Private cloud technology

Development of cloud technology and cyber security

Who we are

We are a startup that has created an innovative cloud storage platform and tools for the 4.0 digital transition, as well as encrypted private communication systems for data and messages. The Cloud is an IT security company, which aims to create trustless solutions, this kind of applications make the user safe because it must not confidence in any intermediary: his data and his privacy for third parties, this is The same concept that gave birth to Bitcoin technology, and that allows you to act without intermediaries. If you operate with GDrrive, Dropbox, OneDrive, essentially you have to trust companies that have already been involved in the datagate, and have had legal consequence about the violation of privacy rules, in a trustless system, on the other hand, there is no subject to whom You have to trust because it manages your data and your communication.

What we accomplished

Following Snowden's revelations which with clear evidence (they won a Pulitzer with the datagate investigation), it became known that the data of European citizens and companies stored in the Cloud of the world's largest companies are all spied on and duplicated by NSA to do industrial espionage and intelligence.
Our aim is to make individuals and companies truly in possession of their data in the cloud, we have therefore created a private cloud storage platform focused on IT security with all the services necessary for telemetry collection, connection to 5G services, and digital security useful for the digital transition 4.0.
It has been demonstrated how mass espionage could seriously endanger journalists, the freedom of thought of citizens and therefore also democracy, it has therefore become indispensable, also in compliance with the European GDPR, to offer useful tools for the protection of personal data.

Summary of the main projects completed

Cloud Client desktop

Features

1. Real-time synchronization of folders with the remote Cloud
2. Daily backup (the PC requires an additional HD to prevent disk failure from also causing the loss of the backup)
3. Backup for versioning (occurs automatically when a file is modified, the backup is created on the additional HD)
4. Creation of digital identity, digital signature of PDF documents and signature validation.

The Cloud

5. Mirroring on a network path. The Cloud path can be maintained in real-time copy on a network path in a similar way to a RAID 1 system, with the difference that mirroring, being on the network, protects the company against data loss due to computer theft.
6. Decentralized account: Saving and recovering the account via passphrase, with technology derived from Bitcoin wallets.
7. Encrypted stealth partition: To prevent access to the local cloud area via a password (we have developed a system of derived keys to protect against quantum computer attacks)
8. Use virtualized applications to work on files without leaving traces on your computer: Every time we use our computer to work on files, we leave traces: Temporary files, data on disk tracks, list of recent files that the editor has worked on, etc.. with this technology no trace is left

Private Cloud home consumer

Device for remote file synchronization, creates a system similar to OneDrive or DropBox but private, that is, the data is not in the hands of third-party companies, but stored on your device in which it is connected to the client with military-grade encryption via 2 possible protocols: Encrypted Socket, or our Rest API implementation to which a level of encryption has been added to the HTML request that is not present in the standard protocol.
You can connect to the Cloud via:

- Desktop application that synchronizes in real time
- Mobile application that consists of a file explorer that allows you to save and download files in the Cloud
- Static web page (file explorer for the browser, with “drag & drop” functions for managing files in the cloud).

Cloud enterprise

This is a stand-alone Cloud, with an operating system and installed on a dedicated server, with scalability functions dedicated to companies. In particular:

1. It is possible to create and mount on the fly from 0 to N Clouds (with the limit of the disk unit space).
2. Create on the fly area sub-Clouds, for example, if a company has different departments within it (marketing, research and development, commercial and sales), it is possible to create for each department a Cloud positioned in a branch of the main Cloud so that the members of the department are limited to a restricted area with respect to the main Cloud, while the company management has access via the connection to the main Cloud located at the root. The sub-Clouds in turn can have sub-Clouds to create restricted work areas.
3. Daily data backup function.
4. It is possible to parring two enterprise clouds located in different geographical locations (for example Europe and the USA): In this case the paired Clouds will have the same

data synchronized in real time: Useful function for disaster recovery in case the company where the cloud is stored is destroyed by a flood or fire that would physically destroy the server and all the backup copies within the company.

5. Data mirroring on a network path.

6. On-the-fly creation of disposable PINs to access the Cloud: The generated PIN allows the creation of a digital identity to connect to the Cloud, to which the network administrator assigns a name. The owner of the digital identity can export it to another machine via a passphrase (similarly to what happens with Bitcoin wallets, the underlying technology is the same).

7. Advanced self-diagnostics and problem-solving functions: The enterprise Cloud requires a system administrator for commissioning, maintenance and assistance: Since the infrastructure can have different configuration models, the Cloud already has all the self-diagnostic tests inside it to identify all types of problems that could arise due to the configuration of the infrastructure.

Encrypted proxy

It is a proprietary implementation of a proxy system that supports a level of encryption for which the proxy does not become trustless: Unlike a traditional proxy or VPN, the data transits natively encrypted and continues encrypted to the cloud without the machine on which the proxy is installed being able to see the transmission in clear. In a traditional VPN, the data is encrypted up to the machine that acts as a VPN and from there on it still travels in clear.
The idea is to keep the entire Cloud infrastructure within a company intranet, without it being directly exposed to the outside (to the Internet), and expose only the proxy which thus acts as a secure machine as a trustless gateway for data traffic coming from abroad and therefore allows the connection of clients to the infrastructure with a high level of security.

Messaging Router

The messaging router is a logical machine that allows you to manage data traffic in a trustless manner (all traffic is encrypted from source to destination and the router has no way of seeing the traffic passing through in clear text). The router also allows you to route messages to logical groups of machines, devices on a precarious mobile network, and to devices with dynamic IP. It was created to manage communications for applications equivalent to Telegram, or Signal. A single machine can manage hundreds of thousands of client devices and the traffic they generate. The ability to also manage binary-level packets (in addition to audio, text, images) has made it the cornerstone tool for connecting clients and servers and routing the traffic generated in any condition.
The Router can work in symbiosis with the encrypted Proxy since the latter is a client device for the router.

At a logical level, it is possible to customize any infrastructure by placing more than one router and proxy inside based on the infrastructure needs. The Cloud enterprise solution in the same machine combines Cloud server, Router and Proxy in order to have a ready-made solution, but ad hoc solutions are possible to adapt to different projects and customized corporate security policies.

Telemetry data acquisition

We have created low-level libraries that can be integrated on small low-cost ARM devices (~20€), to connect the Internet of Things to the router or to acquire the flow of telemetry data from industrial equipment.
The telemetry data is encrypted and routed in real time to any type of device or logical group, such as to the Cloud, to mobile devices, to other devices, even with precarious connection conditions, or dynamic IP, and even through different types of connection (TCP, radio, GSM, RS232, etc.), an internal spooler will take care of getting the data to its destination regardless of the quality of the network and presence of connection at the time of acquisition.
The security level adopted, as regards the privacy of communication, is military-grade.

Glossary

Even if the cloud is very simple in its use, technically it is very advanced and makes use of concepts and technologies that need particular attention, in order to fully understand the innovative aspects of the project we have prepared a dictionary of technical terms that explains in a simple way (not for experts) the technology underlying the project.
Since what the end user sees is only the tip of the iceberg, to have a complete vision of the project it is important in this phase to describe the underlying, because the innovative technologies adopted make this a highly technological and innovative project.

- **Trustless**
  The trustless system was born with the creation of bitcoin and indicates a system that works without my having to trust anyone, for example, if I deposit money in a bank, it is because I trust that bank, this implies that the bank may fail and never give me my money back. A trustless system does not require my trust in a bank or a subject, it is managed by an inviolable algorithm which is made public to prove the validity of the technology used. An algorithm cannot be corrupted and behaves in the same way regardless of who uses and interfaces with it.
  If I open an account on a web service, the service wants my name, surname, email and telephone number to manage my account. This data kept in the backend, if violated by a hacker, would allow anyone to enter my account, this is because the system is based on the trust placed in the person who keeps my account in the backend. In a trustless system the account is kept in the front end, i.e. I keep it and there is no person who keeps my credentials or acts as an intermediary, in practice there is no one I should trust, that's why this type of technology is the safest. In a trustless system My account is created on the client side and is a pair of cryptographic keys (public and private key), and I keep the private key and it is this that allows me to

authenticate my operations by means of the digital signature then to be safely reflected in the open source system.

