WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Data Privacy, Security and Protection at Client Side Offline Mode

*Qaisar Fareed*

**Magadh University**

**ABSTRACT:-**

Study, observations. analysis, extraction of related points, detection, reasons and their possible solution Data Privacy, Security and Protection only at client side offline mode .All possible ways to analyze where data can travel, transfer, transmit, store, retain, retrieve, access and be used in an interconnected system or device which has an IPO (Input Process Output) cycle in order to ensure smooth transfer of data and secure them from unauthorized access. This includes new proposed concepts and features to added further in OPERATING SYSTEM.

**Objectives:-**

Datum or data must not be used by any person/ user without the permission of the owner of the data in any of the cases. Data of any user is private, confidential and valuable which can not be so private , confidential and valuable for other users. So data at any stage or of any kind must be treated as highly sensitive and valuable so they must be used by the owners themselves as well as any authorized user who does have access permission .To secure and protect data from unauthorized access at any stage of data navigation that includes many ways, habits, logic, application, concept unknown unexpected ways that are being summarized.

Mainly there are two types of objectives in order to secure data and protect them from unauthorized access. I want to conclude these

1. To develop a new feature which can save data
2. To optimize existing features to provide more security than ever.

## Introduction:--

Data Privacy is concerned to its importance, security, protection, safety, accessibility for owner, significance, purpose, authorities who can access, accessible for desired environment and users, possibility of being hacked and used unauthorisedly all these are the topics of long discussion and possible alternatives. Purpose of discussion is to discuss all aspects and areas where data can travel and can validate those with data control over those places, areas, paths etc. .

But on the way from data input to receive information, all possible ways are considered for data navigation so that we can understand the possible places where data can be protected and be secured at all stages of its navigation. Moreover OS(Operating System) is designed for the purpose of safe and secure operation.

## Hypothesis:-

Possibility is that the client system may be used by other users who may access data of those users who have already used this system and data were left in this system in unsecure mode. Data can be of any kind that must have belonged to any user, authority, individual, sensitive, high priority, less important, related to security of a person or nation, private , public or dedicated to an individual or organization or any data, intellectual property right data, copyright data, that has to be used while using any device with or without internet or any type of datum or data must be treated as **high sensitive** data. So in this context we continue communicating their navigation, an area where data can travel, transmit, transfer, store and retrieve, reason to do so is at least we should know that all the places where data are concerned at user side or admin side including three tier layers i.e front-end, backend and logic / business layer. We will discuss in a sequence to make our discussion more effective, informative, feasible and usable in smooth propagation. We need to consider all places, areas or possible hardware/software access that may access/retrieve data as we can consider that all available feature of the client system can be used by any user. So we can easily conclude our discussion of where security and protection are needed most to secure data from unauthorized access. Our assumptions, observations analysis and experiences may vary person to person but a few common scenarios that can be common among those people. However our hypothesis is based on our these assumptions, observations analysis and experiences. In continuation of our conversation on the final hypothesis is the central objective that has to be achieved for this purpose we verify all possible feasible steps which are being discussed and their appropriate solutions.

So let us consider data travel in interconnected components of client system at **offline** mode **where data can travel and be accessible at**

1. **User Side:**-- User of a system at client side can enter data to get information, this data can travel through input devices , CPU and at last processed data at Output. Possibility to leak data at any of these devices where breaches should not be applied in order to protect data.
2. **Local Data Base**:-- Local Database refers to storage of data in the system itself with the help of an application that you are using or by default application of the Operating system that a system has in offline mode. So it is required to check data travel path to ensure data security
3. **Internal Network**:-- Client may be connected with LAN (Local Area Network), PAN(Personal Area Network) or any interdependent connected devices which are responsible to transfer data from one place to another internally. are subject to check and to secure transfer of data through these devices.
4. **Admin /Other Desktop User**:-- Admin or other desktop can be created to use a system for various kind of users. However Admin can access all desktops that are created even after password protected. So it is needed that data should not be accessible by any desktop users or admin if it is private mode or opted for secure mode.
5. **Other Unauthorized Access**:-- Possibilities are to use a system that may distribute or share among a number of users. So such cases can be considered while securing data transfer. Any user is not authorized to use data without the wish of the owner in any of the cases. Written permission is required for a person to use data of any person.
6. **Unknown Resources**:--Any unknown resources may be created due to viruses or any unknown reasons which may steal data from the system and can be used or misused by any unknown resource or resources too.
7. **Unauthorized Access**:--We can discuss the most basic reasons behind unauthorized access and how unauthorized access can be prohibited to protect data in order to access, store, retain and retrieve data smoothly.A few reasons how unauthorized access can be made during and after the working stage of a system

