INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Disaster recovery and risk management over private networks using data provenance: Cyber security perspective

Kukatlapalli Pradeep Kumar[1]*, **Vinay Jha Pillai**[2], **K Sarath Chandra**[3], **Cherukuri Ravindranath Chowdary**[4]

1 Assistant Professor, Computer Science and Engineering, School of Engineering and Technology, Christ University, Bangalore, 560074, India. Tel.: +91 9686272678
2 Electronics and Communication Engineering, School of Engineering and Technology, Christ University, Bangalore, 560074, India
3 Civil Engineering, School of Engineering and Technology, Christ University, Bangalore, 560074, India
4 Associate Professor, Computer Science and Engineering, School of Engineering and Technology, Christ University, Bangalore, 560074, India

OPEN ACCESS

Received: 09.12.2020

Accepted: 14.03.2021

Published: 19.03.2021

Citation: Pradeep Kumar K, Pillai VJ, Sarath Chandra K, Chowdary CR (2021) Disaster recovery and risk management over private networks using data provenance: Cyber security perspective. Indian Journal of Science and Technology 14(8): 725-737. https://doi.org/10.17485/IJST/v14i8.1833

* **Corresponding author**.

Tel: +91 9686272678
kukatlapalli.kumar@christuniversity.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To understand of data provenance applications towards cyber security for disaster recovery. To design an attack scenario with appropriate use cases using unified modeling language. To construct and analyze the data collected in the selected private computer network using appropriate graphical representation and comparing variables with null hypothesis. **Methods**: In the existing methods, presence of provenance data is not available with respect to network attack scenarios of risk management. Information security deals about disaster recovery in the form of business continuity planning, however nowhere it specifies about genesis data and its lineage. We propose a methodology for trouble shooting issues concerning over cyber physical systems in private networks. **Findings**: The process of resolving problems is linked with risk management for fairer and guaranteed continued communication as usual. Identity of the systems and users are considered random variables to understand the association between them. These random variables are picked from the provenance data maintained at the administrator login of a specific private network. This association analysis is unique and provides appropriate outcomes for good decision-making at the time of attack scenarios in risk management. **Novelty**: Simulations and their results are represented to show the correlation between risk management and data provenance in the cyber world. The uniqueness and novelty lies in design part of the problem statement with regards to provenance and disaster recovery for computer networks.

Keywords: Cyber security; data provenance; risk management; business continuity planning; information security

1 Introduction

Research with appropriate analysis has happened on the mentioned theme of disaster recovery in the private computer networks. However, inclusion on provenance data in such scenario for risk management in cyber security is first of its kind. There is a need to address the gap which is widely observed in risk management and business continuity planning of the organisations. Vulnerabilities always exists and are exploited by attackers, continuous improvement is required to address the issues and resolve them before a zero day exploit. Newness of this study lies in combination of provenance and security concepts. Data provenance and its outcome is associated to risk management perspective for resolving and troubleshooting the issues raised in private networks. Provenance data is collected in a ledger file related to a data packet attack scenario.

In this regard, data provenance plays a key role in identifying, specifying and resolving an attack on an information asset in an organisation. Provenance can be visualised as a framework which involves log files used for capturing and tracing activities. Log file is an evolving ledger which consists of all transaction oriented data performed by various actors in an application domain.

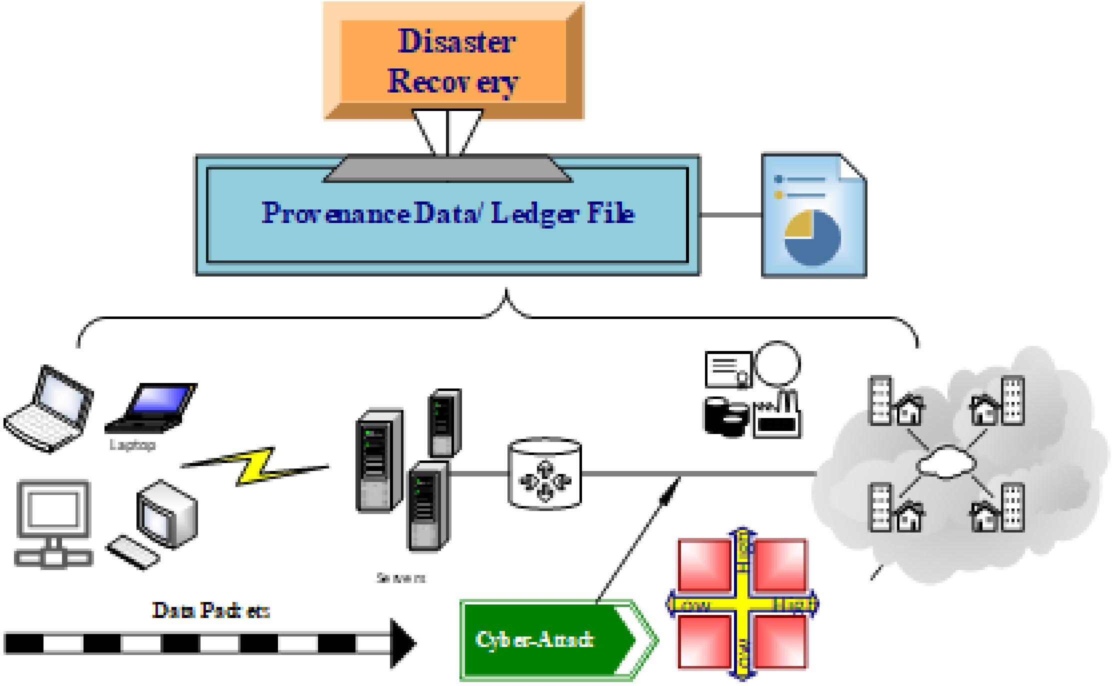

Fig 1. Disaster recovery using provenance data with packet attack scenario

Figure 1 depicts process of risk management with disaster recovery perspective. Here a LAN is connected to local servers which are in turn connected to the outside the untrusted network; internet. Eventually LAN is connected to internet via a router. A cyber-attack is simulated at the router context where incoming and outgoing data can be observed to and from the LAN. We consider a context of a troubleshooting attack scenario which can be seen as a potential threat for the organisation. After the attack, provenance data is used for understanding and analysing the problem through which a roll back scenario is implemented as a recovery process.

This section is followed by a study on risk management, data provenance and cyber security aspects. Software design in unified modelling language is depicted with simulated results at the end of the paper.