- **Zero Trusts**
  Zero Trust is a strategic cybersecurity model designed to protect the digital environment of the modern enterprise, which increasingly includes public and private clouds, SaaS applications, DevOps, robotic process automation (RPA) and much more. Zero Trust is based on the belief that nothing, both inside and outside an organization's network perimeter, should automatically be trusted. Zero Trust models require that anyone and anything trying to connect to an organization's system must be verified before they can access. The main objective of the Zero Trust approach is to mitigate the risk of cyber-attacks in modern environments that are the theater of activity of most organizations.
  Trustless systems are also automatically zero trust, so we can say that trustless is a subset of zero trust that represents a generational evolution in the field of information security. Trustless systems have all the characteristics of zero trust systems with the addition of not having to depend on the human and discretionary factor as these are managed entirely by algorithms.

- **Private cloud**
  The private cloud is the company's internal cloud, this means that your data is not kept by third parties and other companies. Since this type of cloud does not expose data and third parties, it is safer for what concerns industrial espionage and corporate profiling through data processing. The private cloud is conceptually opposed to the public cloud, the data stored on public clouds can be used for the processing of big data or sold to third parties by malicious subjects.

- **Non-custodial wallets**
  Non-custodial, or self-custody, wallets are cryptocurrency wallets that enable you to hold and send assets without the need for a centralized intermediary like a bank. They are used to securely store crypto assets and interact with decentralized finance protocols and decentralized applications.
  These wallets use a private key and public key pair to store assets and help users conduct transactions.
  A private key is like your internet banking ID and password that proves that you own a wallet and the digital assets associated with it. A public key, on the other hand, is generated using the private key and is like your bank account details that you share with others to receive cryptocurrencies from other wallet holders.
  Another concept closely related to the private key is the seed phrase or mnemonic phrase: a 12, 18, or 24-word pattern your wallet generates when it’s first set up.
  Unlike a private key that allows you to access only one wallet address, the mnemonic phrase gives you access to the crypto assets stored in all the accounts within a crypto wallet.
  Having the seed phrase means gaining or recovering access to your digital assets even if you lose your hardware or software wallet.
  So, it goes without saying that you should keep your seed phrase safe, as anyone who knows your seed phrase can import a copy of your wallet and steal your funds.

- **Self-custody**
  Self-custody refers to having total control of your private keys and, consequently, the crypto assets associated with them. When you have self-custody over your assets, no centralized third-party or financial institution can censor transactions and confiscate your assets.
  Another advantage of self-custody is not having to wait for withdrawal approvals, resulting in faster transaction times.

- **Decentralization**
  The peculiarity of decentralization is the lack of censorship, and of subjects who can intervene by changing the rules. A decentralized system works on the basis of algorithms that can be smart contracts or software that runs without depending on a machine on which you can intervene to modify its execution. Decentralized processes are by their nature incorruptible, as there are no subjects who can modify the functioning envisaged by the algorithms. The first example of decentralized software was bitcoin, a virtual currency that works without having a credit institution or bankers behind it who can make centralized decisions. Bitcoin has been an inspiration to many cryptographic projects that aim at independence from third parties for the management of personal or community aspects. A decentralized algorithm is by its nature incorruptible as it cannot be influenced by anyone's decisions but will continue to function as programmed.

How the project was born

Satoshi Nakamoto in November 2008 published the bitcoin protocol, this gave rise to the concept of decentralization in a real application, i.e. an application that worked autonomously, regardless of the will of a subject, even independently of the will of the author himself, i.e. combining cryptography with an ingenious computer algorithm ushered in the era of decentralized applications. Now we do not know if Satoshi Nakamoto really existed or is instead a pseudonym created by a team of mathematicians and developers, however this project seemed compelling to many for what the ethics of wanting to decentralize aspects of daily life, such as payments and of financial transactions, because decentralization is a very powerful weapon against corruption and the arrogance of monopolistic subjects.
In the past, the team that is developing the cloud worked on the development of bitcoin technology, in particular on the creation of non-custodian wallets, and it immediately seemed clear that this type of technology could also be combined in other areas for which it is required the same level of security and privacy. The idea of creating a private cloud based on bitcoin technology was born from the curiosity to experiment with bitcoin technology in other areas where the same level of security and independence from third parties is required, as occurs in decentralized platforms.
The team that initially developed wallets for decentralized digital asset custody began to divide these projects into libraries and then use these libraries by managing them in other ways to create encrypted messaging apps with military-grade security. In a second step, it was then decided to further evolve the project using the messaging app engine with military-

grade security, to send data from point to point, in a protected, secure and confidential manner, and in this step the Cloud, i.e. a storage that as underlying derives from bitcoin technology, as regards cryptographic concepts, privacy, account management and digital identity, however it does not include the blockchain as for this project a public ledger is not it is of no use.
Observing the data on the growth of the cloud market provided by Deloitte and Accenture, which highlight how this tool is increasingly interesting for both companies and private individuals, and also assert how currently the major competitors in the sector are all conceptually at the antipode of the concept of decentralization and being centralizers themselves, we felt the need to create a private cloud that could represent a useful and necessary tool for those who care about their privacy.

Presentation of the project

What follows is an exciting project for those in the sector, who will not fail to fascinate IT and security experts because the authors are representatives of the cypherpunk world, all visionaries who love privacy, freedom from banking systems, lobbies , lovers of decentralization governed by incorruptible algorithms and against the centralization of power that aim to monitor and profile the masses with anti-ethical intent.
Our project is already at an advanced stage, everything described here has already been done, it is a work that has employed a development team of 6 for 3 years, they are experts in computer security, digital asset custody, cryptography .
Our initial idea was to create modular components (the technical term is library), for the development of any type of cloud technology, these are basic functions, which are pieces of a puzzle, which can be composed in different ways , in order to create different cloud solutions with different purposes and technologies, ranging from data synchronization (cloud storage), to messaging apps, both for individuals, companies and data centers.
Essentially, cloud technology is divided into two parts, client and server: the server part is the part that runs the remote infrastructure and represents the cloud proper, and the client, which is the user-side part that manages how the user relates with the cloud and interact with it. The client part can have a user interface that allows you to interact with the cloud, the server part can have a user interface for the data center system administrator, in our project the user interfaces are separate from the software, they are an autonomous program that applies to the underlying library, and they can also be replaced with different interfaces that work with different technologies and languages, and on any type of operating system or embedded machine.
Another very innovative and ingenious aspect is that essentially the underlying libraries are multipurpose and symmetrical, that is, the client and server side libraries are the same, both for the management of communication channels and data transport, and for the synchronization protocols some data. Generally this type of application is created by creating distinct and non-interchangeable client and server software, instead with our solution we have an underlying that is essentially identical for the server and the client giving rise to a large number of applications and scalability including solutions that simultaneously I am both client and server in cloud infrastructure.
These are libraries whose functionality is easily scalable, designed to be instantiated and mounted on the fly, the protocols are built with a low-level command language that can be updated and integrated with new commands that enhance their functionality, and all works at

a low level in order to obtain maximum performance, that is, communications take place at the bit and byte level, and the protocols work on a single byte so as not to add anything more than the minimum necessary information, which instead does not happen with standard protocols based on json or xml in which the data is encapsulated in special tags that add bytes to the packets sent, increasing their size and influencing their performance.
One of the most interesting aspects of the project is the fact that our team has started developing everything focused on the creation of a messaging app that uses all the bitcoin wallet concepts as underlying, to which we have also added wallet functions, this because the technology in the non-custodian wallet sector, combined with the possibility of inspecting the sources, is considered a very advanced concept in terms of IT security, and we have developed a modular cloud from this technology that we have developed as the underlying pieces of a puzzle and which covers all the cases regarding the storage and transmission of data.