- Weak, guessable, common, easy Password
- System availability for everyone
- External memory devices carrying viruses
- No anti virus software installed.
- No Hardware and Software firewall used
- Malfunction due to any internal or external sources.
- Hackers and Crackers developed software for offline client system

Above mentioned points are the main reasons to access data unauthorizedly. So considering these areas and their proper possible solution can save data from unauthorized use.

**Password** and user id , these two credentials are very important to understand before assigning values for these. **Password** must not be common , easy to guess and simple. How strong your credentials are depends on the hardy access of a system.

**System availability** for every\one without any safety used for data privacy security and its protection. Passwords that we discussed is a good option for data protection initially. Additionally biometric parameters can be set to secure system use for unauthorized access. Moreover use of a system can be mapped with biometric inputs which are better possible available options.

**External memory** devices carrying viruses are also reasons for unauthorized access due to which data may be used or misused without permission. Better way is to protect external devices with hardware and software firewalls and scan them properly to avoid use and misuse of data without permission. Keeping complete control on external devices can help data protection from unauthorized access as well.

No **anti virus software i**nstalled can be one of the reasons to access data from unauthorized sources. Viruses can affect system functionalities. Malfunctionality, dead locks, hanging or and appropriate working dysfunction may yield not related required results. However data can travel to an unknown, unspecified or not required path which may damage data and to retrieve data whenever it is required. So **Antiviruses** software installation is a better option to avail a good smooth running system.

In absence of **Hardware** and **Software firewall** installation , the system can not work properly and at the same time output can not as per expectations or required tasks can not be obtained at any stage of processing. Firewalls can be either hardware or software. Both firewalls including hardware and software are required to install in order to get required, desired and expected result after all processing at all stages.In absence of firewalls data can not be traced before and after the processing that can be a data security cause.

**Malfunction** due to any **internal** or **external** sources of a computer system is a major cause to protect data from unauthorized access as data can not be fetched at any stage of processing. This reason is a major reason not only for data , its processing and retrieval but also its real processed output reliability. Data security can be dependent on the proper working functionality of a system.

**Hackers** and **Crackers** developed software for **offline** client system is an again reason for data security .Since Hackers and Crackers can not reach offline mode system directly but they can develop a software attached with any system accessories and when these accessories are used with the system their software can be activated and steal vital, essential information be stolen, then whenever system is connected through internet software can start working in one side at other side whenever such devices are used with other system can transfer stolen data from first computer to others. So check , scan and test with possibly one testing with extra available system properly then try to use your own system. Another way to test external deceived before using with the main system is to use hardware firewall that can test the external device to ready to use. Data can be protected from losses or damages.

8. **No Records**:-- Any scenario that can reveal another scenario where no data found and no record for data storage or any access record. Such cases can be handled properly like unknown resources can not access data.
9. **Server Side i.e client system can be used as a server**:--Anytime a system can be used as a server and other clients can be connected to work together. In this case data transfer becomes more sensitive. matter to handle safe navigation of data to and fro client and server.
10. **Local host**:--Apart from local memory locations , a local host i.e a browser can access data from input devices and store it into memory through a web page controlled by the browser .Browsing history can hold data of any type during its navigation.
11. **Cache Memory**:-- In Virtual machines a few data can be accumulated which has no connection with the data required for access , can be removed to protect data fro unauthorized use.A few unused data can be stored on the way of main data transfer can be considered to secure data and to use system functionality at smooth way
12. **RAM(Random Access Memory)**:-- Random Access Memory has access to keep data for further processing. As we know that memory can be used for basically three purposes. i. To Access Data ii. To Retrieve Data, iii. To Store Data. Therefore RAM has memory storage capacity to pass data to the next processing level unit. When data is required to process then RAM can hold data to access them and after work completion stage , RAM holds some data that is volatile and can be removed after refresh, restart or shut down. So be careful to remove data from RAM when after completion of work with the system or any of the applications.
13. **Shared System, Files, Folders, Applications**:-- Within a client system environment, users can use a feature of the Operating System of the client , any available application one by one or simultaneously.
14. **Internal Memory Hard disk**:-- Hard Disk has capability to store data safely and to provide them whenever they are to be retrieved. A feature at secure mode storage can be developed. Hard Disk Memory Management, Memory Management,

