The Best Methodologies and Techniques to Avoid Data Loss in the World of Computing

Ali Saleh Altuwayjiri[1], Abdullah Sulaiman Alassaf[2]

[1]Cyber Security and Networks Trainer at TVTC, The Shinan College of Technology, Saudi Arabia
[2]Cyber Security and Networks Trainer at TVTC, Hafr Albatin College of Technology, Saudi Arabia

ABSTRACT

The data loss and data corruption are the most common problems of the systems and laptops nowadays. Data loss is associated with losing important data due to accidental issues in hardware or by internal issues related to software. This paper is aimed at addressing the information that helps in managing the data losses and data corruption by providing more insight about the reasons, preventions, solutions, and various data recovery techniques. The reasons of data corruption and loss includes inappropriate exit from system, providing accessing rights to unauthorized users, malware infection and using duplicate software. While the solutions of managing data loss include Adaptive Data Loss Prevention Technique, sensor method and data archiving process. The data recovery techniques are essential for finding out the appropriate data. Data recovery is the process in which the deleted and inaccessible data will be recovered from the storage media. The storage media can be the hard drives, storage devices and the optical media. There are various methods by which the data recovery can be done. The main reasons for the loss of the data are cold booting and heat booting. Therefore this paper highlights the important information related to data loss and data corruption and is aimed at limiting the loss by providing insights about managing the data loss effectively.

Keywords: Data, loss, corruption, prevention, solution, recovery, booting, optical, media, technique, storage, sensor, archiving, hardware, software, process, files, hard disk

Data Loss

The most common problem in the system and laptop nowadays is the corruption of data and the loss of data. Data loss is to lose some important data due to some accidental issues related to the hardware or by any internal issues related to the software. Some major reasons for the data loss are corruption of data, bugs related to the hardware, hacking by specialized hackers and simple failure of power.

How to Prevent Data Loss?

Prevention of data loss is essential for the future. To preserve the data, some points are to be followed. Users should:

1. Not save the data on the same drive where the operating system is stored.
2. Try to keep a backup of the data on the external hard disk or on any other storage devices like Pen Drive.
3. Not open E-mails and attachments without proper authentication.
4. Try to store the hardcopy of the documents.
5. Try to avoid common errors related to the data loss.
6. Be properly encrypted so that it can only be opened through the encrypted key provided by the authorized users (Albright, 2014).

Data Corruption

Data corruption is the damage or maltreatment of the data. In that case, it becomes quite impossible to recover the data again. The reasons behind the data corruption may be human mistakes, lack of hardware responses and Software errors. Data Corruption may also reduce the data quality of the original data.

Data corruption in the file sometimes may also damage the other linked files (Data Corruption, 2009).

Common Signs for Data Corruption

Sometimes it becomes quite a difficult task for the user to identify the signs for data corruption. The conversion of data into symbols and numbers, the changes in the names of files and folders when they run on another machine are some of the common examples. Data corruption may also occur due to an unwanted virus in the system. Some of the common signs for data corruption are the following:

- Change in the format of file.
- Files and folders are renamed with other meaningless names and characters
- Accessing and authentication rights of the files and folders may also change
- The continuous hanging of the computer while working
- The crashing of the hard disk becomes very rapid
- Processing of software becomes slow
- Output generation becomes less productive.

Reasons for Data Corruption

The reasons for data corruption may be in the form of very small mistakes done by the users. The reasons behind data corruption may be certain or uncertain sometimes. The most important reasons for data corruption are as shown below:

- **Inappropriate Exit from the System**
  The inappropriate shutdown of personal mail IDs and unusual closing of the system may also lead to the corruption of the data. Some of the other related issues are pressing and holding the starting button again and again or improper shutdown of the setup. This may also corrupt the system as well as the data associated with it.
- **By providing access rights to unauthorized users**
  Sometimes to complete the task, the accessing rights are provided to unauthorized users who can further access the system and the data for their personal uses. This unauthorized accessing may also corrupt the data and damage the data sometimes. Digital signatures and encoders must be provided to the multiusers who are operating on the same system to avoid the data corruption (Poulsen, 2013).
- **Malicious Malware Infection**
  Malicious malware infection is a serious reason for the corruption of data. Some sources maliciously send Trojan horses, virus and worms to the system in the form of attachments to reveal the information from the system or to corrupt the data in the system. The malicious users may be hackers.
- **By Using Duplicate Software**
  Various users nowadays are using unauthorized duplicate software for their system. This software is available in a very less amount than the original software. But the use of duplicate software will reduce the working efficiency of the computers and can also corrupt the data, for instance, copying of software from one system rather than purchasing the original one from the market.
- **Hardware Defects**
  Hardware defects are related to system failure and other peripheral device failure. These hardware defects will also corrupt the data and the prevention of data loss in this situation becomes quite tough. For example, in the absence of UPS the software may face issues due to sudden power failure, which might delete or can corrupt the data. In fact, after opening the file again the data will appear in the corrupted form.
- **Improper Installation of Firewalls**
  Firewalls are essential for protecting the system from outer, unauthorized accessing. The original firewall provides complete protection to the system and the data stored in the system too. If the firewall is a duplicate or the installation of firewalls is incorrect, it will corrupt the data from outer, unauthorized sources. So the proper installation of the firewall must be done.