1.1 Cyber Security

Extensive use of internet and cyber devices calls for great requirement and dependency of security and privacy. People are becoming more active in the cyber world wherein they are sharing their personal and professional information especially via social network, hence high chance of privacy being jeopardized. Any information in a computer or network is altered or disabled and destroyed for the benefit of a person or a firm is considered as a cyber-attack. These attacks result in the loss of money for most of the cases and also in few cases the reputation of a firm and loss of life was also observed. Cyber-attacks are gaining popularity in the recent times where the various nation's defense systems are in trouble and spending enormous amount of money and labor to protect their nations from the various types of cyber-attacks.

Active attacks and passive attacks can be observed as the two broad categories of attacks in the cyber world. Active attack is an attack where the content is altered or disabled in a system with an intention of creating a threat to the concerned person or firm on the other end passive attack is an attack where information or the content in the system is used to attack others, but they are not altered at any situation. Example of active cyber-attacks are denial of service, spoofing, mixed threat attack, ping flood, smurf attack, buffer overflows, stack overflow, heap overflow and etc. whereas the examples of passive cyber-attacks are wiretapping, fiber tapping, data scaping, etc. At least one million new viruses and malware are released every day and over 100,000 cyber-attacks every hour costing more than $100 billion annually globally (Bowerman, S. Kristopher.[1]. According to Indian cyber security research and software firm Quick Heal, India was hit with 1,852 cyber-attacks for each minute last year[2]. Trojans, most frequently created through unlawful software copies, are India's biggest inflictor of damage over the past year, continuing to slowly improve India's issues with legitimate software. Standalone worms and infectors were the second and third biggest triggers of cyber. More than 60% of the popular infrastructure companies were affected by the malware designed to interrupt their computers as per the McAfee statistics in 2011[3]. In the current scenario a well-known service attack namely DDoS attack is prevailing, whereas in 2013 world has faced the biggest Distributed denial of service attack where the issue of attack touched to 300 Gbps[4] and the research proved that the peak may increase in near future with the more advancement of technology and more desires of the mankind. Zombies are the initiators and the secondary victims of the DDoS attacks and cyber-attack by cyber bunkers, attack on China and Iranian FBI websites and Bit coin issues and so on in 2013 are the major attacks caused by DDoS[5]. SQL injection attacks is another most effective cyber-attack where the important information can be taken form the backend. SQL inject attacks are mostly targeted for hacking the web applications and enrolled in top ten list of web application related cyber-attacks in 2012[6]. In the case of banking and financial institutions password attacks are very common and creates a huge economical imbalance. The first password attack was registered before five decades ago but even today there are lot of cases registered with weak passwords as password attack[7]. These attacks results to the loss of money in most of the cases and also in few cases the reputation of a firm and loss of life was also observed. A large amount of work has concentrated on improving the safety culture of an organization[8–10] and end-user enforcement and/or non-compliance with Organizational Health Policy[11–13].

Referring all the above cases, there is a common understanding on the restrictions and conditions applied by the organizations towards systems security. People and information assets of an organization plays a major role over information security. Software, hardware, networks etc. are the assets in this regard which are to be preserved from internal and external attacks. Security breach can happen unknowingly through email attachments from an innocent employee login. On the other side, novice internet users such as homemakers, non-technical personnel, students etc. also fall prey for cyber-attacks as there are no stringent policies playing at their end. They face challenges to cyber security close to those of users bound by security policies. Accessing digital information and their related services via smart devices introduces yet additional trajectory of danger to these end users.

1.2 Risk management

As mentioned before, risk administration is the method of finding, measuring and controlling the risks in an organisation. Each of these aspects have their own phases of understanding the problem. An illustration depicting information about risk management is shown in Figure 2.

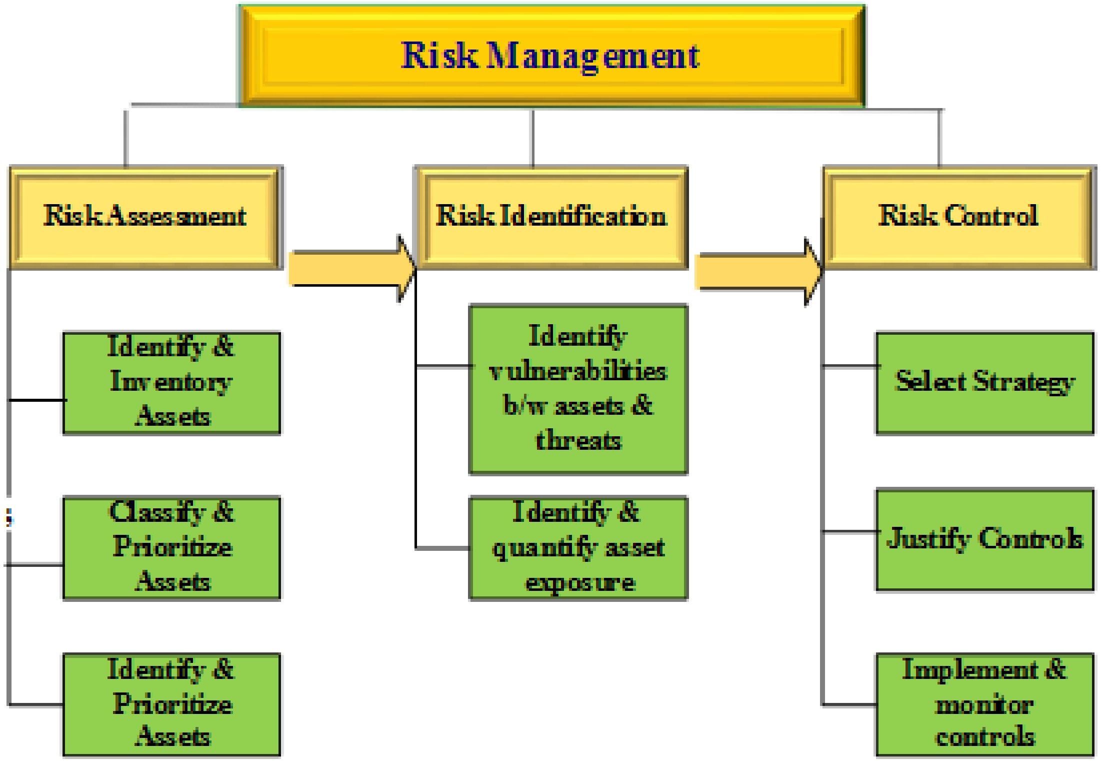
Risk Management
Risk Assessment
Risk Identification
Risk Control
Identify & Inventory Assets
Classify & Prioritize Assets
Identify & Prioritize Assets
Identify vulnerabilities b/w assets & threats
Identify & quantify asset exposure
Select Strategy
Justify Controls
Implement & monitor controls

Fig 2. Depiction of risk management structural elements

Assessment involves steps such as risk identification on information assets, classifying the collection and prioritizing the assets which has the highest risk factor. Risk identification is in continuation with risk assessment phase. It involves identification of vulnerabilities between assets and threats. Further to that, this phase identifies asset exposure through numerical analysis. Finally, risk control provides the strategies to control the identified risks on the information assets namely defend, transfer, mitigate, accept and terminate[14].