File and Disk Management , these types of management are the main functions of the Operating System of the Client System. Data through the algorithm of such management systems of the Operating System can travel in which mode and how this can be used during their transmission.

15. **External Memory Pen drive, DVD, CD, etc:-**External memory is permanent , non volatile, auxiliary , secondary memory where data can be saved, retained and retrieved whenever required. -External Memory devices port available for external memory devices to connect and to store data for portable use. Many various devices like pen drive, DVD, CD etc are normally used to store, retail and retrieve data for a long term. Whenever data is required these devices can be connected with the system and started working.Types of External memory would be

- SDD [Solid State Drives]
- Flash Drives
- NAS [Network Attached Storage]
- SAN [Storage Area Network]
- Cloud Storage(online mode)
- Magnetic Tapes
- Magnetic Disk
- Hard-Disk
- Floppy Disk
- Zip Drives
- Optical Disk
- Pen Drives

These memory devices are slower than internal memory and data saved on these memory can be deleted even after shutting down the system. So my concern is to consider all these data navigation paths and data breaches during the navigation of data.And data can be protected for safe navigation and retrieval.

16. **Virus (Vital Information Resource Under Siege)**:-- Malfunction, deadlocks, hang, not expected output, corrupt files folders, applications, delete file folders applications, spread from one program to another , interruptions, insertion of new thighs in a program are a few functions may happen in the system. May we understand the level of malfunctionality of the system and in such a scenario how can we expect data to secure. So Antivirus is a better option to protect our system from all these mentioned scenarios then up to some extent we can expect data security and protection.
17. **Installed Software**:--Our devices like desktop, laptop, palmtop, Ipad, mobile phones which have an IPO(Input Process Output) cycle must have input devices, processing unit and output devices inter connected to perform collectively and ready to produce required output as a result. In the context of interconnected devices or any other device or devices that are connected at hardware side or any software that is installed which is unknown to us about its functionality, purpose and dependency. may damage data used in these system. So be aware and get much required information about such installed hardware and software if we want to secure our data for any unauthorized access. In case such hardware and software which are not interdependent and not required for our system then they must be **uninstalled** and **deleted** as soon as possible.
18. **Attached Hardware:**--We discussed this topic in previous topic in detail. So unwanted, unnecessary, nor required, not dependent hardware must be detached at earliest.
19. **Hidden file, folder, icon, path**:--Some time users hide files, folders, applications etc..for security reasons. Any hidden application can steal our data without our knowledge and use or misuse our data. So make sure that no such applications are hidden before using the system.
20. **Auto fill**:--This feature of the browser retains data regarding corresponding textbox and fills automatically if this is used. Even password , user , phone number, date of birth etc. that is confidential, private and highly sensitive data. This data can be used or misused by other users. This feature should be off before using the system.
21. **Save credentials in local host**:-- Remember me, save password and store confidential data in the system causes data share, use. Avoid using the data save option.
22. **OS file management, memory management to save data automatically at client side offline mode too**:-- At one side we advocate that data can not be saved in the system using a related application and on the other side if data is not saved automatically then data could be lost. Therefore OS should have a feature like data can be saved but not used by any unauthorized user.