Prevention from the Data Corruption

Nowadays, in modern technology various options are found to prevent the loss of data. (TheXLab, 2015) Various backup plans and data management techniques are found to prevent the corruption of data. Some of them are specified below:-

Proper Fragmentation of Hard Disk

Data corruption may be prevented by proper fragmentation of the hard disk. For an example, the division may be in C drive, D drive, E drive so that each section may get its definite partition. By doing proper partition, if the files and folders of one drive get corrupt, then it may not affect the data of other drives.

Proper Maintenance of Operating System

An operating system also requires weekly or monthly maintenance to avoid the corruption of data. The maintenance includes updating the operating system with an advanced version, checking the hard disk drive and deletion of unwanted data. Following these practices will increase the performance of the operating system.

Proper ejection of Storage Devices

Storage devices--such as pen drives, card readers, compact drives (C.D'S)--should be properly ejected after being used on the system. By doing a proper ejection of the storage devices, it becomes quite easy to prevent data corruption as well as data loss. Pen drives and other storage devices are also one of the reasons for the source of a virus in the system. So it is essential to scan the drives before running them on the system

Basic knowledge of software and Peripheral devices

Basic knowledge of software and peripheral devices (printers, scanners, etc.) are also essential to prevent the corruption of data. The user can be able to understand the basic structure of networking by which the devices are connected with each other ,so whenever viruses affect the system, the user can easily identify and rectify the issue.

Wise use of UPS (Uninterrupted Power Supply)

Sometimes due to the improper support of the UPS, it becomes tough to maintain the data. Various users do not provide support of UPS to the computers. Due to this at the time of power failure, the stored data will be corrupted. The UPS configuration should also match the set ups configuration to obtain the right results.

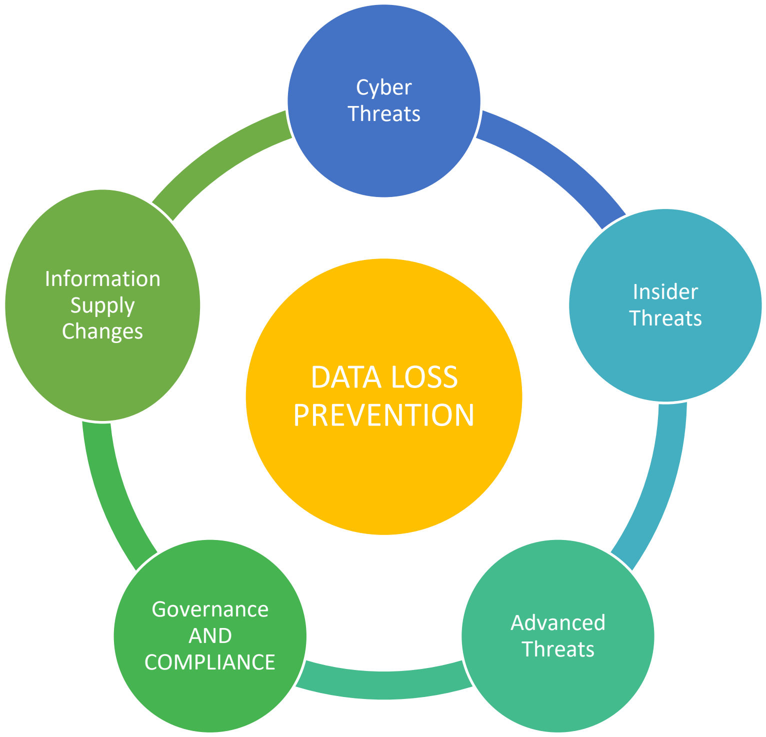
Use of NTFS (New Technology File System)

Advance NTFS is also the solution for preventing file corruption. The NTFS file system's format is really uncomplicated and can easily repair the corrupted and deleted files. The advance file system not only repairs the file, but it can also provide simple wizard, which renames files and folders in case of duplication. Also, filters can search the files on the basis of the priority of repairing them (Centre, 2010).