1.3 Data provenance and disaster recovery over IT infrastructure

Data provenance helps in understanding and analysing lineage of concerned objects in a system[15]. Provenance framework in this regard, helps to know specific point issue resolutions. Provenance and security are symbiotic. Provenance data needs security and robust access control mechanisms needs to be in place. Genesis data is also seen as provenance data in some contextual environments[16]. In the current situation, provenance data is observed in a ledger file which is an evolving file consisting of all transactions, events, timestamps including their meta-data.

Data replication is one of the strategies for disaster recovery in organisations. Two contexts are considered where in, the data replication is performed via a pipeline procedure[17,18]. Data is transmitted from a primary processing environment to a secondary processing environment. This is done for back up of data at secondary processing environment. A particular method along with a system was developed for recovering a host image of a client device. This image is put in a recovery machine by comparing the profile of client machine with recovery machine. These profiles contain a minimum of one parameter which will be used for analysis and assessment at a later point of time. Conformity procedures are followed on equivalent property of recovery machine. Host image transmission is permitted via a network to the recovery machine. Parameter chosen in this regard play a crucial role for processing the host image in the secondary site of recovery machine[19–21]. As discussed in the above literature on storing the data at secondary sites and recovery machines for disaster data recovery also using pipelined structures for data transmission; this concept uses cloud storage facilities for secondary backup simplifying data recovery process. It doesn't need any peculiar secondary storage servers at a specified location. Data is encapsulated in back up data streams which are then transmitted to a cloud storage. However, a backup metadata is created for each back up data stream and is transferred to the cloud service. This can be the forms of manifest files which contain all basic information about the original backup data [22,23]. A special recovery back up system is enabled for accessing the data deposited on the internet (environment being cloud). Pictorial representation is shown in the Figure 3.

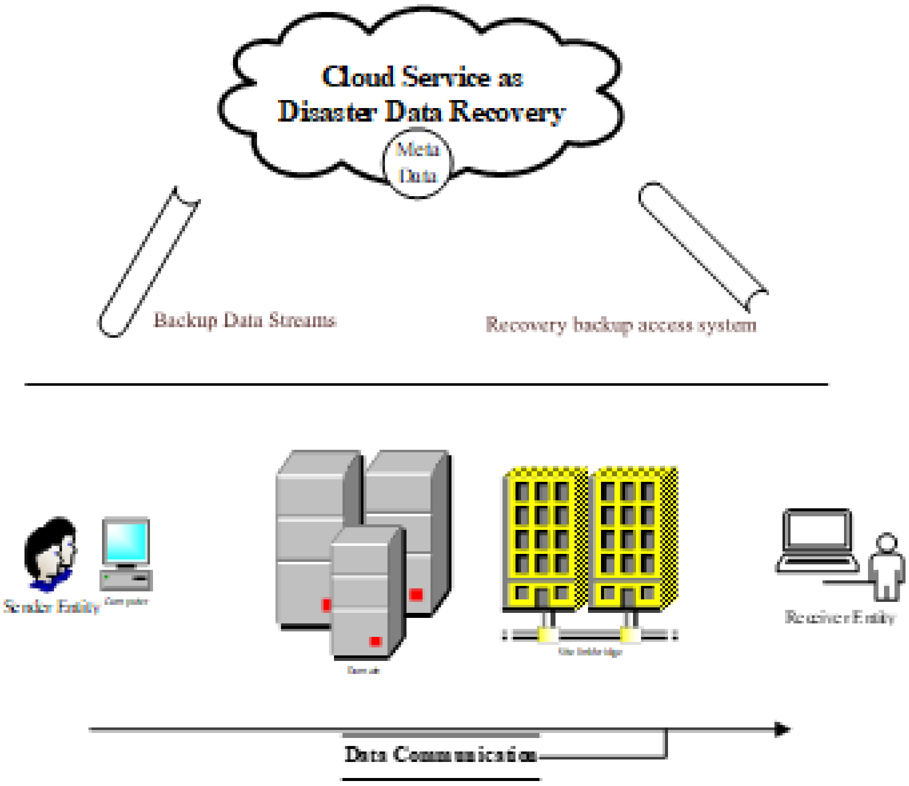

Fig 3. Cloud service scenario for disaster data retrieval

BCP (Business continuity planning) is achieved through a thorough and effective disaster recovery process in place for any organisations [24,25].

A method related to utilization of quorum disk in split storage cluster environment is illustrated with regards to disaster recovery over databases. Access to the admin is provided through quorum disk when there are communication issues among storage systems which is in turn based on storage system I/O performance. Accesses and their respective priorities are provided for the storage systems which has higher performance just before the link failure. Cluster formation and quorum disk access is given based on a predetermined timer concept [26]. Cloud computing generally has multiple service; one to mention is 'software as a service'. These mechanisms provide various facilities for its customers. Similarly, an optimised system is introduced named as 'disaster-recovery-as-a-service'. It performs an effective check on to attacked data sets for replicating the information from a source site to a target site. This is done with minimum cost for the target site to perform well in disaster recovery process [27].

Cost plays a crucial role in disaster recovery process and its allied methodologies. In this regard in order to monitor the cost related issues a dash board kind of graphical user interface (GUI) is developed with appropriate parameters for analysis. There are two windows cascaded in the GUI, first one having catalogue of modules and second one contains generated disaster recovery configurations. Metrics are used to generate the disaster recovery configurations in correlation with both the windows for graphical comparisons [28].