Some realized software projects:

- **Secure Storage**

  The necessity and desire to secure personal information is one thing that everyone shares around the world in the recent times, ranging from businesses to governments to military structures. Data security is critical whether it is being stored, sent, or delivered. Data breaches, hacking, and lost or stolen devices can have catastrophic financial and reputational costs. The need for a Library to protect data generated and handled by applications arose from a desire to protect not only public structures, but also individual citizens, who are even more at risk if their freedom of expression, gender, religion, and any data relating to their person and loved ones is not protected.

  Any application that does not secure the data it generates and manages carries the risk of revealing sensitive information that can be used to profile users, scammers to invent scams, and hackers to carry out their plans to pirated programs. The information created by the applications can easily be gathered and marketed on the dark web.

  SecureStorage is a library that provides effective encryption to the apps that use it, making the data generated by it inaccessible and inviolable.

  Any application creates a large quantity of data; some of it serves just as a warning, while others are essential to the application's operation and users, and some of it, if interfered with, can allow the application and its content to be hacked.

  To protect yourself from malicious hackers and organizational data breaches, encrypt all data generated by the application and prevent it from being saved in a way that may be read externally. In the case that unwanted access is permitted to a computer network or storage device, other apps on the same device, or system applications designed with fraudulent purpose by the device's maker, encryption provides an extra level of protection. The hacker will be unable to access the application data encrypted through SecureStorage.

What is encryption?

Simply said, encryption transforms data entered into a digital device into gibberish-like pieces. The encrypted data becomes more unreadable and indecipherable as the encryption technique becomes more complex. Decryption, on the other hand, restores the encrypted data to its original state, making it readable again. Unencrypted data is referred to as normal data, and encrypted data is referred to as encrypted data.

Software vs Hardware encryption

Software encryption encrypts data on a logical disk using a number of software packages. A unique key is created and saved in the computer's memory when a drive is encrypted for the first time. A user passcode is used to encrypt the key. When a user enters the passcode, the key is unlocked, allowing access to the drive's unencrypted data. The drive also stores a copy of the key. When data is written to the drive, it is encrypted using the key before it is physically committed to the disk; software encryption works as an intermediate between application read / write data on the device. Before being given to the software, data read from the drive is decrypted using the same key.

Hardware - level encryption is possible on some devices: Hardware - based encryption is used in Self - Encrypting Drives(SEDs), which takes a more comprehensive approach to encrypting user data. SEDs include an AES encryption chip that encrypts data before it is written to NAND media and decrypts it before it is read. Between the operating system loaded on the drive and the system BIOS is where hardware encryption takes place. An encryption key is generated and stored on NAND flash memory when the drive is encrypted for the first time. A custom BIOS is loaded when the system is first booted, prompting for a user password. The contents of the drive are decrypted and access to the operating system and user data is provided once the pass is entered.

Self-encrypting drives also encrypt and decrypt data on the fly, with the built-in cryptographic chip encrypting and decrypting data before it is written to NAND flash memory. Because the encryption procedure does not use the host CPU, the performance penalty associated with software encryption is reduced. The encryption key is typically placed in the SSD's built-in memory at system startup, which complicates recovery and makes it less vulnerable to low-level attacks. This hardware-based encryption solution provides strong data security in the event that the device is lost, cannot be disabled, and has no performance impact. However, it is a type of low-level encryption that is completely transparent to the device that uses these storage units, as well as to all software programs that run on the device. As a result, this type of encryption does not protect the data of individual applications and users from other resident programs that can see all of the data stored in clear text.

SecureStorage provides an additional layer of security for individuals who utilize primary hardware encrypted devices, rendering the data unreadable outside of the single program that created and is using it.

The Advanced Encryption Standard (AES) is a cryptographic technique that is based on the Rijndael family of algorithms. It is now one of the most widely used encryption and decryption techniques. Vincent Rijmjen and Joan Daemen created the Rijndael algorithm, which is a block cipher. It's a symmetric-key algorithm, which means it encrypts and decrypts data with the same key. As a consequence of the NIST Advanced Encryption Standard competition, the Rijndael algorithm was chosen as an Advanced Encryption Standard and the successor to the Data Encryption Standard (DES). The competition was held in order to produce a new cryptographic standard as a replacement for the obsolete DES. Because to the modernization of computer technologies, the Data Encryption Standard's key length (56 bits) was insecure at the time. The Rijndael family of functions is represented by three algorithms in the AES standard. They have varying key lengths of 128, 192, and 256 bits, but they all use the same 128-bit block length. More variations of encryption algorithms, cyphers, and other cryptographic functions are included in the Rijndael family of hashing functions than in AES. The Advanced Encryption Standard was designed to work equally well in software and hardware implementations. With the deployment of the substitution–permutation network design, it was possible. This network design is similar to the Feistel network, which was utilized in DES, but it is faster to compute on both hardware and software, which was critical given DES's software implementation inefficiency.

Our cryptography is the same as that used in Bitcoin, which has been put to the test by hackers all around the world without ever being broken: Breaking this form of cryptography would give you access to coins stored in wallets, which no one has ever done before.

The Advanced Encryption Algorithm (AES256) is an AES algorithm with a key length of 256 bits.The computational difficulty of the decryption is affected by the length of the AES version. The key recovery for AES 256-encrypted data requires more computational power than the 128 and 192-bit variants. The biclique attack, for example, can decrypt AES128 with a computational complexity of 2126. The computational complexity of biclique attacks on AES 192 and AES 256 are 2189.9 and 2254.3, respectively.However, for every key length, real execution of the attacks on the AES-protected data is currently impractical. All of the AES attacks are hypothetical. Every known AES attack would take millions of years to complete, regardless of the algorithm's key length.

- **Encrypted Messaging**

  Encrypted communication library to create applications similar to Telegram or Signal but with greater attention to IT security and privacy

  This project uses the Communication Channel project as its underlying, which creates a shcket communication channel for transmitting and receiving encrypted data upstream from the library. Communication Channel underlies the encrypted messaging protocol, we have separated the two parts because the idea is to provide an universal communication protocol, which can work on any type of communication medium and

hardware. Communication Channel creates a tcp socket communication channel, but this underlying one can be replaced with an analogous communication channel working with GSM data networks (without using the internet), or with rs232, rs485 ports, or any other communication devices either digital and analog. Just change the underlying encrypted communication protocol and we can easily implement encrypted communication on any type of device and in any scenario. If necessary, we can create implementations of new communication channels on different hardware, on commission.

Encrypted Messaging is a data exchange library between any type of device, usable for both desktop, mobile and internet of things applications:

- Support of digital signature on packages, and security level in military standard.
- This library, in terms of functionality and type of use, currently has no analogues.

Examples of use:

- Encrypted communication to create applications similar to Telegram or Signal but with greater attention to computer security and privacy.
- Data transmission between device and cloud.
- Acquisition of telemetry data produced by equipment.
- Connecting the Internet of Things and wearable devices to the cloud.

The library works correctly under all kinds of circumstances and data lines, and is ready for production scenarios,

Our mission is to exacerbate the concept of security in messaging and create something conceptually new and innovative from a technical point of view. Top-level encrypted communication (there is no backend , there is no server-side contact list, there is no server but a simple router, the theory is that if the server does not exist then the server cannot be hacked, the communication is anonymous, the IDs are derived from a hash of the public keys, therefore in no case it is possible to trace who originates the messages, the encryption key is changed for each single message, and a system of digital signatures guarantees the origin of the messages and prevents attacks "men in the middle"). We use different concepts introduced with Bitcoin technology and the library itself: there are no accounts, the account is simply a pair of public and private keys, groups are also supported, the group ID is derived from a hash computed through the public keys of the members, since the hash process is irreversible, the level of anonymity is maximum). The publication of the source wants to demonstrate the genuineness of the concepts we have adopted! Thanks for your attention!

- **Communication Channel**

  Communication Channel underlies the encrypted messaging protocol, we have separated the two parts because the idea is to provide an universal communication protocol, which can work on any type of communication medium and hardware.

Communication Channel creates a tcp socket communication channel, but this underlying one can be replaced with an analogous communication channel working with GSM data networks (without using the internet), or with rs232, rs485 ports, or any other communication devices either digital and analog. Just change the underlying encrypted communication protocol and we can easily implement encrypted communication on any type of device and in any scenario. If necessary, we can create implementations of new communication channels on different hardware, on commission.