Data loss Prevention

Data Loss prevention is the process in by which data can be prevented from being taken by various prevention measures. Technically, the DLP is product based on the central management policies which always try to protect and block the loss of data which is in rest, in motion and in use through the analysis of the contents. (Clearswift Team, 2015)

Data loss prevention is also identified by the various names in the market. The common names for data preventions are information leak/loss prevention, Filtering and Monitoring of Contents etc. The Diagram below shows the process of data loss prevention.



Why data loss prevention is essential

data loss prevention (DLP) is primary to protect and secure the data from heavy loss. By data loss prevention techniques, the stability and reliability of the data become more positive. DLP helps an organization in identifying more about the content and also reduces the amount of mistakes generally done by the users while saving the data. By this, data can be saved for a very long time.

By data loss prevention, personal identifiable information (PII) and thinker property can be saved easily from malicious attackers. There are various tools available on the internet which can help the attackers to send the mails to users by which data loss chances will automatically increase. So to avoid this and to prevent data loss, the data loss prevention technique is primary (Team).

DLP solutions VS DLP Featuring

The DLP solutions are related to the prevention of data loss from the central management: creation of the policy, security solutions and basic workflow of the data. In DLP solutions, various types of interfaces are developed, but the user interface is useful in securing and preventing data loss and securing the contents of the data.

The DLP features are useful in analyzing the aspects of DLP solutions and to identify the most appropriate use of DLP solutions in solving the issues and securing the data. DLP features are not really dedicated to solve the issues related to the prevention of data and to create the content awareness.

Process of DLP Selection

It is important to identify the most appropriate DLP selection process for preventing the data loss on a very wide level. The DLP selection process includes the various steps before finding the most suitable technique to stop the data loss.
First, it is required to identify the needs of the organization so that it becomes easier to understand the actual required prevention techniques. (Francia, 2014)

After identifying the needs, the requirements are formalized according to their specialization areas. In formalization, the requirements are distributed to their respective technical fields.

Third step is the evaluation of the products. First, the evaluation plan is prepared on the manual basis and then, the technical application is done according to the plan.

In the last step of the DLP, testing is done. Testing is essential for checking the appropriate technique for maintaining the data's safety and protecting the data from loss. (Liu & R Kuhn, 2010)

Role of Antivirus in DLP

Antivirus plays a very important role in the data loss prevention technique. Some of the very common Antivirus programs are named McAfee, Avast, Kaspersky, etc. The antivirus like McAfee always tries to deploy the data in its actual form and condition. By this deployment, the program streamline the process, and the management of data can become possible. Some ideas related to the role of the antivirus program are also helpful in securing the data.

Policy management can also be done in a very simple manner. Whenever any antivirus is installed in a system, it possesses various terms and conditions regarding the policy to install the antivirus. If the user agreed to those terms and conditions, then only the original antivirus can be installed and this installation of antivirus can help the users protect the data loss.

Installing the appropriate antivirus and upgrading these antivirus programs time to time provides protection of the system from the data loss. The antivirus which is installed on the central network and central server can also help to protect the other systems which are related to that network.

Solution for Data Loss Prevention

The corruption of data and stealing of IP addresses from the office systems becomes common nowadays. To avoid these conditions, some preventive measures should be taken into consideration. The most common preventive measure used is an adaptive data loss technique (A-DLP).

