performance characteristics.

This security risk prediction requires a consistent framework in which to couch the expected functions. The features of the proposed model are as follow:

i. **Synergistic Approach**: It combines the synergy effects of both quantitative and qualitative risk analysis methods. The working together of both methods will produce an effect greater than the sum of their individual effects.

ii. **Updateable:** The model incorporates the use of technical repository for assets, threats and vulnerabilities. This makes the results of the risk analysis to be properly stored so that it can be updated, modified and retrieved easily.

iii. **Reusability**: It is possible to reuse the result of a previous risk analysis on a system, sub system or component and to include these results in a new analysis. This leads to less risk management time and increased dependability.

iv. **Modularity:** The methods used in this model are based on documented models i.e. Risk management model, Risk Prediction model, Risk Treatment model. The model comprises of entity-based or object-based data models. In effect, it is possible for a user to improve or to replace these models.

3.1 Model Specifications

Computer networks have experienced an explosive growth over the past few years and have become the targets for hackers and intruders. With this rapid growth of computer networks, network security has become a crucial issue. As depicted in Figure 1, the computer networks is opened to an increasing number of security risks from which organizations must protect themselves in order to ensure network performance which is the main mission of Quality of Service (QoS). It is worthy of note that no systems are absolutely secured. Network security risk comprises of:

i. Threats: These are anything that can have a negative impact on network systems. Threats may be intentional (e.g. malicious intent) or unintentional (e.g. misconfigured server, data entry error).

ii. Vulnerabilities: These are flaws or weaknesses in the network system security procedure, design, implementation, or control that could be intentionally or unintentionally exercised by a threat.