- **CloudBox**

  Multi-purpose multi-platform library to create both server and client cloud systems on the fly, this library allows you to virtualize a cloud system on the fly.
  This library has been created to provide all the functions of both client and server cloud storage, both for small embedded systems and for large infrastructures: The possibility of being able to mount cloud units on the fly (hot create and destroy) allows you to create powerful infrastructures cloud as well as simple cloud si minilali systems.
  The prerogative of this library is that it is a symmetric library for server and client, i.e. this library is valid for both server and client cloud functions, as the platform was designed to be symmetric, i.e., the same code allows to create instances of cloud client and cloud server, giving rise to great flexibility as, for example, machines that using this library can act as both clients and servers with little intervention on the part of the developer.
  CloudBox through the underlying CloudSync library implements a low-level data synchronization system between client and server which saves on transmitted data, as the packets are minimalistic, it is a purely binary protocol which does not add anything to the bare essentials for transmission and data synchronization, which does not happen, for example, for protocols that encapsulate data in json or xml structures.
  The underlying encrypted messaging libraries add to this library an extreme security based on symmetric key protocols deriving from bitcoin technology and from bitcoin derive all the concepts in terms of security and trustless: Both client and server machines, when instantiated, do not require any user account, therefore there is no place where user databases and authentication data are kept, the client and the server are instantiated with exactly the same system used for bitcoin wallets (and to do this we use the same technology), i.e. at when the instance is created, a passphrase is randomly generated which allows account recovery, and which acts as a generator for the cryptographic keys (public and private), the private cryptographic key will never leave the device while the public one is used by the client for be able to access the server with a PIN. In this type of technology, the private key as generated also represents a sort of inviolable digital identity, which also has a digital signature to authenticate documents and data packets, in fact, during the synchronization procedure, the data, in addition to being encrypted, sees the addition of the digital signature to ensure maximum certainty on the origin.
  This type of technology is known and appreciated by users of cryptocurrency cold wallets such as Ledger and Trezor, who are considered among the most secure IT solutions for storing digital coins: Since the violation of digital wallets represents a

great reward for hackers who succeeded, and therefore it is reasonable to believe that this is the best technology to secure the data.
In practice, the server generates a QR code that represents its public key which allows a client to establish a cryptographic connection with the server and communicate with it in a secure manner.
To ensure that the private key can never leave the device, we have developed a special library (SecureStorage), which uses the best possible technologies to prevent private data from being accessible, including the hardware components present in modern devices to save key-data pairs.
The communication protocols implemented by the cloud through this library are two, a binary socket that represents the best possible technology in terms of performance, and one derived from the Rest API technology, to which we have added an encryption level that would not be present in standard technologies which relies on https requests to secure data, a bad solution because it allows the machine receiving the https requests to see the data in clear text, risking the security of everything that passes through: Https protects the point-to-point traffic on the internet but not inside the machine that receives the data or sends them through, having added an encryption layer we are going to create a protected tunnel that is not simply from machine to machine, but from client application to server application and vice versa, none of everything in the middle can intercept in plain text what passes through.
The main functions provided by the library are:

- Instantiate cloud clients and servers on the fly.
- Establish connection between client and server using a software router as a hub.
- Provide real-time data on synchronization status, data transmission and network problems.
- Automatically manage synchronization by means of a specific underlying library.
- Administrative functions of instanced clouds (server and client).
- Create sub clouds for internal areas.
- Digital signature functions on documents using the private key that represents the digital ID of the instance.

Notes: This library, to work as a server, needs the CloudServer library which adds small aspects that are not necessary in the client for obvious reasons, such as for example the generation of thumbnails, the exposure of encrypted APIs and the management of a proxy to directly expose the machine to internet while using the API.

- **CloudSync**

The Cloud Sync library is a highly specialized and scalable library dedicated to synchronizing data between local and remote storage, where the local device is intended as the client cloud and the remote one is the cloud server. The library is multipurpose, i.e. it is the same for both client and server systems and its utility is to monitor local and remote files and synchronize changes in real time so as to always have a redundant copy of the data you are working on , on the cloud.
The synchronization library is placed at a higher level than the CommunicationChannel Library and the EncryptedMessaging, and uses the characteristics of the latter to be able to expand with a binary command language, minimalist in data transmission and which therefore allows optimal use of data via the Internet by optimizing the use of bandwidth. EncryptedMessaging also offers a level of encryption and digital identity based on Bitcoin technology, making the communication protocol secure, with a type of encryption transparent to the developer that integrates the commands in the Cloud Sync library. The CommunicationChannel instead works as the underlying at a lower level to manage the TCP socket connection via the internet, theoretically we can replace this library with one specialized in GPRS, or RS425 communication and with relative simplicity we can adapt the Cloud Sync library in scenarios where instead of the internet as a communication channel, we have instead a GSM line or a serial communication or a transmission via modem. Having therefore unpacked the cloud technology into multiple libraries, we can relatively easily adapt a cloud project and different scenarios for which different hardware and technical solutions will be implemented.
The Cloud Sync library is technically an underlying of the CloudBox library and adds to this an efficient and fast data synchronization protocol which takes place by means of a set of commands at the binary level which are transmitted between client and server, to check the synchronization status and proceed with updating the files if necessary.
Another task performed by the library is the management of three types of events: Events on the current state of synchronization, events on file transfer, input output events (i.e. events that are triggered upon receipt and sending of communication between client and server), events about file errors, and events that the antivirus system could trigger during the synchronization of presumed infected files. This series of events can launch code that is executed on a possible app with user interface, which uses the library, in order to show the user in real time what is happening during synchronization and inform him of any problems found and on the synchronization progress.
This library also deals with the management of credentials useful for user login (when connecting the client to the server), the management of roles, and provides a class with all the utilities for managing access pins and other things useful for synchronization .
Synchronization takes place through data analysis both on the client side (user) and on the server side (the cloud), and an algorithm optimized for the transmission of the least amount of data between machines, as soon as it is clear what the differences between client and server are, puts in scheduler all the operations to be performed for synchronization, which will be immediately performed, and resumed in the event of an error or drop in the communication line. In any case, if the client should not be online, the synchronization will start automatically as soon as the connection will allow to

calculate the differences between client and server and what needs to be updated.

- **Trustless cloud client**

  The project is centered with a military safety standard.

  Easy to use Cloud Client + Backup Drive (Bonus)!

  Cross-platform desktop cloud client, for compatible clouds (works in conjunction with cloud server to sync files).
  This project has dependencies with other libraries which you can find open source in the same account as separate projects as the underlying libraries are in common with other projects:
  Therefore, the projects not included can be added by searching for them on the github repository, some are also available as nughet packages (you can add them to the solution instead of the missing projects).
  If you don't have the Cloud Server, alternatively you can use this software with a network address as a remote repository (the path must be set in the "git" parameter under the backup settings), for example you can set a pen drive connected to your router (in this case, the samba network path of the pen drive must be entered in "git").

  Description

  To use this software you need to have the relevant Private Cloud and compatible Cloud service (otherwise where does the cloud connect?).
  This program is an open source desktop cloud client to automatically synchronize, encrypted and with military grade security, files from your PC to your private cloud or cloud service.
  The synchronization algorithms are very fast and the software with hundreds of thousands of files does not go into crisis as it happens with similar products.
  This is an open source product and is published here in exactly the same source format version as you find here: https://github.com/Andrea-Bruno/CloudClient without any additions or modifications.
  Respect for your privacy is total, and the military level of security protects you and your data from hackers who would like to sneak into the cloud to access your personal data and information.

  Safety:

  We have transmitted our experience in the development of "non custodial wallet" bitcoins to this application so the underlying uses the same concepts and the same libraries, which are the foundations of the trustless technology used for the blockchain (the maximum current concept in terms of security) . The application generates a passphrase which creates a pair of cryptographic keys (public and private), which represent your digital identity and you can also sign documents with it. This digital identity is used by the server to recognize you, it is the underlying for encrypted communication. Using the passphrase you can restore your account on the client side,

just like cryptocurrency wallets. Just like with bitcoin wallets, your account is client-side only, there is no website where you need to register or a place where your account is kept, which makes this application conceptually superior to all similar ones.

