# A Systematic Survey on Multidimensional Spinning Cube of Potential Doom Resource Utilization in Network Visualization

**Nirmal Kumar A*, Sai Keerthi C, and Poorna Shree V**

Dept. of Information Technology, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Anna University, Chennai, India.

***Corresponding author: E-Mail: sa.nirmalkumar@gmail.com**

**ABSTRACT**

Network Security is the policies and practices adopted to present and monitor unauthorized access, misuse, modification or denial of a Computer Network and Network access resources. It involves the authentication of access to data in a network, which is controlled by the network administrator. In the existing system is focused on the major technical perceptions for a network visualization connectivity with the host and the server utilization of the system, packet traces, server logs, server vs host interaction, level of activity through port, intrusion alerts and dns traces. In the proposed system they couldn't identify the implication of the major disaster or network flow in a system. In our system we are trying to project the detailed view of how the problem occurred and possible solution for the servers. Advantage of this system is security events from the server and the interaction with the client were visualized. Traces of the data navigation happening in the network seeing data's in visualization manner.

**KEY WORDS:** Data Security, Network Visualization, Network Security.

## 1. INTRODUCTION

Although the visualization of network security events is the subject of this survey, this paper does not focus on designing and developing a specific visualization system. Instead, we consider network security with respect to information visualization and introduce a collection of use case classes. In this study, we provide an overview of the increasing relevance of security visualization. We explore a novel classification approach and review the artifacts most commonly associated with security visualization systems. We provide a historical context for this emerging practice and outline its surrounding concerns while providing design guidelines for future developments. Visual data analysis help to perceive patterns, trends, structures, and exceptions in even the most complex data sources. As the quantity of network audit traces produced each day grows exponentially, communicating with visuals allows for comprehension of these large quantities of data. Visualization allows the audience to identify concepts and relationships that they had not previously realized. Thereby, explicitly revealing properties and relationships inherent and implicit in the underlying data. Identifying patterns and anomalies enlightens the user, provides new knowledge and insight, and provokes further explorations. It is these fascinating capabilities that influence the use of information visualization for network security.

**Methodologies:** In the existing system, we are focusing on the major technical perceptions for our network visualization areas. Connectivity with the host and server will be monitoring for any downfall time. Utilization of the system – details about the host vs server utilization. Number of accessible users - Calculating the individual and concurrent users on the system. Packet Traces – tracing the packets traversing between the systems. Server logs – monitoring the security, application logs in the server. Servers host interactions – monitor the port and protocol used in communication. Level of activity through the port. Intrusion alerts – alerts create by the developers on anonymous activities. Dns traces – recording anonymous entries in the domain. The disadvantage of this system is we couldn't identify or specify the implication of the major disaster or network flaw in a system.

**Proposed System:** In the existing system, they've proposed various techniques in visualizing the network data. But unfortunately, they couldn't identify or specify the implication of the major disaster or network flaw in a system. In our proposed approach, we provide the detailed visualize of the network information as Number of Total Packet Reads, Latest packets read in a specific interval, Number of Total Writes on The Packets, Latest packets write in a specific interval, Complete Input/output busy time, Complete CPU busy schedule, Complete Input/output Reads, Latest number of seconds Input / Output reads, Number of process info reported errors.

**Architecture:** In our system, we are trying to project the detailed view of how the problem occurred and possible solution for the servers. Intrusion related information's were considered and precautionary measures towards intrusions will be addressed in our future work.

**Sequential data processing:** Number of spid's reported error in the server, Authentication information's, Disabled services in the server.

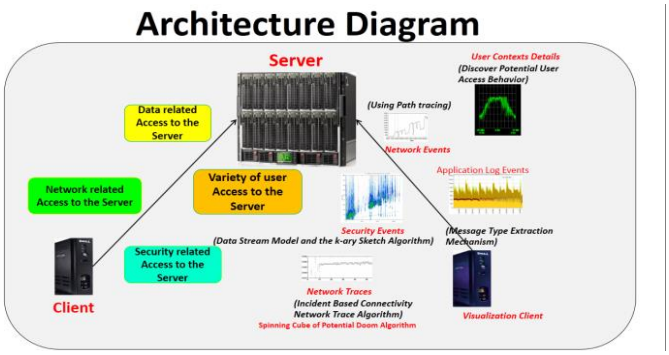


**Figure.1. Visualization Client**

**Initial Virtual Machine Information Module:** The Initial Virtual Machine Information Module defines the network and traces the initial; machine information using the algorithm Data Stream Model and the k-ary Sketch Algorithm which is generable from a network, and produces a network N such that is generable from N and not from any other network.