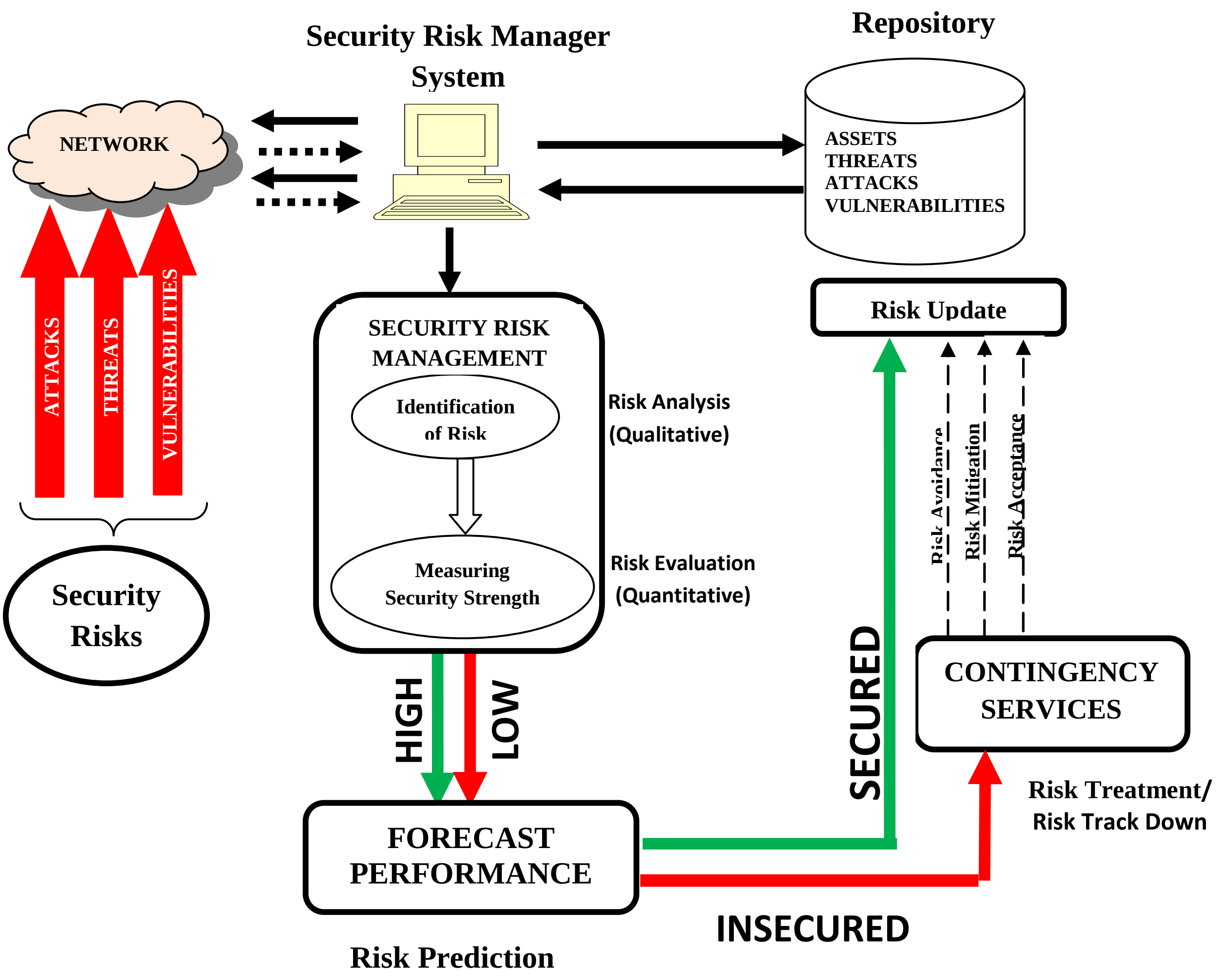

Figure 1: Conceptual Framework of a Performance Prediction Model for Network Security Risk Management:

iii. Attacks: These exploit network vulnerabilities in order to gain entry to the network and starts manipulating it.

The network security manager or administrator is the main actor-on-the-scene. In essence, the network security manager or administrator must have intimate knowledge of the network environment and a thorough knowledge of the working operations of the servers to ensure minimal downtime. They must be able at any time to provide any information regarding the state of the networks. When security risks occur in a network, most network administrators respond to the security events after they have occurred and have caused network performance inefficiencies, thereby reducing the Quality of Services of the network. This is a reactive measure, it can be regarded as the response to security risks that has already been exploited and turned into security incidents. It is therefore imperative that a proactive approach be considered. The model in Figure 1 thus depicted how the security risk in a network could be pre-empted before their manifestation, so that proper measures will be taken to prevent or mitigate the effect of the security risks.

The proposed model as shown in Figure 1 is made up of five major operational modes and several functions for each operational mode. The model incorporates the standard risk management processes as described by [15] and [16]. Thus the scheme to specify, visualize and construct the data flow within the proposed model blueprints shown in Figure 2 is described using algorithm in Figure 3.

3.2 Proposed Model Problem Formulation

The model problem definition is formulated as "Given a network domain, predict the probability of a security risk effect given information about the causal factor?" The three dependent elements of this model are as follows:

3.2.1 Network Domain Structure

The Network Domain Structure represents the knowledge structure, describing the activities involved in the domain. This is as shown in Figure 4. In this study, the desiderata for the network domain are:

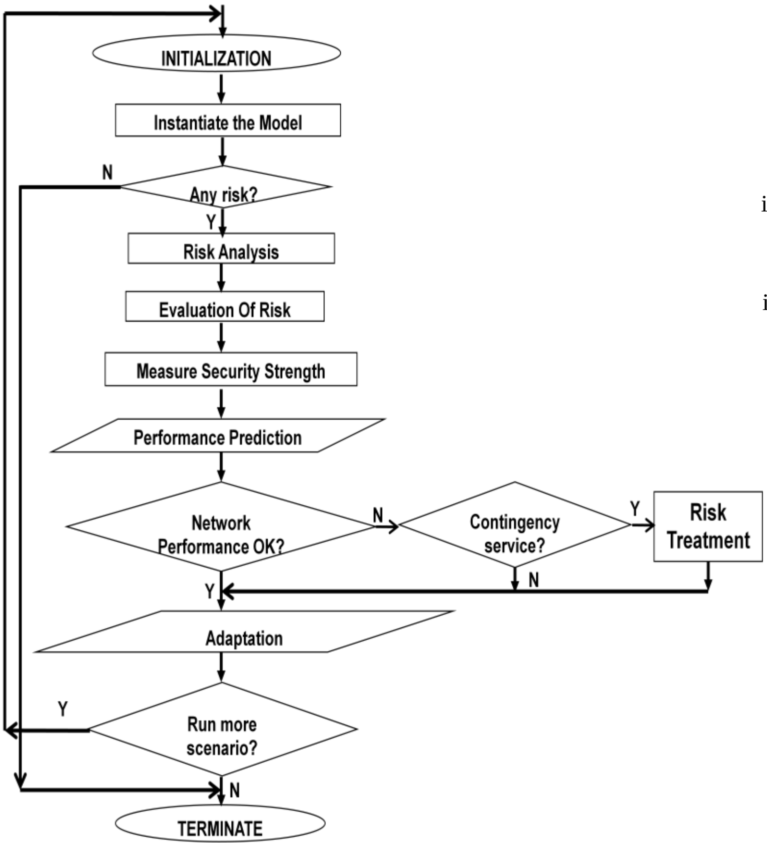

Figure 2: Data Flow Of The Proposed Model

i. It must have a centralized network administration, in which the permissions that grant access to resources in the network are maintained in one or more servers.