As a bonus we have added some extra features:

- Automatic virus detection (occurs at the same time as cloud file synchronization).
- Daily automatic backup: To take advantage of this function you need to have an additional physical HD since the backup done on the same disk is useless because it does not protect against physical disk failure. The backup uses hard link functions so it doesn't take up much space, new backups only take up the difference of what has changed since the previous backup was done.
- Versioning: A new backup is created every time a file is modified in order to keep its previous losses and allow rollback (very useful function for software developers).
- Synchronization of the cloud area on the pen drive or disk attached to the router: You can specify the network path of your device connected to the router's USB port and have a real-time synchronized copy of all your data so if your computer were stolen or should you lose it, you will still have a copy of all your data.
- Digital signature of documents, i.e. the software creates a digital identity with which you can sign documents and validate the signature affixed by others.

The software needs to run in administrator mode for the following reasons:

- Automatic date and time adjustment in your computer (if the date is wrong the files will be recorded with wrong dates and could be mistakenly mistaken as older than versions contained on the cloud).
- Create hard links for backups (this saves a lot of space during backups).

Privacy Policy

The application does not collect or send personal data, all communication is exclusively with your private cloud or cloud service.
Since the privacy policy is trustless (you don't have to trust us but it is the code that demonstrates honesty), the source code irrefutably demonstrates that our work is sincere and loyal and that your data is protected, and the communications between client and Cloud server are impossible to intercept because they are covered by military-grade encryption systems with digitally signed packets to prevent "man in the middle" attacks in a preventive manner. The versions that we publish on the store are the same (without any modifications) that you can find here in source format.

- **CloudServer**

  Scalable and cross-platform cloud server technology

  It is a library that allows one or more cloud systems to be instantiated on the fly, creating a scalable structure. Since this is a library, it has no graphical interface which must be developed by the developers based on the specifics of the required scenario. Having decoupled the client functions from the graphical interface, above this library it is possible to apply a graphical interface based on the technology that best suits the

specific purpose of the cloud solution to be created, for example it is possible to add a web interface to create a cloud kiosk mode, or a cloud managed by windows panels, or purely software clouds whose interface is on a remote mobile app, etc.
Essentially CloudServer is a superior layer to the CloudBox library which being both a cloud server and client library does not implement the specific features only for the server, i.e. CloudBox only has common functions between client and server, while everything that is purely specific to the server (the cloud itself), is added with a software layer thanks to the CloudServer library.
The Cloud Server library implements server-specific functions, is written to be universal, i.e. it can run on both Windows and Linux operating systems, and adds features such as file thumbnails, license management, on-the-fly instantiation of new cloud, access pin management functions, diagnostic functions, generation of various types of QR code to pass the public key to the client and allow it to connect, descriptive report on system status, API for communication with a second encrypted protocol of communication (in addition to that provided by the underlying socket-type system), which allows a client to communicate with it through an innovative revamping of the Rest API protocol, to which encryption and key exchange with asymmetric encryption has been added, yes it is a protocol for communication with our encrypted proxy technology (normally a server that receives json requests, even if these are https, would be able to clearly see everything that passes because https creates a tunnel only up to the machine with which you interact with the post and get methods, instead encrypting the data that transits, with our solution the proxi will only act as a pass through without having the possibility of knowing anything of what transits.
Why have we implemented a protocol that requires a proxy? In many scenarios, for security reasons, you may not want to expose the cloud machine to the Internet, and prefer that the use of the post and get methods with the APIs take place via a machine exposed outside the infrastructure that acts as a proxy by resending the encrypted commands that receives in socchet mode to the cloud within a company intranet, the concept is to increase security by not exposing the cloud directly to the internet. In any case, with our software, the communication with the APIs must go through a proxy, which must have a static IP, while for the cloud the static IP address is not necessary since it is he who establishes the connection first, in this way it is also possible to create cloud servers that can work without a static IP or in areas covered by a firewall and interact with it from the outside using our encrypted proxy technology.

- **Data Redundancy library**

  It is a library that allows you to synchronize files in real time on a local or remote device (data mirroring with the addition of intelligent merge functionality).
  Being a library, this is not a software component that can be used directly but must be included in a solution in order to add the functions that we will describe below:
  The idea is to keep a copy of a directory with all its structure on a remote network device, as a baskup unit and with some unique and interesting additional functions:
  In the context of working in cooperation with multiple users, especially in the context of software development, it happens that you want to work on the same files, but there is no software that allows you to do it automatically and create the merge of files in real time.

This library was initially created as a patch for what git doesn't do, which is the automatic merging of work between multiple users. Essentially this is a library designed to work in software development but it works with any kind of software that is able to work cooperatively with multiple users, (the merge is a function that in software platforms is always done manually because it would require a very complex algorithm to do it automatically because there are many factors to consider, we have created this algorithm!).
The concept is this: All users who wish to participate in a common and collective work must configure the same network GIT path in which the files on which they work in a shared manner will automatically be maintained and updated.
Operation is very simple as users will never have to work on files in the shared directory on the network (called GIT directory or network path), which acts as a real-time mirror of the shared files stored locally. In practice, each user continues to work locally on his own files (as he normally would) and when these are modified, AntyGitLIbrary will automatically update the remote mirror, and if necessary it will merge the document with the texts edited by multiple users. At the same time when a file in the network directory is updated, all users using the library-based application, if connected, receive in real time an update of the local file with the one just updated remotely, so that everyone works on the latest version of documents and files generated by applications. If a user is not logged in (the computer is turned off), he will still receive the update the first time. In practice, whenever someone locally adds a new document or a new photo or other, or modifies an existing document, a copy is sent to the remote GIT repository and then from there it is propagated to all users participating in the same group using the app based on the Data Redundancy library.
The User can also work from a laptop workstation from another place and when he will be in the office or where the git directory will be visible, the software will synchronize the data, in practice the documents are always synchronized working in the same workplace, or they will be synchronized when possible on the first occurrence, all this automatically, i.e. without any necessary action on the part of the user.
A very versatile and powerful function that has no equal is the code merge function, expressly designed for developers who use VisualStudio, but which can work in all contexts: The software monitors when a file is modified and if it has been modified by more sources, merges the parts added by all members who have worked on the same file, basically the files automatically get the additions and changes made by other users. One could believe that this function could be unwelcome during software development as a non-definitive code could make the software non-compilable to other users, but this is not the case as the merge is performed when the software is compileable, and not during writing the code. In practice, when text is added, it is synchronized with the file on the remote git directory, only when the compilation is successful, and therefore the changes will be propagated to all users only on the really working code (the additions that do not produce compileable code, will not be propagated).
However, if you think your code might interfere with that of other developers working on the same project, you can hide it from the compiler using a custom symbol and #IF USER1 statements, to hide the effects of your code from other users. still in progress and not definitive.
In some scenarios you may want to use a git directory in a remote infrastructure

(outside your intranet), in which case you can do it using a VPN.

- **Backup Library**

  The backup library is a cross-platform library that makes it easy to integrate powerful backup functions.
  The purpose of this library is to make available and automate two types of backup: the daily one and the versioning one which is activated automatically whenever a file is modified.
  The library doesn't perform a brutal backup as it would take up a lot of space but it performs an intelligent backup that is completely transparent to the end user, for which it seems to all intents and purposes a full backup copying all directories and contents.
  The intelligent backup works that first the software analyzes the entire structure composed of files and directories and compares it with that of the previous backup, and the new backup will copy only the modified files while for those that have not undergone changes a link will be created (in the file system) to the same file as the previous backup: This type of solution is full backups but in reality they take up little space due to the fact that only the differences actually create files in the backup structure, while for everything that has not changed there is a link to the data of an identical file that transparently looks like a file for all intents and purposes.