Adaptive Data Loss Prevention Technique (A-DLP)

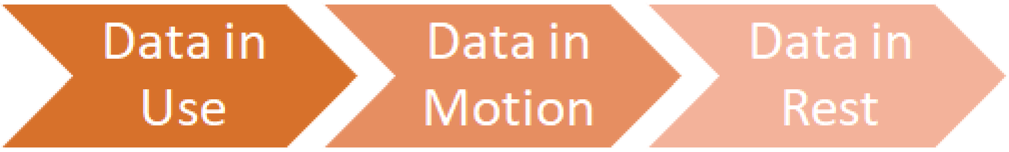
This is the most reliable technique to recover the lost data. In this technique, the centralized data can be easily prevented from loss from all the conditions. To secure the data and to make the network system fully authorized, A-DLP technique is used. (Lakshmi, K. Parish Venkata Kumar, A. Shahnaz Banu, & K. Anj, 2013)

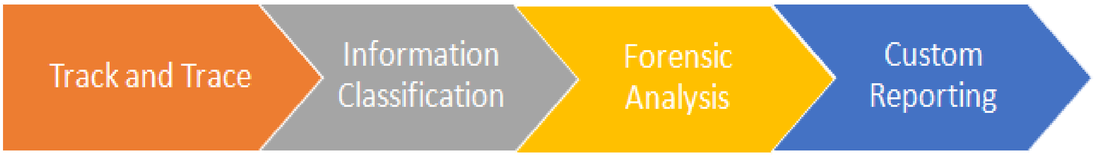
A-DLP can also provide the security solution to the structured, unstructured and semi structured problems which occur in the data on a daily basis. This technique mainly depends on the structure of three processes together, which are described below:

- **Data in Use**
  The used data are related to the utilization of data from various sources either in an authorized manner or in an unauthorized manner. The use of data by the users can be for corporate use or it may be for the external unprotected network. In this step, the security confirmation of the data can be done either in the offline mode or it in the online mode.
- **Data in Motion**
  The data in motion require the online collaboration and coordination of the tools available on the internet. When the data is in motion, the Secure Gateway will provide the protection to sensitive data. This sensitive data may be in the form of corporate data, encrypted data, external and internal data.

- **Data in Rest**
  The data which are prepared or authorized but are not used by the users for ongoing projects or tasks are considered as data at rest. The critical protection agent (CIP) is certified to provide the data which is protected in all the units, namely the HR unit, IT unit and the other auditing units of the organization. The diagram below shows all the steps which are included in the Adaptive Data Loss Prevention Technique. Also the other diagram below shows all the processes related to the completion. (Rouse, 2014)

Diagram of A-DLP





Other Solution
Instead of using adaptive data loss prevention technique, users can also use other techniques to solve the issues related to data prevention. One of the techniques is a pattern matching process which is used at the international level. In this process, appropriate observation of the online data is done like on E-mails, web browsing surfing etc. This process is mainly used to check the insecure transfer of the of data and information related to social security and credit cards. When any unauthorized data get transferred at that time with the help of pattern matching, the data pattern will be checked and prevented if some issues are found at the same time.

The prevention of data from getting leaked can be secured by using the sensor method. Whenever the data like files, documents or file fingerprints are transferred, these sensors will detect an abnormality in the data and the appropriate methods for the prevention can be applied.

One of the most common methods to prevent data loss is the content archiving process. By the content archiving process, the content is stored in the appropriate folders, which are defined by the users. An organization can prepare their archiving folders in to which the data can be transferred. The archiving of data is essential at the time of internal and external auditing.

Data recovery
Data recovery is the process in which the deleted and inaccessible data will be recovered from the storage media. The storage media can be the hard drives, storage devices and the optical media. There are various methods by which the data recovery can be done. Various techniques are defined for the recovery of the data to solve the issues related to loss of data. As it is already been mentioned in the outline of this writing, the data recovery techniques are essential for finding out the appropriate data. The main reasons for the loss of the data are cold booting and heat booting. For this, the recovery techniques can be planned according to the requirements.

The general causes of loss include a virus in the computers, corruption of the data, loss due to computer crimes and human errors, natural disaster and mechanical failure. To avoid this loss, the recovery techniques are required. Data recovery may also help to recover the legal documents and restore the hidden or deleted information. By data recovery, the privacy of the data will remain constant and the data prevention in every situation can become possible.

Data Recovery Techniques
Data recovery techniques are those techniques which are mainly related to the recovery of the data. These techniques are various in number and also possess different qualities in providing the output. The recovery techniques can be applied in various fields like database recovery, recovery related to Linux and Unix, recovery related to loss of documentation files, etc. There are various types of recovery techniques which are presented below to prevent the loss of the data. (Amari, 2009)

Active Partition Technique
The main technique used to secure or to recover the data is the active partition technique. By using this technique, the chance of data loss becomes very low, and the recovery of the data can be done very easily. In the active partition, the

disk is divided into various sections or the logical units. After this, the data can be divided into those sections according to the requirement. In this technique one physical drive will be divided into various multiple sections. The software, named as partition editor software, is used which basically focuses on handling and setting the structure of the hard disk. (Team, 2015)

To identify the damage partition and to repair it again, the mini data tool software will be used. This software searches the crash partitions of the hard disk and then repairs that section of the disk so that it may work in an appropriate manner. Whenever the data is lost or damaged while partitioning the disk, it becomes difficult to identify how to recover the data. In this condition the external tools cannot help, so the mini data tool internally helps in making the recovery process of the lost data.