ii. The network must use a hierarchical structure that enables assigning different permissions to users who collaborate with different departments in an organization.

iii. The network must employ client-server model i.e. utilizes client and server devices each designed for specific purposes.

iv. It must be service-oriented, and employs a request-response protocol.

3.2.2 Network Domain Uncertainties

Uncertainty in a network domain can be described as the lack of certainty, a state of having limited knowledge in which it is impossible to describe precisely existing state or future outcome. Decision making is widely recognized by network administrators as an integral part of the whole network management process in guaranteeing quality of service to end users.

There are essentially three kinds of sources of uncertainty in the network domain. They are:

(a) Deficiencies in the configuration,

(b) Deficiencies in the network services; and,

(c) Real-world features.

Some of the security risk-related problems caused by these uncertainties in the network domain are:

i. **Incomplete information**: When collecting information about one determined phenomenon which involves several variables in a network, it is quite usual that in some cases such information cannot be found due to various reasons.

*i. Identify a **problem domain**(single domain environment)*
ii. Input the network structure using Bayesian Approach

Initialization

*iii. **Quantify the network** by identifying the security risks (Threats, Vulnerabilities)*

Risk Analysis

iv. Find the probability distribution of the risks using sensitivity analysis
*v. Find the **probability inferences** of the risks using propagation algorithm*

Risk Evaluation

*vi. Use the inferences to measure the **network security strength***

Measuring security strength

*vii. If the strength is high **go to(ix) else go to (vii)***

Forecasting network

*viii. Apply **contingencies** techniques*

Risk Treatment

Figure 3: Algorithmic Description Of The Proposed Model

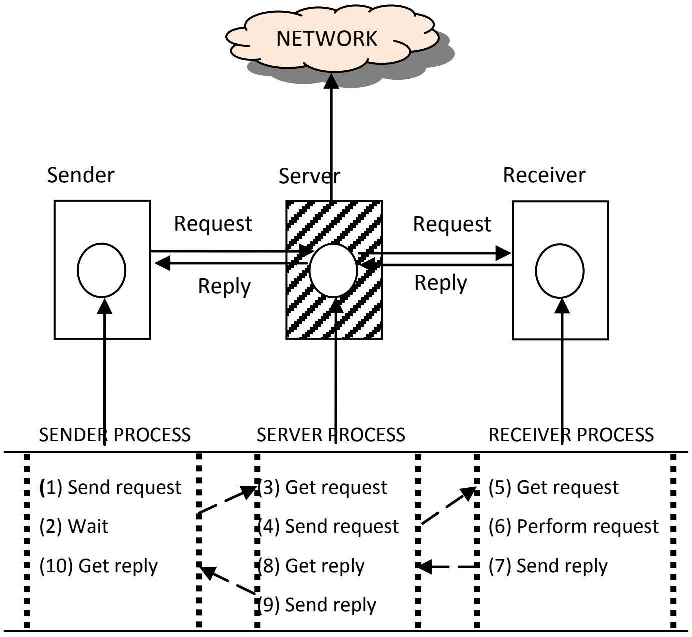

Figure 4: Network Domain Structure

ii. **Erroneous information:** Within the several phases in which the process of collection of information is divided, it likely results to aberrant values.

iii. **Inaccurate information**: Some interest data that are easily expressed by means of natural language are vague or fuzzy in nature and result too difficult to be expressed in a numerical way.

iv. **Non-deterministic real world:** Many times, the obtained effects from the same causes of a security risk are different as a consequence of this feature present in the real world.

v. **Incomplete model:** In many occasions the model used for approximating the reality of a certain security risk problem is incomplete, in the sense that the causes of many security risk problems are unknown.

vi. **Inexact model**: It could also happen that the model structure is the appropriate one, although the determination of the parameters that rule this model behaviour could have been carried out only in an approximate way**.**

3.2.3 Network domain Causality- Effect Model

Causal-Effect model are cognitive structure that represent the causal knowledge of subject-matter experts in the network domain. This causality-effect modelling is used to represent experts' knowledge of network domain. They describe the relationships between network security risks, causes (causal factors) and effects. It organizes and graphically represents the causes of a particular security risk. The main purpose of the Cause and Effect Diagram is security risk identification.