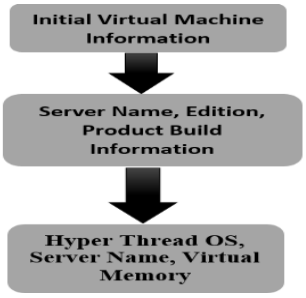


**Fig.2. Initial Virtual Machine Information Module**

**Virtual Machine Disk Space Details Module:** The Disk Space Details modules define the "Virtual Disk Space Details information" such as Drive info details (C:/DRIVE, E: DRIVE), Also the memory/Free space allocation in Megabyte (MB) will be observed.

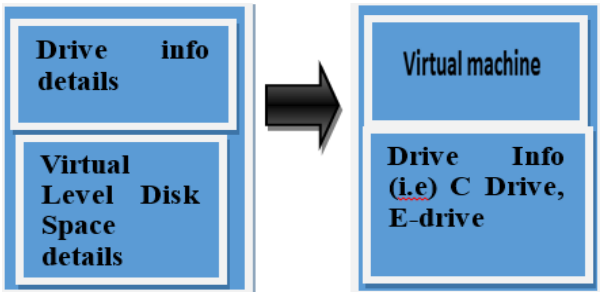


**Fig.3. Virtual Machine Disk Space Details Module**

**Server Level Information Module:** The Server level information module tends to define the Number of packets Received/Send Status will be notified. Along with that the Graphical Representation of the server level status information will be notified and shown in the graphical illustration. The network packets info will also be defined in this module by indicating the packer revived status, Packets sent status & the Error packets status.

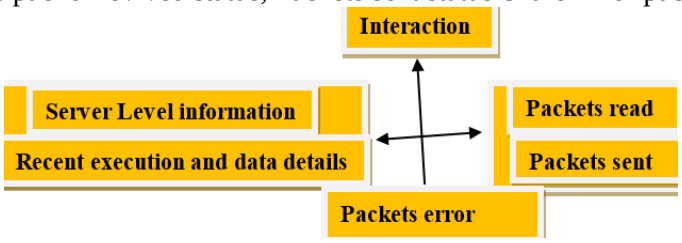


**Fig.4. Server Level Information Module**

**Network Path Tracing Module:** Path tracing is a graphical method of rendering traces of the data navigation happening in the network such that the global illumination is faithful to reality. This algorithm is integrating over all accumulation of data arriving to a single point on the surface of an object. This accumulation is then reduced by a into sub paths based on the different access points in different intervals. Following items were visualized under this module: Number of Total Packet Reads (In terms of bytes) since the last server was started. Latest packets reads in a specific interval (Data read in bytes). Number of Total Writes on the Packets, since the last server starts. Latest packets writes in a specific interval. Connection established since the Laster Server Starts in a specific interval.

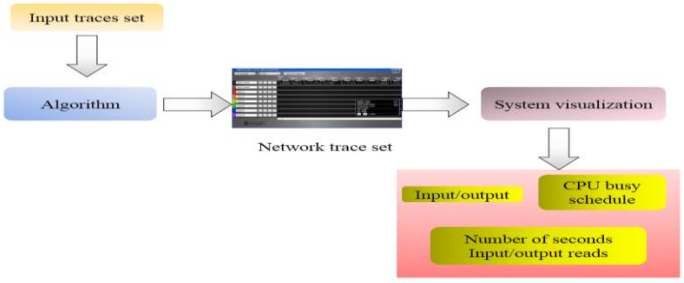


**Fig.5. Network Path Tracing Module**

**Read/Write Status Module:** Security events from the server and the interaction with the client were visualized in the module: Analytical values of a login have been added or removed as a database user to a database. Login was added or removed from a fixed server role. Login has been added to or removed from a role. Database role was added to or removed from a database, password has been changed for an application role. Backup or restore statement has been issued. Reports audit messages related to Service Broker dialog security, Service Broker transport security. Indicates that an audit trace modification has been made. Indicates that the permissions to change the owner of a database have been checked.