On track Easy Recovery

On track easy recovery process mainly helps Windows to recover the deleted files and retrieve those files which are also damaged due to human errors. This technique is also used to recover the data related to the corrupt files and is used in the form of easy recovery software technique. The On track recovery software licenses are available for users for both Windows and Mac operating systems. (Kroll Ontrack Team, 2015)

On track easy recovery process possesses various versions which are able to work on different types of drives as well as the local storage and external media type. The three versions of the On track easy recovery process are named as professional, home and enterprise. Different users use the “On track easy recovery” process to protect the data and securely erase the data. This software can work on various types of drives and is helpful in easy recovery of the lost or deleted data.

Scanning Probe Microscopy (SPM)

This is the recently used technology which is used to recover lost data. In this technique, a sharp magnetic tip is attached to the pillar to recover the lost data. This structure combines with the lost field stemming to find out the topographic view of the device from where the data has been lost. The cost of this recovery technique is very high, but nowadays for speedy recovery, many organizations are using this recovery technique. The initial introduction of this technique takes more time and money, but once the technology gets introduced in the organization, it will try to provide the productive feedback. (team K. , 2015)

Magnetic Force Microscopy (MFM)

Magnetic Form Microscopy is also derived from the Scanning probe Microscopy. The mechanism of recovery is quite similar to the SPM technology, but after scanning the topographic view, the actual image of the data lost will be created and the data recovery becomes easier. The resolution of this technique will be quite high and the sample selection of this method is very nominal. By this process of sample selection, the organization has to spend the least amount on the completion of the process.

Data recovery algorithms

Data recovery methods are pre-planned and logical ways to recover the data. The data recovery techniques are mainly meant for the consistency, integrity and strength of the data. By using these methods, the data recovery becomes very easy. The recovery methods are mainly divided into two parts, namely actions taken before the data loss and the action taken after the data loss. In the second part, the recovery of data will be done and in that recovery the consistency and transactional activities of the data will be identified. The name of the most common method used for the Data recovery is ARIES (Algorithms for recovery and isolation exploiting semantics). The ARIES algorithm contains three steps named as analysis, Undo and Redo. (Verhofstad, 2012)

Ways to recover the data

The above topic is related to the recovery of the data. The techniques relate only to the common type of data recovery. But sometimes the situation is related to a specific type of recovery of the data. There are various conditions which may occur in the system which will lead to the crashing of the hard drive or data loss. These conditions are cold boot, heat boot and various emergency conditions. The discussion of these situations is defined below.

Data Recovery from Cold Booting

Cold booting is the process in which the computer again starts the booting process by simply switching off the system from the main switch or the main power supply button and again the power supply button needs to be started. Though this is the very simple method to close the system in any situation, sometimes the damage to the hard disk and the data stored on the disk will be very high.

If the data is not saved, even after considering all the precautions, the user has to stop switching off the computer directly. Appropriate steps should be taken into consideration while switching off the computer. (Rouse, reboot (warm boot, cold boot), 2005)

Data Recovery from Heat Booting

The heat boot is also known as the warm boot, soft boot and the gentle boot. These names are provided to heat boot due to the actions performed by the process. The organized shutdown of the computer can be done in the heat boot process.

In heat booting, the data loss chances increase more if the system hangs while performing the task or some internal issues related to hard disk arise. At that time the user has to stop the system by pressing ALT, delete and escape keys continuously. On regular personal computers, the warm boot can be performed by just pressing the control, ALT and delete keys in coordination and in Mac operating system the switch off to the system can be done from the restart button.

Data Recovery from Hard Disk

There are various emergency conditions in which it becomes quite impossible to recover the data quickly, though it is not very hard to obtain the data if the data is lost from the hard disk. But due to very small mistakes done by the users, the condition of losing the data may be created. The initial step to recover the data from the hard disk is to switch off the computer when any error occurs. In various scenarios, the switching on and off to the computer will create damage to the data. The known software can be used for recovery of the data and the use of unknown software will create severe damage to the existing data. And finally, if the situation gets out of control, the users have to take the experts' views to recover the lost data. (Computer Weekly Staff, 2008)

Storage Devices

Storage devices are those devices which are mainly meant to store the data. These devices can be used as the backup for the data. This stored data in the storage devices can be used afterwards, according to the requirement of the user.