**where data can be damaged, lost or destroyed at**

1. **Power cut , sudden shut down or battery loss**:--Unanticipatedly power cut , battery down or loss causes permanent data loss. Better is to save data partially rather than save whole data at once or at last. Like google sheet has an option to save data automatically while using this sheet online. Similarly data must be saved automatically in offline mode too.
2. **Outer sources like accidents or damaged hardware**:-- Hardware damage means software damage. In such types of cases nothing can be done. However an alternative can be considered like before accidents , data whatever saved can be retrieved in a very hard device like black box in the airplane.
3. **Natural disasters flood, earthquake**:--In offline mode data can not be saved in case hardware is damaged completely. In the previous point a very hard material made device should be used to save data like black box in the airplane.
4. **Stolen system**:--Stolen system means, stolen data which can not be used by other users as a safety pattern must be developed and used.
5. **Not saved data**:-- Data should be saved automatically in offline mode too.
6. **Human error**:-- Human error is always there, and with this error a new technology is always invented and discovered.To avoid human error , a few suggestions are suggested and implemented in most of the cases.
7. **System Bugs**:--Human error is natural and system bugs are the consequences of human errors. Avoiding this is not so easy but reduction can be done.
8. **Hardware dysfunction**:--Hardware dysfunction means software dysfunction. Data security is concerned with the proper functionality of a system.
9. **System upgradation**:--Sometimes it happens when a system is upgraded then existing data is lost. Do not believe in a system or software that could save existing data , keep record or save existing data prior to upgrading the system.

**Explanation:-**

We will discuss those areas where data can travel and all possible solutions for data security and its protection with possible live examples one by one.

Let us make our discussion simpler, any device that can be either with or without internet connection further we can say online or offline mode respectively.

Let us start with offline mode that simply means internet connection is not availed for the said device, system, laptop, desktop, server etc. However offline mode system can take data from input devices and send to Memory and Processors to get data processed and to retrieve data as an information. Users system can be used by another user and data may be accessed by another user too. So We will find the possible ways to secure and protect data and conclude them in our discussion.

Above analyzed point under hypothesis title where data is being used in any form offline mode will be discussed sequentially in more details possibly with live examples.

## Conclusion:(Privacy, Security and Protection):--

1. Autosave at offline mode
2. A new copy should be saved to local disk or external memory device automatically and can be accessed by owner only
3. In case of system malfunction , the system should have an alert messaging system before starting processing of data.
4. Particular user desktop accounts should map with user credentials or biometric input.
5. Credentials must be accessible with the owner only.
6. A user desktop should not be shareable to anyone including admin.
7. In case any change in text or original data , accessible credentials must be required.
8. Data can be stored in encrypted form and where required to retrieve must be decrypted .
9. At the end of the work all features which keep data with them, like autofill, suggestions, must be disabled by refreshing, disabling or clear cache, browsing data..ext.
10. If any related file, folder, application , feature, are opened by mistake , should not be visible or accessible to any other user other than owner, should be invisible for other users.
11. A feature must be **developed** while working with any application at client, if anyone wants to see the application working and data that are used in it should not be visible to him or her until the feature allows for it This feature can be accessible by the owner only at the time of using that application.
12. Disable External memory port for another users
13. Enable database encryption for your current application software with which you are working for your file, images, animation, text, multimedia, audio and video. Encryption feature ensures data is saved in encrypted form in the local database which can be decrypted further as per requirement.
14. Do not connect local equipment with your PC until it is required .However after work completion disconnect local devices and make sure access for your local devices are in your control otherwise delete data if shared, saved with local devices permanently.
15. An alternative hardware device can be considered like BLACK BOX IN AIRPLANE where data can be saved, retained and retrieved easily.Data whatever is saved in such a hard device that can be retrieved easily even after any accident, natural hazard.
16. Data saving algorithms must be built in offline mode too ,to save data consistently.
17. Hardware devices are interconnected and in case of non functionality of any single device should not affect other connected devices so data stored or traveled through such damages or faulty device can be detected and to replace it with new one.

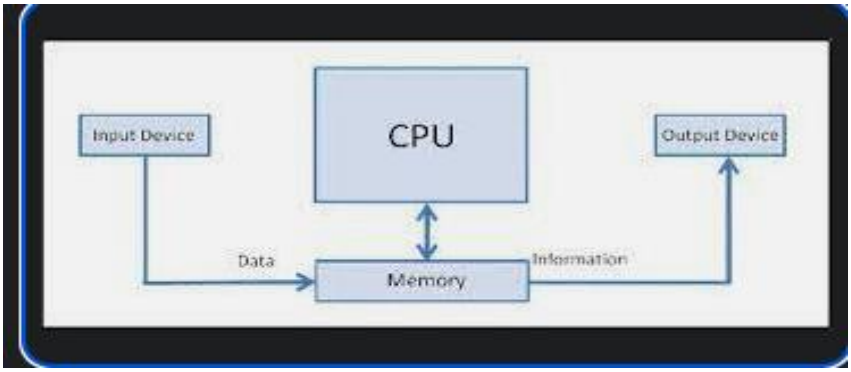
## New Concepts:-

New data saving , storing, retrieving , transferring and manipulating concepts can be developed as the concept is new for the client system offline mode.