  - Symbolic link
    A symbolic link contains a text string that is automatically interpreted and followed by the operating system as a path to another file or directory. This other file or directory is called the "target". The symbolic link is a second file that exists independently of its target. If a symbolic link is deleted, its target remains unaffected. If a symbolic link points to a target, and sometime later that target is moved, renamed or deleted, the symbolic link is not automatically updated or deleted, but continues to exist and still points to the old target, now a non-existing location or file. Symbolic links pointing to moved or non-existing targets are sometimes called broken, orphaned, dead, or dangling.

- **CloudServerUISupport**

  It is a middleware between the graphical interface of the cloud administrative panel and the underlying cloud technology, this library gives full support for the realization of all the panels for cloud administrative use.

  It is a library that groups and manages all the underlying libraries to form an enterprise type Cloud platform, and creates an all user-friendly graphical interface utilities, basically it is an intermediary library, between those that form the cloud technology and the graphical interface, to make it easy for those who develop the front end to use cloud technology.
  In practice, although the graphical interface could directly use the underlying libraries, it was decided to create a very simple intermediary library that facilitates its use, normally this part of the code could be merged into the graphical interface but it was

decided to unbundle it so that if you were to create multiple graphical interfaces with different technologies (Blazor, Windows Forms, MAUI, Xamarin, Uno Platform, Flutnet, etc..), this would result in a reusable and identical part under the hood of each graphical interface.
The idea is to keep in the front end project with the graphic interface only the part purely useful for displaying the panels with which the user can interact, so as to have a truly minimalist and easy to understand project for the front end developer, and absolve it from managing the underlying functions that make up the complex cloud technology.
The underlying part of this library consists of these libraries:

- BackupLibrary
- CloudServer Library
- DaraReundancy Library
- MessengerStorage
- ProxyApiSupport
- RouterServer
- UISupportGeneric (is an artificial intelligence library for the automatic creation of the front end)

To see specifically what the underlying libraries do, look at their documentation.
In practice, new libraries can be added to this middleware library, in order to add new features to the cloud platform or software.

The middleware creates the functions for the creation and management of the following panels:

- Backup management panel.
- Machine boot management panel.
- Dashboard for cloud management and support.
- Panel for managing and monitoring the connection to the router.
- Panel for diagnostic functions and easy identification of problems.
- Panel for customization in the graphical interface.
- Panel for managing cloud instances on the fly and creating them

- License management panel
- Panel for the main settings
- Dashboard for cloud-based messaging software support
- Panel to couple two servers and thus have remote data redundancy
- Panel to instantiate and manage an API proxy
- Panel for managing local data redundancy within the infrastructure
- Pallello for viewing diagnostic reports
- Router management panel
- Panel for displaying system information
- Keyboard panel
- Utilities panel

Each panel can be easily enriched with features giving scalability to the project, and an artificial intelligence system transforms these parts of the library into panels that are truly part of the user interface.

- **CloudServerWebUI (project)**

  This application is a graphical interface based on web technology, therefore usable via browser. All technologies used, including the underlying libraries, have been designed to work on both Linux and Windows platforms
  The graphical interface derives its functions from the underlying middleware library (WebServerUISupport), which organizes all the cloud server subsystem to create an enterprise cloud environment that can be easily scaled (expanded) using the graphical interface at the service of the administrator of the cloud infrastructure.
  Graphical interface in web technology can be easily modified by front developers using html and css code.
  This user interface has been focused to administer completely stand alone server machines, i.e. that start in Kiosk mode and this interface exposes the only panels to which the administrator has the right to access, in order to give greater security to the system by not giving full access to the operating system and other functions outside the cloud.
  To adorn the web interface there is also an agile terminal that appears inside the browser, with which commands can be given from the keyboard: Everything that can be done through the panels of the graphical interface can also be done from the terminal with commands dedicated to cloud technology.
  The naiffe aspect of this panel is the technology we have developed to create them:

the graphical interface is completely automatically generated on the fly (no need for a front end developer!), via our artificial intelligence system which analyzes the assembly of the backend in real time, memory allocations, etc., decompiles it for the interested party and builds a structure useful for the automatic creation of the front end side graphical interface.

This is a short description of some panels showing the UI, it is a partial description not complete, which includes the main features:

1. Connections
   Monitor active connections with software router. The router acts as a clearing house between the clouds and the clients, and also provides connection to the proxy which acts as a gateway with the APIs. All encrypted communications are forwarded to the router and then redirected to the destination application or device.

2. Diagnostics
   Set of tests and utilities for diagnostics and troubleshooting

3. GUI
   Graphic settings of the interface with which the user interacts with the application

4. Instances
   Information panel on currently unsatisfied clouds and a function on this machine
   One machine can instantiate multiple clouds, or multiple clouds can be instantiated on different machines. The cloud cannot be reached directly by the client but the communication takes place through a router, this allows you not to expose the cloud to the internet in order to have more security (only one router port must be exposed to the internet, which can be even in a remote machine, and the Cloud does not need a static IP). If the client is started correctly, it will automatically remain connected to the router via the entry point specified in the settings. Since the communication between client and cloud is encrypted, the router cannot know the transmitted data.
   At the first start, each client generates key pairs for asymmetric cryptography, the QR code represents the access point and the public encryption key so that communication takes place confidentially from the beginning. Each data packet is encrypted and signed with the private key of those who generate it (client or cloud server).
   The cloud supports two client communication protocols, the native one based on tpc socket with cryptography, and a proprietary REST API protocol to which we have added several point-to-point encryption methods to increase its security compared to the standard protocol.
   The encrypted REST API protocol uses RSA encryption for the exchange of encryption keys, so it is necessary to use the QR code including the RSA code to connect to the Cloud through this type of client.

We have created a web client in javaScript based on our protocol that serves as an example for software producers who want to create their own compatible client. Instead, the client based on the encrypted tcp socket native protocol, is provided to developers in the form of an open source library.
Clients using the encrypted REST API protocol cannot connect directly to the cloud, but must connect via a proxy, which is connected to the cloud via the router, so that it is possible to communicate to the cloud by exposing only the proxy to the internet and leaving the Cloud in an isolated place in order to increase security and still make the Cloud reachable even in those cases where it does not have a static IP

5. Licenses
   Utility for creating OEM licenses
   The cloud to connect to the router needs a license.This tool allows you to create a license that will automatically be implemented in the router.
   The license is an encryption key that is used to digitally sign the cloud connection request to the router.

6. Main settings
   Cloud system setting information

7. Messenger
   Encrypted messaging software support
   The router used for the cloud can also function as a control unit for encrypted messaging devices (they use the same protocol as the cloud). It is therefore possible to create a completely internal corporate messaging circuit whose data is encrypted and visible only to the sender and recipient. The messaging device/software also allows documents to be sent for sharing or saving them in the cloud: The cloud, in the communication device, is a contact in the address book to which documents or messages can be sent.

8. Pairing
   Pairing allows you to pair 2 devices in remote geographical locations, one acts as master and the other acts as slave and keep the synchronized version of all data in real time.
   Pairing is the best methodology to secure data against the theft of hardware devices, seizure of machines or destruction due to accidental events such as floods, earthquakes, wars, destruction due to a meteorite fall on the place where the cloud is kept , etc..
   A company can secure the data by coupling two machines, at two offices located in different geographical locations, this technique is the only one that gives the maximum guarantee against the loss of data due to breakages or accidental events.