The various types of storage devices used for storing the data are pen drives, hard disk drives, secondary storage memory, etc. There are various aspects in considering which data can be stored on the storage devices. The fundamentals of storing the data on storage devices are explained below.

Fundamentals of storing the data on storage devices.

The temporary storage of data will increase the chances of losing the data very frequently. The permanent solution is essential. To store the data permanently, it is essential to select permanent storage devices. The permanent storage devices are also called secondary storage devices. The data will remain consistent even if the system gets shut down. The data can also remain safe from a virus and natural disasters. (CSCI Team, 2003)

The **Mass storage** of the storage devices is advanced with a very strong storing capacity. These devices are able to store the data up to a strong level. The backup of a whole organization can even be taken into one storage device. The technical person can increase the storage of the device by simply dividing the disk into various sections. If the division of the disk are appropriate, more storage capacity will be developed to store more data. The division of the disk may be done in two ways, namely SATA and PATA.

The storage devices also possess a **non volatile** nature to store the data. By the non volatile nature of these devices, the consistency of the devices remains constant. The data will remain stable even if the power is off or the user switches off the computer. This data can be saved for a very long lasting period. Whenever the users require this data, they can use it according to the requirement. (Thakur)

The Cost Effective approach is also considered as an additional advantage of the storage devices. There are various storage devices which are useful to store the data and are available at a lower price in the market. Nowadays, with the improvement in technology, the medium to store the data is changing and the storage devices are available in a very small size with a large storing capacity. The USB storage devices, data storage memory cards for smart phones and iPhones, hard disk to take the backup of the data stored in an organization are the best examples of cost effective storage devices.

Reusability of these storage devices will make the device cost effective. By using these devices regularly, the storage capacity of the storage devices can be used again and again. For data storage, these devices can be reused whenever required. In the very initial stage, the CD drives and the pen drives are used for storage. These devices possess less storage capacity so to recover this issue the new storage devices are introduced. By introducing these storage devices, the chances of reusability are increased.

Steps of storing the data on Devices

In computer systems, the data can be stored in various steps. The internal structure of the computer system consists of different parts. The fundamentals to store the data are essential to identify. Generally, when the data is lost, it becomes quite difficult to identify that part which is creating the technical barrier. The steps to store the data are decided according to the parts composed in the system.

In the first step, the memory hierarchy should be identified properly. Memory hierarchy means whenever the data is recovered, The program chooses which memory is most helpful to the user in recovering the data. Various types of memory are found in the memory hierarchy named as volatile memory, primary memory, secondary memory and cache memory. The easiest way to recover the data is mainly from the secondary memory. In secondary memory, the data will be saved for a long time and will be very secure.

After identifying the memory hierarchy, the disk storage and the structure related to the disk storage will be identified. In disk storage the magnetic sectors are responsible for storing the data. These sectors are also divided into the tracks which are helpful in storing the data individually. These sectors also increase the storage capacity of the secondary memory.

In the last step, whenever the user saves the work on the system, that work will directly get saved in the secondary storage memory so that it may be used in the future. Various users also use devices to store the data and take a backup of this data in the storage medium like pen drives, USB and Hard disk drive. The reasons for the data loss may be the human errors, corruption of files, attack of a virus on the system and many others. In this condition, if the data is lost, it can be recovered by using various recovery techniques.

Various disk controllers or disk management devices are used to show the appropriate disk checking process. These disk controllers are also helpful in sorting the data according to their priority to be stored in the secondary storage medium. For sorting the data, various types of sorting techniques are applied to the data to manage it appropriately. After these steps, the data will be stored in the storage medium and can be used for the future perspectives.

By the above, it becomes quite clear that with the increase in technology the storage medium for data storage and the techniques for recovery will also increase. These techniques will help the users to establish the integrity, consistency and strength of the data. The various steps shown in storing the data are also presenting the sequential storage of data in the secondary storage medium.