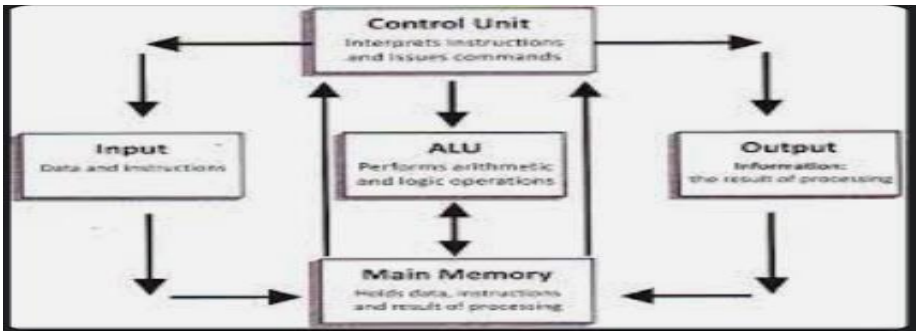
1. Offline mode should have a feature to save data automatically.
2. Intervened users or unauthorized users can be prohibited to access the said data by developing a feature to ask for text or biometric authenticity. Example: a user is using client system and accessing an application in between another person wants to use the system without the wish of the first user , a proposed feature should be active and can ask a new user to enter related text or permission with biometric inputs. Simply an authorized access can not produce required credentials and system can be secured from authorized access
3. Secure mode a new feature can be developed that can disallow the user to use the system for new users without permission.
4. A new private desktop which has a feature to activate all related applications that the owner wants to use and disable for new users without permission.

**Diagram:-**

1. **IPO (Input Process Output)** cycle that plays an important role in a computer system and indicates the ways where data can travel primarily. Raw material for a computer system is data , figure and facts which are further processed in CPU (Central Processing Unit) to yield processed data that is called information that are retrieved as an output

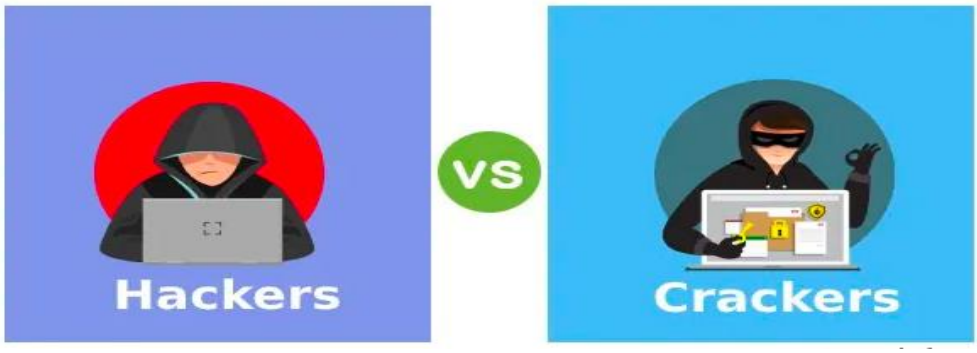



2. Computer system model has simple data input , processing and processed data i.e.information as an output for our considerations of the path of data traveling.




3. Data Breaches: Data breaches can be maintained by providing various validations at the stages of data navigation.


4. Hackers and Crackers:-- Hackers never damage or harm any kind of data.They Steal data for good purposes and there is no financial loss. Crackers steal data and cause a huge financial loss.




5. Data Privacy, Security and protection. Data protection means internal data validations.


**References:-**

1. Images from google search
2. Based on knowledge gained from different books , discussion, training, workshop, seminars, self analysis, observations, search engines,

**Disclosure statement:--**

**Perceptions, opinions, suggestions, thoughts, concepts and hypotheses may vary person to person. No conflict of interest was declared by the author.**