2 Design aspects of the application domain

This section provide an insight on to the design perspective of proposed notion of disaster recovery for an attacked network. It is explained with use case mode representation in Unified Modelling Language (UML) [29]. In software development life cycle, modelling phase has two sub phases Analysis and Design. These sub phases are better explained with UML which is a descriptive language which helps to visualize design of a particular application. The following Figure 4 is a use case modelling which has actors, use cases, connection among use cases and association between actor and use case. Relationship amongst use cases are called as 'includes' and 'extends'. Linking between a use case and an actor is generally an association. All the use cases are put in a system boundary or application boundary. Actor is an object who cooperates with the structure's use cases. Use cases are the activities executed by the actors of a system. They contain set of events or transactions required to bring out the action. Three main use cases are considered in the context of the application with three actors playing their respective roles in the system. Three actors are as follows:

- **User in the Network:**
  User entity working with the personal computers in the private network, he is controlled by the policies and regulations from the admin's desk. He will have credentials provided for accessing the resources of the network.
- **Network Admin:**
  The one who monitors, identifies and controls the issues over the network. He also provides appropriate rights based credentials to the users and systems.
- **Attacker:**
  Attacker is an assumed entity, where he plays a crucial role in attack simulation scenario. He can think as a pen tester/ white hat hacker who intentionally penetrates into the system to find the security holes.

2.1 First scenario: Data transmission use case

As mentioned before every use case is defined by the set of events carried as a whole to perform the activity involved in the use cases. Network admin and user are the actors connected to this use case. It has a sub use case called as 'erroneous_case'. Events for the use case are as follows.

1. User of the system logs in to the network
   (a) Enters his/ her unique credentials
2. User drafts a message and transmits to the destination
   (a) Data link layer forms the frames by adding header and trailer (error check)
   (b) Network layer uses IP protocol and forms packets and sends it to the outside network
3. There can be a chance of error in transmission due to network issues or
4. The message gets delivered to the appropriate recipient

2.2 Second scenario: Troubleshooting use case

This use case is connected to network admin for the purpose of resolving issues over the network. It has two sub use cases one being Provenance_Data and other Packet_Analysis. Events for the use case are as follows.

1. Log in to the server of the network
2. Collect the provenance ledger file
3. Identify the issues with packets using packet analysis process
4. Identify the communication links and connected systems which were found to be inactive or seemed to be inactive
5. Marking the system Id, Packet Id and communication links of the respective resources
6. Troubleshooting the same by isolating the identified resources
7. Resuming the network for as usual business from the disaster recovery

2.3 Third scenario: Attack module use case

Attack module is connected to Network_Admin and Attacker actors in the system domain. It has an exception use case named 'Network_failure'. Events for the use case are as follows.

1. Penetrates into the system as vulnerable entity
2. Attacker searches for a security hole in the network
3. Compromises a weakly connected computer in the system
4. Transmits virus files into the network and attacks the server

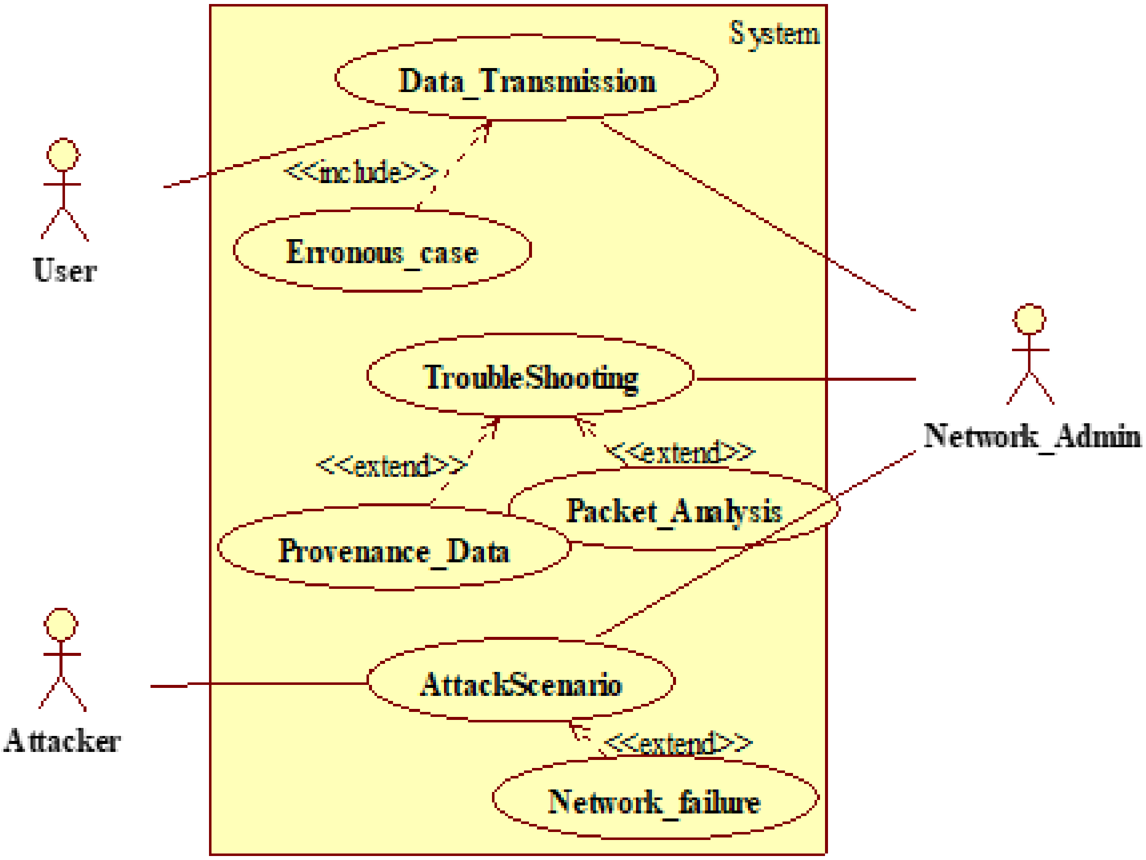

Fig 4. Use case modelling in UML for the considered application domain

3 Results and Discussion

Five parameters have been considered for simulation and experimentation related to a private network attack scenario. All this information and variables associated to considered parameters are collected from provenance data which is represented as a ledger entity. A data set is collected as a record of utilizing the application with a sample size of 200 entries on all parameters. Graphical analysis and visualizations are run in IBM's SPSS tool [30,31]. User_ID, Packet_ID, System_ID, TimeStamp and Operations are the parameters chosen. Timestamp is captured and considered for one 24-Hr interval over the network operations namely Inject, Delete, Update and Transmit. Operations are recorded as events related to cyber-attack context on to the information assets in the private network. All the four parameters of the 'operation' variable are numbered from 1 to 4 for numerical analysis. Operation variable is considered to be ordinal variable whereas remaining all are scale variables in SPSS.

3.1 Histogram analysis of the selected parameters

The histogram analysis with a normal curve of the variables chosen are depicted in the following representation of the Figure 5.