9. Proxy
   Panel related to the proxy for communication with the API, installed on this machine

Proxy is software that allows clients that support the encrypted REST API protocol to communicate with the clouds connected to it, without the clouds being directly exposed to the internet.
The proxy communicates with the clouds in encrypted tcp socket protocol, through the router, while the clients communicate with the proxy in an encrypted way through GET and POST methods, typical of REST API technology.
The addition of encryption to the REST API protocol is our invention to increase its security and privacy, in fact the proxy is not aware of the data it transmits and there is no system to capture this data, because you create a direct encryption tunnel between clients and cloud.
In the QR code generated by the Cloud there is the public encryption key, the client uses it to connect and to scrape a symmetric encryption key that will remain secret, and will serve to encrypt the communication.
The public cloud encryption key will never leave your machine, our encryption and communication protocols are open source and therefore can be inspected for a security check.
To connect to the cloud, clients must prove that they know the PIN: the PIN is never sent for security reasons, the server creates a cryptographic puzzle and if the client solves it then it will have proven that it knows the PIN without ever having transmitted it.
This proxy is more secure than a VPN, while the VPN creates an encrypted transmission up to it and then the communication continues in the clear, this proxy only acts as a pass of encrypted data from the source to the destination.
The only data that the proxy can see are the User Agent and the IP of the connected clients, this data is transmitted to the Cloud and recorded in the event log to keep track of the activity and access attempts.
To avoid brute force attacks, you can make a maximum of 3 login attempts every 5 seconds.
Each proxy (there can be more than one) has a cryptographic key pair, the cloud needs to know the public key in order to connect to it through the router. The cloud doesn't need to know the IP of the proxy to connect to it, the public key is enough, but it must be properly connected to the router. Instead the client needs to know the IP of the proxy in order to pass data through it. Proxies and routers can reside on the same machine. The location of the proxy is also indicated in the QR code generated by the client, so the client will configure itself automatically by scanning the code.

10. Redundancy
    Keep a redundant copy of the unit synchronized in real time

11. Report
    Program event reports, useful for diagnostics

12. Router
    Panel related to the router that manages the encrypted communication between the clouds and their respective clients

The cloud is not connected directly with the client, but through a dispatcher, this dispatcher is the router, which acts as a node for everyone (for all cloud instances, and clients). Communication is encrypted and the router must be publicly exposed to the internet for clients to connect.
The router can be started on the same machine that instantiates the clouds, or you can keep the clouds in machines protected by firewalls and not reachable from the internet, and connect the clouds to a router exposed to the internet (with public ip). The best performance is to have Cloud and Router on the same machine. The communication protocol of the router also allows the sending between the network of messages of various types, encrypted from point to point, and also group messages, containing text, audio and images, with a reading notification system. Privacy: The router does not save any type of data, has no database and does not use writing media, the communication is encrypted and the router is not aware of what is being transmitted.
Each machine connected to the router (client, server or proxy) has an ID that corresponds to the public encryption key. To increase the level of anonymity and privacy, the public key of the connected machines is never used in the communication protocol with the router, but an ID derived from the hash of the public keys, since the hash algorithm is not reversible, from this the identifiers represented by public keys cannot be obtained.
The communication protocol provides for the generation of a new symmetrical encryption key for each packet sent, and the digital signature of the packet using the private key of the asymmetric encryption. We have made the communication protocol public so that anyone can examine it and evaluate its safety

13. System info
    Information about your system and hardware

- **CloudUIWeb**

  (Minimalist web interface for single instance private cloud server, home consumer)

  It is a minimalistic program that launches a single instance of a cloud server using the powerful CloudServer underlying library and displays its operation via textual information.
  This software allows the creation of a private cloud, very simple to use, without administrative control tools with a simple panel with information on the status and use of the cloud, for diagnosing problems and knowing the status of the connection.
  This type of cloud server, being designed for home consumer customers, unlike the corporate one, does not require a static IP, however to function it requires a proxy and a router with static IPs that act as a bridge, and multiple IP-free "home consumer" clouds. The proxy and the router can also be on the same machine, in which case the fixed IP can be the same for both.
  The idea is to make the cloud that does not have a static IP that identifies it always reachable, via a proxy which is instead placed on a static IP that is always reachable, for communication with it via encrypted APIs, or via a software router with static IP using socket synchronization protocol.

The Cloud has its own cryptographic digital identity, made up of a pair of keys (public and private) which is used both as a unique identification ID and to encrypt the data that is transmitted, and in this way everything that passes through the proxy does not can be captured and seen in the clear.
The connection between the cloud and the proxy does not take place directly but via a router which acts as a hub for all the clouds, and then routes the communication towards the proxy, which is also identifiable via digital identity given by the pair of cryptographic keys. Therefore, in order for the cloud to connect to the proxy, the public key of the proxy (which acts as an ID) must be set in the application settings file, in this way the router will route the packets destined for the proxy to the correct machine.
In a network with heavy traffic it is also possible to connect several proxies to the router, with different cryptographic keys, so that each proxy has a different ID and then set the clouds with the public key of the proxy that you want to use in order to divide the traffic between all clouds on different proxies.
The graphical interface of the cloud shows the following salient data: A QR code that contains the location of the router and the cloud public key, this QR code allows socket-based clients to connect to the cloud and synchronize.
A second QR code that contains in addition to the data of the first one, also a public RSA cryptographic key, which is used to connect clients based on our encrypted rest API implementation. And finally an encrypted QR code which is our latest cryptographic connection implementation that allows both encrypted rest API clients and socket clients to connect by exchanging some packets which allow them to obtain the clear QR code without it passing through the data communication . This type of QR code is more compact than the others because the data in the QR are not complete but must be fished through the exchange of some packets, the more compact QR code allows easier scanning by the client device that wants to connect.
Other salient data visible from the graphical interface are: The status of the connection to the router, the status of synchronization and the number of files sent, the amount of bytes sent, transfers in progress both in upload and download, any errors, a list of clients that have access to the machine with some brief information about them.
Since this is a user interface that instantiates a cloud dedicated to the home consumer range, it is really very minimalistic, the concept on which we based ourselves is that of creating a machine that does what it has to do without any type of external intervention, clearly then starting from source to this graphical interface if the need arises, more information can be added, or allow an administrator to interact with it as for example occurs with the graphical interface of the enterprise and scalable version of the cloud.

- **ProxyAPISupport (Proxy API Support library)**
  It is a library to add proxy functions to a software for communication between cloud client and server via API.
  What is the proxy for?
  The proxy allows you to have an access point with a static IP that is always available to clients, and to be able to keep the servers (the clouds) in a private intranet without a static IP and without exposing them directly to the internet, basically the clients that use the proxy they do not communicate directly with the cloud. The proxy also allows users of cheap private clouds to be able to install the cloud on a network without a static IP, as the clients will still have access to the cloud via the proxy which will always

be available at a fixed and pre-established address.
What does the cloud identify the proxy: In the QR code that allows the client to connect, there are the public cryptographic keys and the position of the proxy, so a scan of the QR code is enough to let the client understand how to establish the connection.
The APIs are our exclusive and innovative implementation of the REST API protocol, to which we have added encryption to make them secure in the context of cyber security. The traditional standard APIs do not have a robust information security system, at most they are protected by an https protocol which only covers the passage of information from client to proxy, but then on the proxy machine the information is unencrypted, and can be captured by by personnel assigned to the machine or by malicious software installed. Our cryptographic implementation protects the transit of packets in a highly secure way from client to cloud storage, and only the cloud software is the only one that sees clearly everything that is transmitted to it at the level of data packets.
This library allows you to create a proxy that can be queried by a set of commands by means of POST and GET methods, typical of the REAT api protocol, with the addition of a native encryption layer on the packet, this innovative non-standard security implementation , is our addition that works like this: In the QR code that the client uses to connect, there is either a cryptographic public key or encrypted information on how to find the public key, using the asymmetric encryption public key, is exchanged between clients and servers a symmetric encryption key which will be used to secure the communication. The proxy retransmits everything it receives from the client to the router via a TCP socket communication channel and the router retransmits them to the cloud which is identified via a digital identity created with a pair of cryptographic keys (in our infrastructure, every machine, server, cloud , proxy, messaging device, generates a cryptographic key pair and a pass phrase using Bitcoin technology, this cryptographic key pair corresponds to a digital identity and is used to uniquely identify the device, to secure packets by signing digital, and to encrypt data).
The system bases its security on the trustless concept (the most modern concept in the field of information security), that is, even programmers or those who manage the network, who wanted to see the messages that pass between the client and the cloud, cannot do so as technically backdoors are not feasible.
The function of the proxy is essentially to resend the packets it receives to the client or server, and some diagnostic functions on the problems encountered which are notified to the client by means of 4xx or 5xx response errors which, based on the number, describe the problem encountered so that support personnel and developers can figure out what's wrong and how to fix it.
When the proxy is initialized, it has a pair of cryptographic keys (public and private), which also create a digital identity of the machine, and this digital identity allows the router to identify the proxy and communicate with it.
Through this library, the proxy also generates a textual description showing the connected clients, the number of packets sent and received, the machine ID, the public encryption key, the entry point of the router, the connection status, the 'host (the internet location of the proxy), and other useful information.