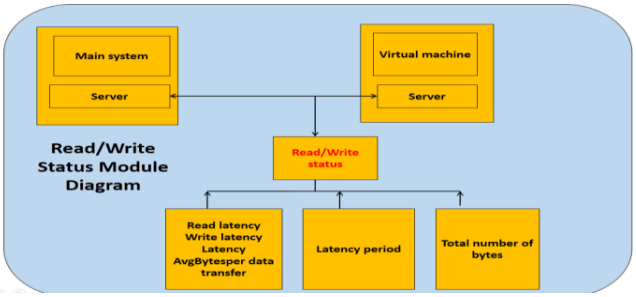


**Fig.6. Read/Write Status Module**

**Application Log Events Visualization Module:** Security events from the server and the interaction with the client were visualized in the module; Successful trusted logins, Successful non-trusted logins, Failed user logins and Insufficient resources events.

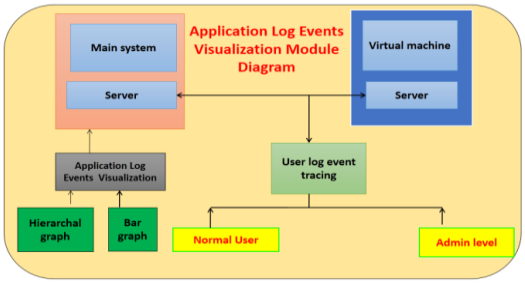


**Fig.7. Application Log Events Visualization Module**

**User contexts visualization module:** Identity management indicates the management of individual identifiers, their authentication, authorization and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity. Identity management systems, products, applications, and platforms are commercial Identity management solutions implemented for enterprises and organizations. Technologies, services, and terms related to Identity management include Active Directory, Service Providers, Identity Providers, Web Services, Access control, Digital Identities, Password Managers, Single Sign-on, Security Tokens, Security Token Services.

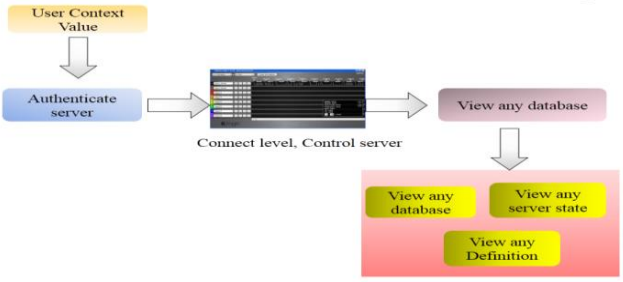


**Fig.8. User Contexts Visualization Module**

## 2. MATERIALS AND METHODS

**CNM Graf Algorithm:** CNM Graf Algortihm uses knowledge fromvariety of user Access to the Server to produce frequent Network Events in a network. CNM Graf uses a "bottom up" approach, where frequent subsets are extended to one item at a time in the network groups of candidates are tested against the data in the network.

**VLNT Algorithm:** VLNT Algorithm traces the movement of the data packets in the network. Post-operative evaluation was performed at standardized time points and included qualitative assessment and quantitative volumetric analysis in the network.


**Figure.9. VLNT Algorithm**

**Data Stream Model and the k-ary Sketch Algorithm:** Data Stream Model and the k-ary Sketch algorithm defines the complexity of network architecture faced by a user in solving a network monitoring problem. Most of the visualization techniques exist in generating the captured network data, Application log event into informative graphical 2D or 3D view and to improve decision making and organization management performance.

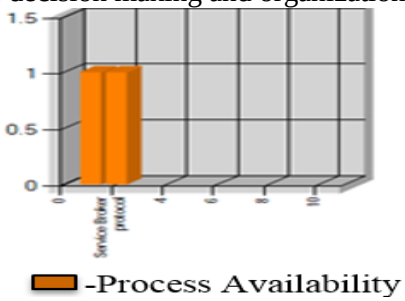


**Figure.10. Data Stream model**

**Spinning Cube of Potential Doom Algorithm:** Spinning Cube of Potential Doom Algorithm is used to perform aggregate queries in network traffic. Security events & User contact details in the network traffic must have the recording data structures with linearity, i.e., two traffic records can be linearly combined into a single record structure as if it were constructed with two data streams directly. Thereby it helps to monitor the network visualization effectively to determine the set of flows whose size changes significantly from one period to another.