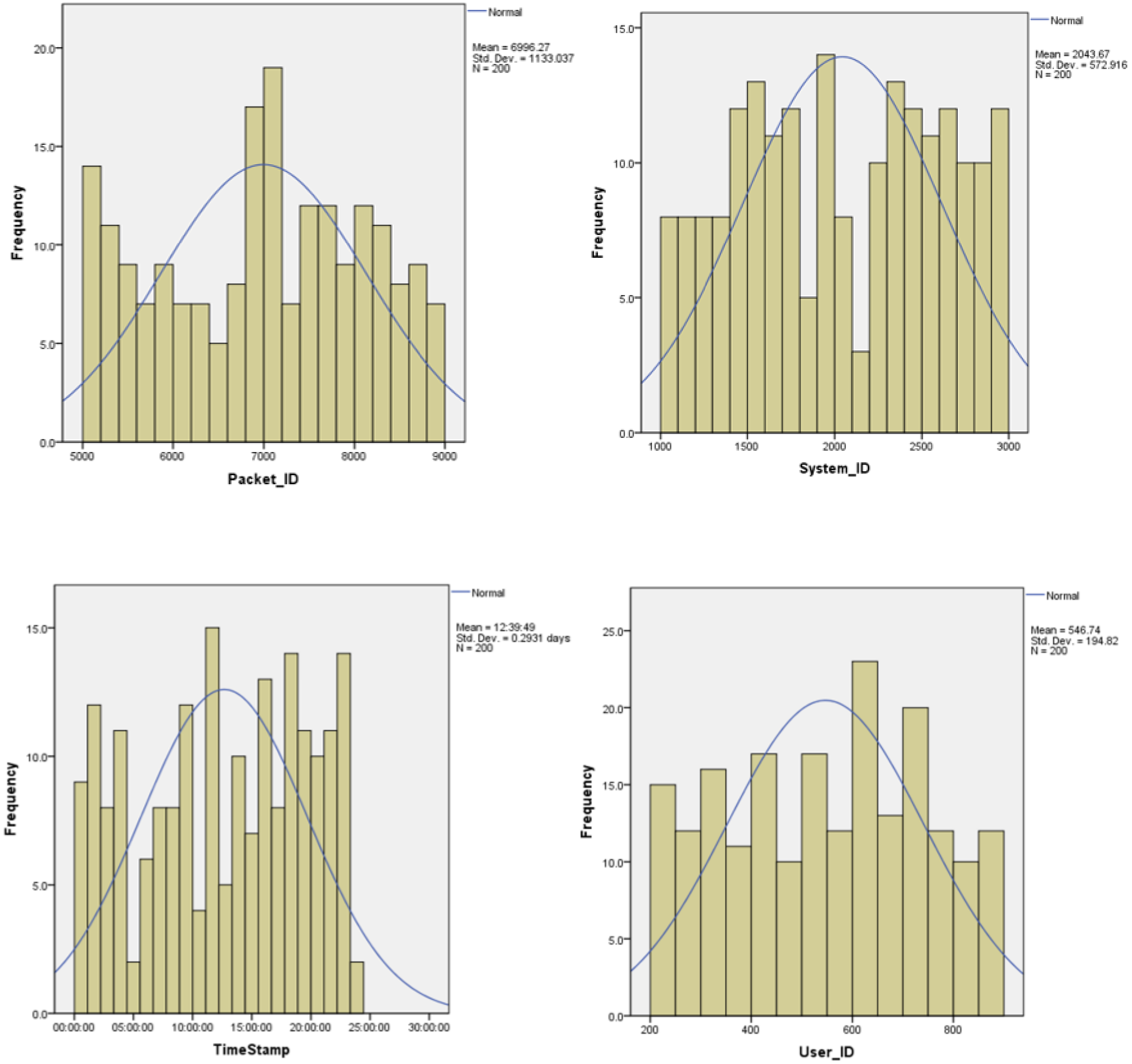

Fig 5. Histogram analysis of Packet_ID, System_ID, User_ID and TimeStamp (clock-wise) values against their frequency of occurrences.

3.2 Analysis on numerical variables across their frequency and operations

The representations from Figure 6. Depicts the information about users in the network performing four mentioned operations captured with their user id, system id and timestamp.