The conceptual causality model development involves identifying the important system variables and establishing the links between variables. The causal conceptual structure shown in Figure 5 was inferred from Knowledge Engineering method, which is an information elicitation approach used in structuring the situation for reasoning under uncertainty. It involves the following process:

i. Qualitative information elicitation- interview with subject-matter experts;

ii. Gathering(validating expert knowledge); and

iii. Consolidation.

This knowledge-based approach is especially useful in a situation where domain knowledge is crucial and availability of data is scarce. Hence, the knowledge-based approach uses causal knowledge of domain experts in constructing the causality model. Data elicitation is first drawn from a domain expert, and is followed by a detailed analysis of the context through a systematic content analyzing technique to map the causal relations within the expert's domain, leading to the creation of the causal map shown in Figure 5.

Expertise knowledge is gathered and documented concerning the topic in question with an interview with a subject-matter expert yielding important insights into general knowledge held by a variety of individuals. The technical specialists were selected based on their expertise and understanding of security management of a network. The key issue of this interview is to gather information of hazards, causes and consequences.

Interviews were conducted in a conversational style to allow a complete and uninterrupted flow of thought from the interviewee. To ensure a full understanding of the interviewee's knowledge was captured, probing questions were asked, for example "How" and "Why". This style of questioning encouraged responses detailing the interviewee's understanding of risk causes and effects. Care was taken during the interviews to not ask leading questions and thus bias the interviewee's response.

Some of the issues that were addressed during the course of the interview are:

i. What can go wrong?

ii. What are the causes?

iii. What are the effects and consequences?

iv. What are the controls used?

v. Why the controls do fail? Etc

The responses to these interviews are gathered and transcribed in textual fashion to get narrative information. Structured methods are used for confirming or validating the expert knowledge by gathering the factors relevant to the decision.

3.3 Formulation of the Prediction Model as a Bayesian Network Problem

An adaptive network performance prediction was formulated as a Bayesian Network (BN)-based problem. A Bayesian network is employed as a tool to represent uncertain, ambiguous or incomplete knowledge of the client-server model described in Figure 4. Bayesian networks make use