## 3. RESULTS AND DISCUSSION

As the number of security related events generated in modern networks is on the rise, the need for network security visualization systems is felt more than ever. In this paper, we have examined recent works in network security visualization from a use-case perspective.

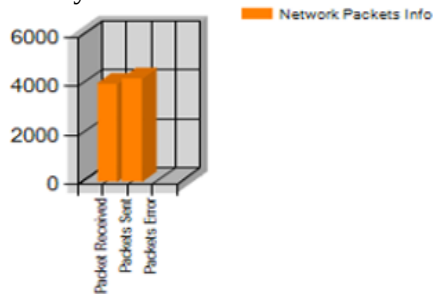


**Figure.11. k-ary Sketch algorithm**

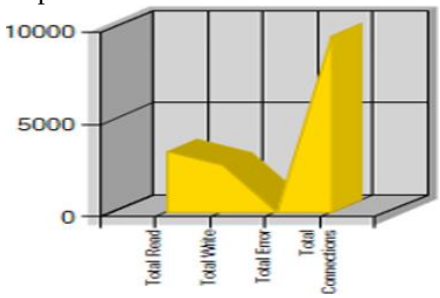


**Figure.12. Spinning cube**

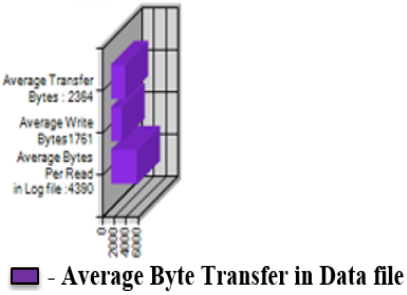


**Figure.13. Potential Doom algorithm**

## 4. CONCLUSION

As the number of security related events generated in modern networks is on the rise, the need for network security visualization systems is felt more than ever. In this paper, we have examined recent works in network security visualization from a use-case perspective. Five use-case classes, each representing a different application area, were defined and several recent works in each category were thoroughly described. We detailed the underlying data sources of network security visualization and gave a few examples of each category. Analysis of these systems motivated us to examine several issues and concerns surrounding this emerging field. We elaborated on the

advantages and shortcomings of all use-case classes and shed light on paths that researchers should focus toward. We aggregated the findings of our work into an informative table for future references. While the field of visualization is as wide as imagination allows, we hope that the analysis and taxonomy presented here will motivate better future work in this area.

**Conflict of interest:** The author declares having no competing interests.

## 5. ACKNOWLEDGEMENT

The author wish to thank Vel Shree Dr. R. Rangarajan, Chancellor, Vel Tech High Tech Dr. RR and Dr. SR Engineering College, for the support and facilities provided for the preparation of this paper.

**Financial disclosure:** No financial support was received for this implementation.

## REFERENCES

Conti G, Security Data Visualization, No Starch Press, 2007.

Erbacher R, Intrusion Behavior Detection through Visualization, Proc. IEEE Int'l Conf. Systems, Man and Cybernetics, 2003, 2507- 2513.

Erbacher R, Walker K, and Frincke D, Intrusion and Misuse Detection in Large-Scale Systems, IEEE Computer Graphics and Applications, 22 (1), 2002, 38-48.

Lakkaraju K, Yurcik W, and Lee A, N Vision IP: Net flow Visualizations of System State for Security Situational Awareness, Proc. ACM Workshop Visualization and Data Mining for Computer Security, 29, 2004, 65-72.

Marty R, Applied Securit Visualization, Addison-Wesle Professional, 2008.

Takada T and Koike H, Tudumi Information Visualization System for Monitoring and Auditing Computer Logs, Proc. Sixth Int'l Conf. Information Visualization, 2002, 570-576.

Ware C, Information Visualization: Perception for Design, Morgan Kaufmann Publishers, 2004.