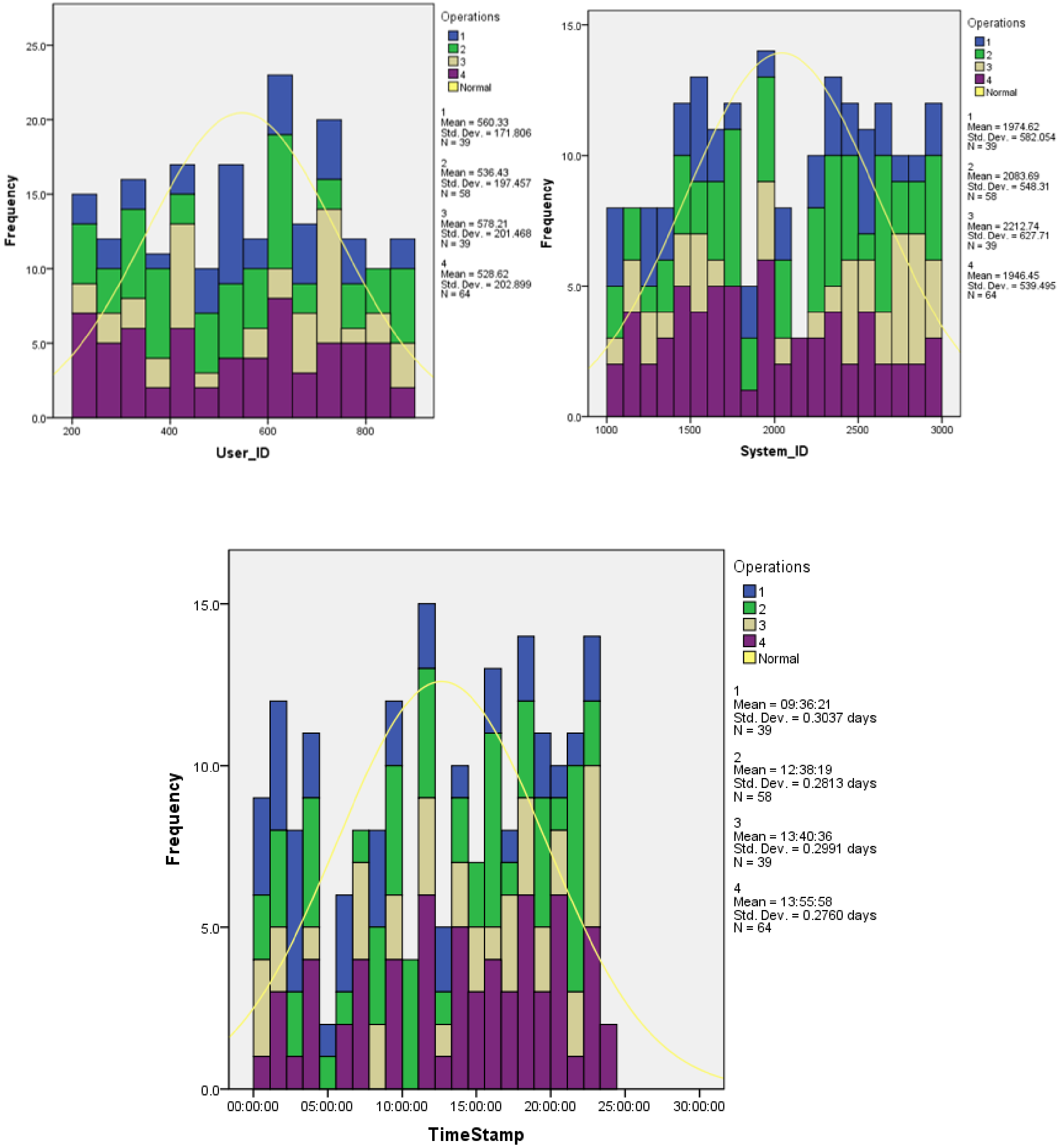

Fig 6. User_ID, System_ID and TimeStamp variables across Operations performed (clockwise) for statistical analysis

600 to 650 user ids have more operations performed and the same can be observed from the above Figure 6. 1900 to 2000 numbered and associated systems in the network have performed more number of times the four operations in the network. 10:00:00-11:00:00 seems to be the time period where the highest number of operations performed in the network. The same is drawn from the Figure 6.

3.3 Scatter dot analysis against System-Id variable

The scatter dot graphical representation of packet id, user id and timestamp against system id over the four operations with appropriate colours are represented in Figure 7. This analysis will help in identifying the cyber-attack based issue at a particular system/ computer in the private network.

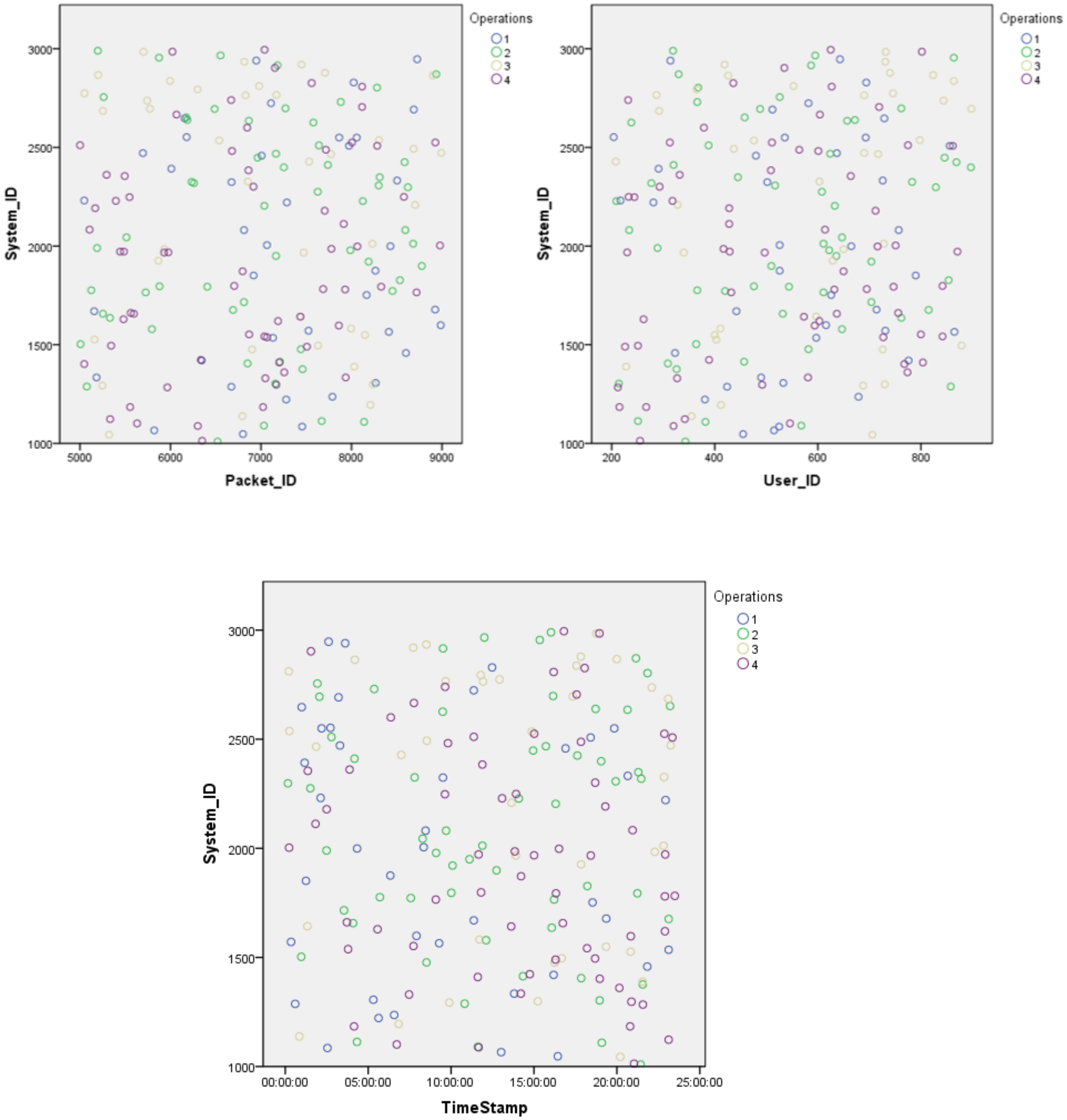

Fig 7. Packet_ID, User_ID and TimeStamp variables across System_ID (clockwise) for statistical analysis on scatter dot graph

Below Figure 8 is the depiction of captured used Ids from the network. Almost all of them have unique identities in the network. Similar contexts can be captured for other variables which are system Id, Timestamp and packet Id. The four operations Inject, Delete, Update and Transmit named from 1 to 4 and their respective occurrences/ frequencies are shown in Table 1 with percentages.