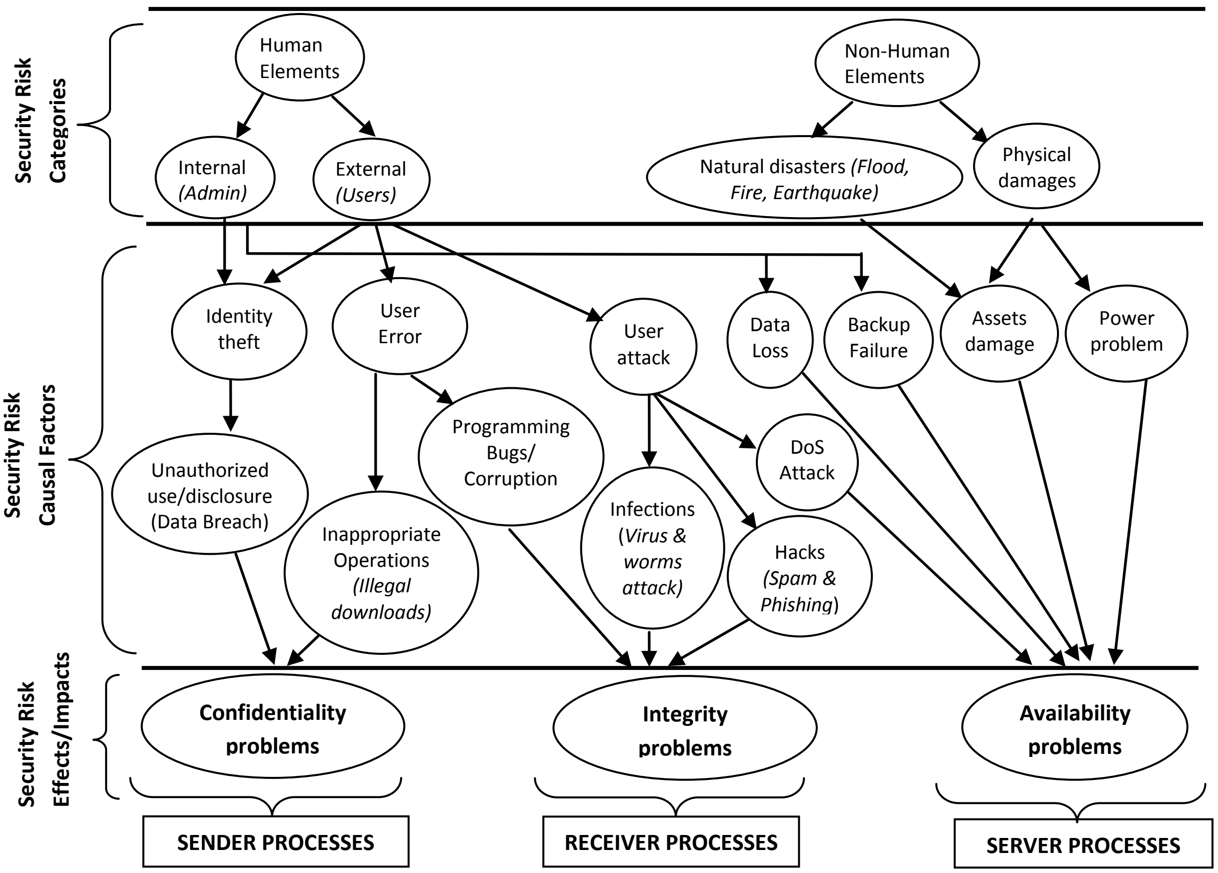

Figure 5: Causality-Effect Model of Network Security Risks

of probability theory to represent the uncertain knowledge. Bayesian networks are probabilistic networks derived from Bayes theorem based on the Bayesian theories, which allows the inference of a future event based on prior evidence.

Applying Bayes' theorem:

$$P(F \mid E) = \frac{P(E \mid F)\, P(F)}{P(E)} \quad (1)$$

Where:

F - represents Risk Causal Factor

E - represents Risk Effect

P(F) - represents Prior Probability of Risk Causal Factor (F) i.e. the Unconditional Probability

P(E |F) - represents the Conditional Probability of Risk Effect (E) given the Risk Causal Factor(F)

P(E) - represents Marginal (unconditional probability) of the Risk Effect (E) also called the normalizing constant or prior predictive distribution i.e. the probability that risk effect occurs when there is no specific information about the event or factor that influence it.

P(F |E) - represents Posterior probability of the Risk Causal Factor (F) given the evidences of Risk Effect (E).

Thus, this prediction model will use Bayes' law to find the probability of the effect of a security risk on network performances in terms of its Confidentiality, Integrity and Availability given that one of the possible causes the risk has occurred. Thus, Equation (1) can be written as:

$$P(F_i|E) = \frac{P(E|F_i)P(F_i)}{\sum_{j=1}^{n} P(E|F_j)P(F_j)} \quad (2)$$

$$i = 1,2,\cdots,n \qquad j = 1,2,\cdots,n$$

4. EXPECTED RESULT

This paper only reveals the theoretical background of the performance prediction model for data communication network security risk. This study presents procedures that support dynamic decision-support model that will predetermine the impact of network security risk on the selected network domain given the causal- effect model. The research will provide a system that will monitor and report the security status or posture of a network to enhance network performance and facilitate efficient quality of services.

5. SUMMARY AND CONCLUSION

This study is still an on-going research work. The study will provide information on the severity and overall nature of the security risk in a network. The proposed model will assist network managers in predicting the effect of security risk in networks as well as recommend actions for optimal network performance.

6. AUTHOR'S PROFILE

Akinyemi Bodunde Odunola obtained her B.Tech in Computer Science at Ladoke Akintola University of Technology, Ogbomoso, Nigeria in 2005. She also obtained her M.Sc. and Ph.D in Computer Science at Obafemi Awolowo University, Ile-Ife, Nigeria in 2011 and 2014 respectively. She is currently a Staff of Obafemi Awolowo University, Ile –Ife. Her research interests are: Data communication and networking, Operations Research, Simulation and Modeling. She has actively participated in organizing a number of learned conferences. She is an active member of local organizing committee of the Application of Information Communication Technologies to Teaching, Research and Administration (AICTTRA) international conference and the Faculty of Technology international conference, Obafemi Awolowo University, Ile Ife.