REFERENCES

[1]. Albright, D. (2014). Data loss and data recovery. Retrieved from www.makeuseof.com: http://www.makeuseof.com/tag/data-recovery-work/

[2]. Amari, K. (2009). Techniques and tools for recovering and analyzing data from volatile memory . SANS Institute. Retrieved from http://www.sans.org/reading-room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory-33049

[3]. Centre, A. D. (2010). Tips to prevent data loss. support. Retrieved from http://www.adrc.com/sm/prevent_data_loss_tips.html

[4]. Clearswift Team. (2015). Discover, secure and manage your critical information. Retrieved from www.clearswift.com: http://www.clearswift.com/solutions/data-loss-prevention

[5]. Computer Weekly Staff. (2008, May). Computer data recovery -- Essential guide. *TechTarget* Retrieved from www.computerweekly.co: http://www.computerweekly.com/feature/Computer-data-recovery-Essential-Guide

[6]. CSCI Team. (2003, Spring). Fundamentals of data storage for databases.Retrieved from http://www.cs.cofc.edu/~pother/courses/csci432/chapter1.pdf

[7]. Data corruption (2009). Retrieved from http://www.datarecovery.com.sg/data_recovery/data_corruption.htm

[8]. Francia, J. (2014). Data loss prevention (DLP) solutions. FORTINET Retrieved from www.fortinet.com: http://www.fortinet.com/solutions/data_loss_prevention.html

[9]. Kroll Ontrack Team. (2015). *Ontrack EasyRecovery, brings your Windows data files back to life!* Retrieved from www.ontrackdatarecovery.com.au: http://www.ontrackdatarecovery.com.au/file-recovery-for-windows/

[10]. Lakshmi, B., K. Parish Venkata Kumar, A. Shahnaz Banu, & K. Anj. (2013). Data confidentiality and loss prevention using virtual private database. International Journal on Computer Science and Engineering, 5(3), 143-149. Retrieved from http://tcna.primo.hosted.exlibrisgroup.com/primo_library/libweb/action/display.do?tabs=detailsTab&ct=display&fn=search&doc=TN_doaj6e2246698c0743a2a81e201e2cebabd6&indx=3&recIds=TN_doaj6e2246698c0743a2a81e201e2cebabd6&recIdxs=2&elementId=2&renderMode=poppe

[11]. Liu, S., & R Kuhn. (2010). Data loss prevention. IEEE Journals & magazines, 12(2), 10-13. Retrieved from http://tcna.primo.hosted.exlibrisgroup.com/primo_library/libweb/action/display.do?tabs=detailsTab&ct=display&fn=search&doc=TN_ieee10.1109%2fMITP.2010.52&indx=1&recIds=TN_ieee10.1109%2fMITP.2010.52&recIdxs=0&elementId=0&renderMode=poppedOut&displayMode=ful

[12]. Poulsen, L. (2013). What is data loss and how can your business prevent it?Retrieved from www.businessbee.com: http://www.businessbee.com/resources/technology/security/what-is-data-loss-and-how-can-your-business-prevent-it/

[13]. Rouse, M. (2005,September). Reboot (warm boot, cold boot). *Whatis* Retrieved from whatis.techtarget.com: http://whatis.techtarget.com/definition/reboot-warm-boot-cold-boot

[14]. Rouse, M. (2014). data loss prevention (DLP). Retrieved from whatis.techtarget.com: http://whatis.techtarget.com/definition/data-loss-prevention-DLP

[15]. Team, K. (2015). Data recovery software *:* Ontrack® EasyRecovery. Retrieved from http://www.krollontrack.com: http://www.krollontrack.com/data-recovery/recovery-software/

[16]. Team, M. T. (2015). Recover damaged partition. Retrieved from www.powerdatarecovery.com: http://www.powerdatarecovery.com/free-file-recovery-software/recover-damaged-partition.html

[17]. Team, S. L. (n.d.). understanding and selecting a data loss prevention solution. SANS Institute. Websense. Retrieved from https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf

[18]. Thakur, D. (n.d.). Storage devices. *Computer notes* Retrieved from DINESH THAKUR: http://ecomputernotes.com/fundamental/input-output-and-memory/explain-secondary-storage-devices

[19]. TheXLab. (2015). Data corruption and loss: causes and avoidance. x book. Retrieved from http://www.thexlab.com/faqs/datacorruption.html

[20]. Verhofstad, J. (2012). Recovery techniques for database systems. University of California, Department of Electrical Engineering and Computer Sciences, Berkeley. Retrieved from http://infolab.stanford.edu/~manku/quals/summaries/spiller-recovery.htm