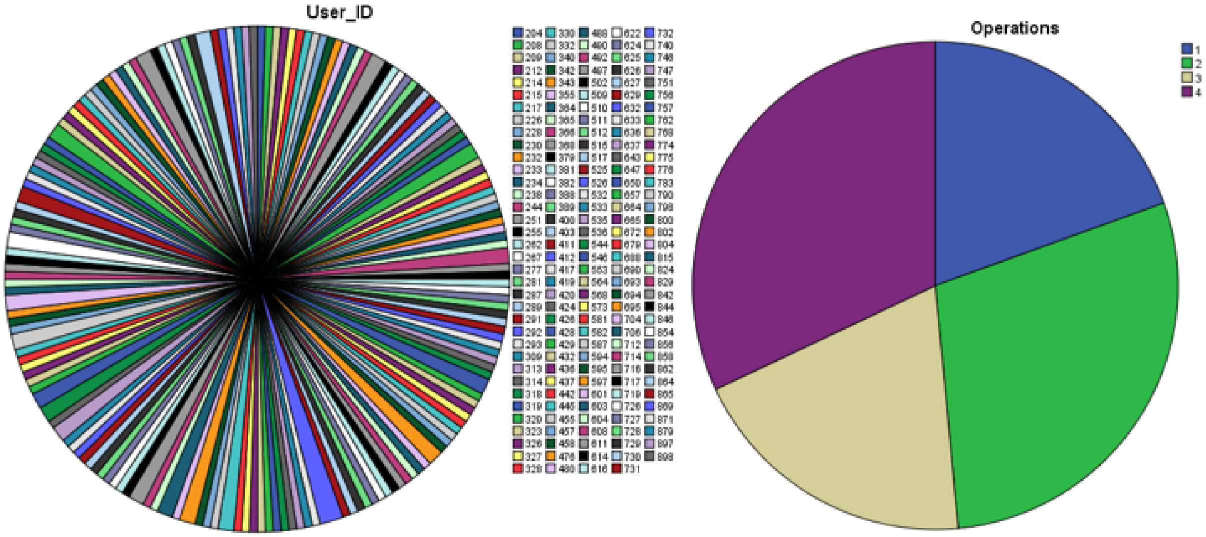

Fig 8. Pie chart analysis of considered variables in a network attack scenario

Table 1. Frequency and percentages of considered operations by user

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	39	19.5	19.5	19.5
	2	58	29.0	29.0	48.5
	3	39	19.5	19.5	68.0
	4	64	32.0	32.0	100.0
	Total	200	100.0	100.0	

3.4 One sample T-Test results

In order to know the connectivity concerns between two variables System_ID and User_ID, a statistical test names 'One sample T-Test' is conducted[32]. Connectivity between the aforementioned variables is considered to be the hypothesis in this regard. Values associated to Mean, Standard deviation and Standard error mean are mentioned in the Table 2. Confidence intervals with mean difference and significant values are shown in Table 3. As the significant value which is 0.00 and is less than 0.05 (pre-determined probability value); we discard null hypothesis and confirm that the availability of handful difference between the obtained values of System_ID and User_ID Appropriate representations of in bar graph and line graph associated to statistics of one sample t test are provided in Figure 9.

Table 2. Values of mean and standard deviation of one sample T Test

Name	N	Mean	Std. Deviation	Std. Error Mean
System_ID	200	2043.67	572.916	40.511
User_ID	200	546.74	194.820	13.776

Table 3. Significant value, mean difference and confidence intervals of two variables

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
System_ID	50.447	199	.000	2043.67	1963.78	2123.56
User_ID	39.688	199	.000	546.740	519.57	573.91

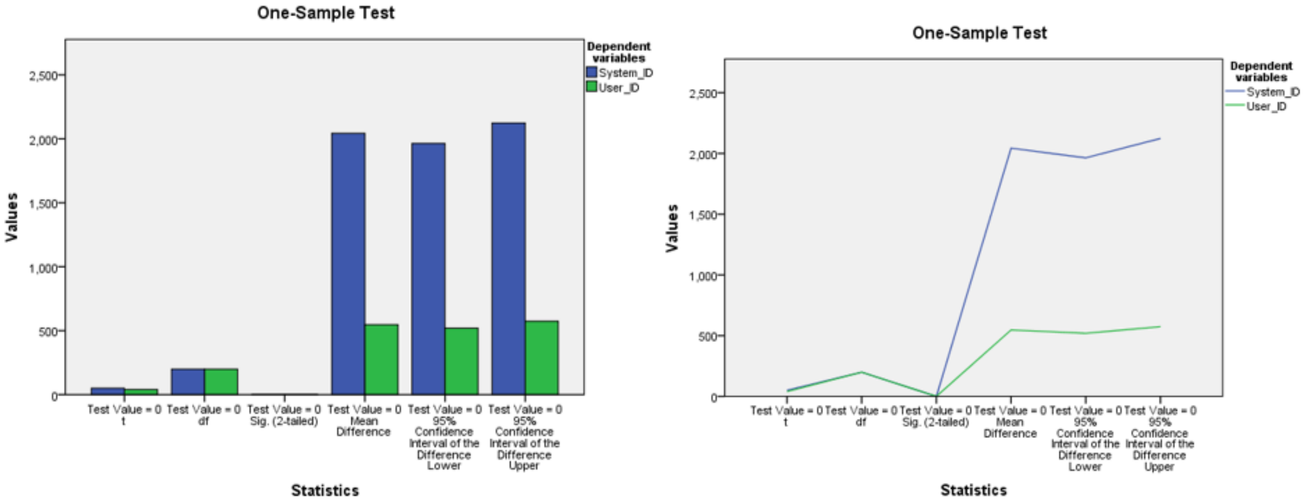

Fig 9. Graphical analysis of one sample T-Test results

Using such approaches and methodologies which are considered from provenance data, a particular issues can be identified, assessed and controlled in private networks. Troubleshooting the issue using such process oriented methodology helps in resolving the problem with a decent success rate.

4 Conclusion

A private network environment is taken into consideration for understanding and analyzing the trouble shooting process of a cyber-attack scenario. The variables considered for the statistical analysis are picked from the provenance data of the network which is the unique aspect of the proposed problem statement. Captured results via graphical analysis provides information on specific issue resolution and related disaster recovery process of computer networks. Associated literature on provenance, risk management, disaster recovery and cyber security are provided with appropriate pictorial illustrations. In conclusion, carrying out such activities for resolving network related problems helps in business continuity planning and acts as disaster recovery process for the organizations. We have shown the association between the selected variables using statistical test of significant probability value. We connect provenance data as a solution for disaster recovery and execute the same with risk management approach of information security. Small size private network for experimentation is considered, the same troubleshooting process can be extended to a mid-sized or a larger organization.