Amoo Adekemi Olawumi obtained her B.Sc and M.Sc in Computer Science at Obafemi Awolowo University, Ile-Ife, Nigeria in 2008 and 2014 respectively. She is currently a post-graduate Student and Staff of Obafemi Awolowo University, Ile –Ife. Her research interests are: Data communication and networking, Data Mining and warehousing. She has actively participated in organizing a number of learned conferences. She is an active member of local organizing committee of the Application of Information Communication Technologies to Teaching, Research and Administration (AICTTRA) international conference and the Faculty of Technology international conference, Obafemi Awolowo University, Ile Ife.

Olajubu Emmanuel Ajayi is a Senior Lecturer of Computer Science from Obafemi Awolowo University, Ile-Ife, Nigeria. He is a member of the Nigeria Society of Engineers (NSE) and also a registered Computer Engineer with Council for Regulation of Engineering Practice in Nigeria (COREN). He is also a member of Nigerian Computer Society (NCS). He has over 10 years of experience in teaching and research. He is an author of many journal articles in Nigeria and abroad. His special interest includes computer communication and network.

7. REFERENCES

[1] Wang, C. and Wulf, W. A. 1997. Towards a Framework for Security Measurement. In Proceedings of the Twentieth National Information Systems Security Conference, Baltimore, MD, October 1997, 522-533.

[2] Eloff, J. H. P., Labuschagne, L. and Badenhorst, K. P. (1993). A Comparative Framework for Risk Analysis Methods. Computers & Security, 12:597-603.

[3] Hyland, P.C. and Sandhu, R. 1998. Management of Network Security Applications. In Proceedings of the 21st NIST-NCSC National Information Systems Security Conference, Arlington, Virginia.

[4] Alberts, C. J. and Dorofee, A. J. 2002. Managing Information Security Risks: The OCTAVE Approach, Addison -Wesley Professional, ISBN: 0321118863.

[5] Lund, M. S., Solhaug, B. and Stølen K. 2011. Risk Analysis of Changing and Evolving Systems Using CORAS. Foundations of Security Analysis and Design VI (FOSAD'11), in Lecture Notes in Computer Science, Springer, 6858:231-274.

[6] Dimitrakos, T., Ritchie, B., Raptis, D. and Stølen, K. 2002. Model -based Security Risk Analysis for Web Applications: The CORAS approach. In Euroweb 2002 - The Web and the GRID: from e-science to e-business.

[7] Mayer, N., Heymans, P. and Matulevičius, R. 2007. Design of a Modelling Language for Information System Security Risk Management. In Proceedings of the 1st International Conference on Research Challenges in Information Science (RCIS 2007)Ouarzazate, Morocco, pp 121–131.

[8] Dubois, É., Heymans, P., Mayer, N. and Matulevičius, R. 2010. A Systematic Approach to Define the Domain of Information System Security Risk Management. Intentional Perspectives on Information Systems Engineering, Springer. pp 289-306.

[9] Stroie, E. R. and Rusu, A. C. 2011. Security Risk Management - Approaches and Methodology. Informatica Economică, 15(1):228-240.

[10] Gehani, A., Zaniewski, L. and Subramani, K. 2011. Algorithmic Aspects of Risk Management. Agha G., Danvy O., and Meseguer J. (Eds.): Talcott Festschrift, LNCS, 7000: 262–276.

[11] Saleh, Z. I., Refai, H. and Mashhour, A. 2011. Proposed Framework for Security Risk Assessment. Journal of Information Security, 2:85-90.

[12] Paokanta, P. and Harnpornchai, N. 2009. Construction of Bayesian Networks for Risk Assessment of Software Project by Knowledge Engineering. 3rd International Conference on Software, Knowledge, Information Management and Applications, ISBN: 9781851432516. 154-158.

[13] Xie, P., Li, J. H., Ou, X., Liu, P. and Levy, R. 2010. Using Bayesian Networks for Cyber Security Analysis. In Proceedings of the 40th IEEE/IFIP International Conference on Dependable Systems and Networks. China. 211-220.

[14] Poolsappasit, N., Dewri, R. and Ray, I. 2012. Dynamic Security Risk Management Using Bayesian Attack Graphs. IEEE Transactions on Dependable and Secure Computing, 9(1):61-74.

[15] Calder, A. and Watkins, S. G. 2007. Information Security Risk Management for ISO27001/ISO17799, IT Governance Publishing.

[16] Stoneburner, G., Goguen, A. and Feringa, A. 2002. Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930, NIST Special Publication 800-30.