References

1) Bowerman, S. Kristopher. ”Cybersecurity Threats and Technology Applications in Homeland Security.” Homeland Security Technologies for the 21st Century (2017): 135-148. .
2) Sharma S, Krishna CR, Sahay SK. Detection of advanced malware by machine learning techniques. In: Soft Computing: Theories and Applications. Springer. 2019;p. 333–342. Available from: https://doi.org/10.1007/978-981-13-0589-4_31.
3) Asri S, Pranggono B. Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure. *Wireless Personal Communications*. 2015;83(3):2211–2223. Available from: https://dx.doi.org/10.1007/s11277-015-2510-3.
4) Yu S. Distributed denial of service attack and defense. New York. Springer. 2014.
5) Deshmukh RV, Devadkar KK. Understanding DDoS Attack & its Effect in Cloud Environment. *Procedia Computer Science*. 2015;49:202–210. Available from: https://dx.doi.org/10.1016/j.procs.2015.04.245.
6) Kumar P, Pateriya RK. A survey on SQL injection attacks, detection and prevention techniques. *Third International Conference on Computing, Communication and Networking Technologies (ICCCNT’12)*. 2012. Available from: https://doi:10.1109/ICCCNT.2012.6396096.

7) Morris R, Thompson K. Password security: A case history. *Communications of the ACM*. 1979;22:594–597. Available from: https://doi.org/10.1145/359168.359172.

8) Mishra S, Dhillon G. Information systems security governance research: a behavioral perspective. In: and others, editor. 1st annual symposium on information assurance, academic track of 9th annual NYS cyber security conference. 2006;p. 27–35. Available from: https://www.albany.edu/iasymposium/proceedings/2006/mishra.pdf.

9) Dhillon G, Syed R, Pedron C. Interpreting information security culture: An organizational transformation case study. *Computers & Security*. 2016;56:63–69. Available from: https://dx.doi.org/10.1016/j.cose.2015.10.001.

10) Veiga AD. Comparing the information security culture of employees who had read the information security policy and those who had not. *Information & Computer Security*. 2016;24(2):139–151. Available from: https://dx.doi.org/10.1108/ics-12-2015-0048.

11) Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*. 2009;18(2):106–125. Available from: https://dx.doi.org/10.1057/ejis.2009.6.

12) Huang HW, Parolia N, Cheng KT. Willingness and Ability to Perform Information Security Compliance Behavior: Psychological Ownership and Self-Efficacy Perspective. *PACIS*. 2016. Available from: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1079&context=pacis2016.

13) Sommestad T, Karlzén H, Hallberg J. The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems*. 2019;59(4):344–353. Available from: https://www.tandfonline.com/doi/10.1080/08874417.2017.1368421.

14) Whitman ME, Mattord HJ. Principles of information security. Cengage Learning. Cengage Learning. 2011.

15) Buneman P, Khanna S, Tan WC. Data provenance: Some basic issues. In: International Conference on Foundations of Software Technology and Theoretical Computer Science. Berlin, Heidelberg. Springer. 2000. Available from: https://doi.org/10.1007/3-540-44450-5_6.

16) Bhuyan FA, Lu S, Reynolds R, Zhang J, Ahmed I. A Security Framework for Scientific Workflow Provenance Access Control Policies. *IEEE Transactions on Services Computing*. 2019. Available from: https://dx.doi.org/10.1109/tsc.2019.2921586.

17) Ramakrishnan KK, et al. "Pipelined data replication for disaster recovery." U.S. Patent No. 10,152,398. 11 Dec. 2018. 2018.

18) Elkhodr M, Alsinglawi B. Data provenance and trust establishment in the Internet of Things. *Security and Privacy*. 2020;3(3). Available from: https://dx.doi.org/10.1002/spy2.99.

19) Po-Hsin WEI, et al. "Automated disaster recovery system and method." U.S. Patent No. 10,073,745. 11 Sep. 2018. 2018.

20) Hu R, Yan Z, Ding W, et al. A survey on data provenance in IoT. World Wide Web 23, 1441–1463 (2020). . Available from: https://doi.org/10.1007/s11280-019-00746-1.

21) Siddiqui MS, Rahman A, Nadeem A, M A. Secure Data Provenance in Internet of Things based Networks by Outsourcing Attribute based Signatures and using Bloom Filters. *International Journal of Advanced Computer Science and Applications*. 2019;10(5). Available from: https://dx.doi.org/10.14569/ijacsa.2019.0100529.

22) Parab N. "Cloud-based disaster recovery of backup data and metadata." U.S. Patent No. 9,501,365. 22 Nov. 2016. .

23) Saad MIM, Jalil KA, Manaf M. Achieving trust in cloud computing using secure data provenance. In: 2014 IEEE Conference on Open Systems (ICOS). 2014;p. 84–88. Available from: https://doi.org/10.1109/ICOS.2014.7042634.

24) Wallace M, Webber L. The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets. Amacom. 2017.

25) Haque S, Atkison T. A Forensic Enabled Data Provenance Model for Public Cloud. *Journal of Digital Forensics, Security and Law*. 2018;13(3). Available from: https://dx.doi.org/10.15394/jdfsl.2018.1570.

26) Cao, Ke M, Yin W, Zhao N. "Disaster recovery for split storage cluster." U.S. Patent No. 10,534,767. 14 Jan. 2020. .

27) Hagan T, et al. "Optimized disaster-recovery-as-a-service system." U.S. Patent No. 10,572,354. 25 Feb. 2020.

28) Bates JW, Vekiarides N, Geisel B. "Method for data disaster recovery assessment and planning." U.S. Patent No. 10,481,962. 19 Nov. 2019.

29) Fowler M, Distilled UML. A brief guide to the Standard Object Modeling Language. and others, editor. 2003.

30) Wagner EW. Using IBM® SPSS® statistics for research methods and social science statistics. Sage Publications. 2019.

31) Homer MS. An introduction to secondary data analysis with IBM SPSS statistics. *Educational Review*. 2018;70(2):251–252.

32) Joseph MA. Getting started with SPSS, one-sample t-test, z-test for single proportion. In: and others, editor. APHA's 2019 Annual Meeting and Expo. American Public Health Association. 2019.