- **SecureStorage Library**

The necessity and desire to secure personal information is one thing that everyone shares around the world in the recent times, ranging from businesses to governments to military structures. Data security is critical whether it is being stored, sent, or delivered. Data breaches, hacking, and lost or stolen devices can have catastrophic financial and reputational costs. The need for a Library to protect data generated and handled by applications arose from a desire to protect not only public structures, but also individual citizens, who are even more at risk if their freedom of expression, gender, religion, and any data relating to their person and loved ones is not protected.

Any application that does not secure the data it generates and manages carries the risk of revealing sensitive information that can be used to profile users, scammers to invent scams, and hackers to carry out their plans to pirated programs. The information created by the applications can easily be gathered and marketed on the dark web.

SecureStorage is a library that provides effective encryption to the apps that use it, making the data generated by it inaccessible and inviolable.

Any application creates a large quantity of data; some of it serves just as a warning, while others are essential to the application's operation and users, and some of it, if interfered with, can allow the application and its content to be hacked.

To protect yourself from malicious hackers and organizational data breaches, encrypt all data generated by the application and prevent it from being saved in a way that may be read externally. In the case that unwanted access is permitted to a computer network or storage device, other apps on the same device, or system applications designed with fraudulent purpose by the device's maker, encryption provides an extra level of protection. The hacker will be unable to access the application data encrypted through SecureStorage.

What are the functions of the library: The library offers 2 types of functions, saving objects, and saving values. Objects are nothing more than instances of class, which can have different properties or sub-objects that by means of this library will be saved and frozen in encrypted form to then be able to be fished out again. This feature allows many applications to save the internal working status safely to be recovered after reboot. A practical example of using this library is using it to save contacts, items for sale, announcements, encryption keys, personal and sensitive data, and anything else that in computer science can be represented with a class and you want to make it secure and inaccessible. Internal saving takes place first by means of serialization of the objects, followed by the addition of encryption and then finally with the secure saving of the data on the internal archiving system.

The second type of saving allows you to save the value of text, numeric, bolean, and DateTime variables in an encrypted and permanent way. These variables to which a key is assigned can also be recalled after restarting the application.

Securing takes place via the encryption which can be strengthened by passing the hardware saving functions of keys and values, during the initialization of the library for use.

It often happens that several applications, although they work in a very secure way, can be violated by modifying the data they generate and manage, this is not possible if the developers use this library.

What is encryption?
Simply said, encryption transforms data entered into a digital device into gibberish-like pieces. The encrypted data becomes more unreadable and indecipherable as the encryption technique becomes more complex. Decryption, on the other hand, restores the encrypted data to its original state, making it readable again. Unencrypted data is referred to as normal data, and encrypted data is referred to as encrypted data.</para>
Software vs Hardware encryption
Software encryption encrypts data on a logical disk using a number of software packages. A unique key is created and saved in the computer's memory when a drive is encrypted for the first time. A user passcode is used to encrypt the key. When a user enters the passcode, the key is unlocked, allowing access to the drive's unencrypted data. The drive also stores a copy of the key. When data is written to the drive, it is encrypted using the key before it is physically committed to the disk; software encryption works as an intermediate between application read / write data on the device. Before being given to the software, data read from the drive is decrypted using the same key.

Hardware - level encryption is possible on some devices: Hardware - based encryption is used in Self - Encrypting Drives(SEDs), which takes a more comprehensive approach to encrypting user data. SEDs include an AES encryption chip that encrypts data before it is written to NAND media and decrypts it before it is read. Between the operating system loaded on the drive and the system BIOS is where hardware encryption takes place. An encryption key is generated and stored on NAND flash memory when the drive is encrypted for the first time. A custom BIOS is loaded when the system is first booted, prompting for a user password. The contents of the drive are decrypted and access to the operating system and user data is provided once the pass is entered.

Self-encrypting drives also encrypt and decrypt data on the fly, with the built-in cryptographic chip encrypting and decrypting data before it is written to NAND flash memory. Because the encryption procedure does not use the host CPU, the performance penalty associated with software encryption is reduced. The encryption key is typically placed in the SSD's built-in memory at system startup, which complicates recovery and makes it less vulnerable to low-level attacks. This hardware-based encryption solution provides strong data security in the event that the device is lost, cannot be disabled, and has no performance impact. However, it is a type of low-level encryption that is completely transparent to the device that uses these storage units, as well as to all software programs that run on the device. As a result, this type of

encryption does not protect the data of individual applications and users from other resident programs that can see all of the data stored in clear text.

SecureStorage provides an additional layer of security for individuals who utilize primary hardware encrypted devices, rendering the data unreadable outside of the single program that created and is using it.

The Advanced Encryption Standard (AES) is a cryptographic technique that is based on the Rijndael family of algorithms. It is now one of the most widely used encryption and decryption techniques. Vincent Rijmjen and Joan Daemen created the Rijndael algorithm, which is a block cipher. It's a symmetric-key algorithm, which means it encrypts and decrypts data with the same key. As a consequence of the NIST Advanced Encryption Standard competition, the Rijndael algorithm was chosen as an Advanced Encryption Standard and the successor to the Data Encryption Standard (DES). The competition was held in order to produce a new cryptographic standard as a replacement for the obsolete DES. Because to the modernization of computer technologies, the Data Encryption Standard's key length (56 bits) was insecure at the time. The Rijndael family of functions is represented by three algorithms in the AES standard. They have varying key lengths of 128, 192, and 256 bits, but they all use the same 128-bit block length. More variations of encryption algorithms, cyphers, and other cryptographic functions are included in the Rijndael family of hashing functions than in AES. The Advanced Encryption Standard was designed to work equally well in software and hardware implementations. With the deployment of the substitution–permutation network design, it was possible. This network design is similar to the Feistel network, which was utilized in DES, but it is faster to compute on both hardware and software, which was critical given DES's software implementation inefficiency.

Our cryptography is the same as that used in Bitcoin, which has been put to the test by hackers all around the world without ever being broken: Breaking this form of cryptography would give you access to coins stored in wallets, which no one has ever done before.

The Advanced Encryption Algorithm (AES256) is an AES algorithm with a key length of 256 bits.The computational difficulty of the decryption is affected by the length of the AES version. The key recovery for AES 256-encrypted data requires more computational power than the 128 and 192-bit variants. The biclique attack, for example, can decrypt AES128 with a computational complexity of 2126. The computational complexity of biclique attacks on AES 192 and AES 256 are 2189.9 and 2254.3, respectively.However, for every key length, real execution of the attacks on the AES-protected data is currently impractical. All of the AES attacks are hypothetical. Every known AES attack would take millions of years to complete, regardless of the algorithm's key length.

- **Anonymous Messenger**

  Encrypted communication software with trustless technology (military security level)

We exacerbated the level of security by eliminating the backend: There is no backend that manages accounts, since there is no backend, ackers cannot enter a server that does not exist! Accounts are client-side only, just like for Bitcoin the account is a private key generated by a passphrase which is kept securely on the client side (the project derives from the Bitcoin project library and inherits its fundamental concepts).

Our mission is to exacerbate the concept of security in messaging and create something conceptually new and innovative from a technical point of view. Top-level encrypted communication (there is no backend , there is no server-side contact list, there is no server but a simple router, the theory is that if the server does not exist then the server cannot be hacked, the communication is anonymous, the IDs are derived from a hash of the public keys, therefore in no case it is possible to trace who originates the messages, the encryption key is changed for each single message, and a system of digital signatures guarantees the origin of the messages and prevents attacks "men in de middle"). We use different concepts introduced with Bitcoin technology and the library itself: there are no accounts, the account is simply a pair of public and private keys, groups are also supported, the group ID is derived from a hash computed through the public keys of the members, since the hash process is irreversible, the level of anonymity is maximum). The publication of the source wants to demonstrate the genuineness of the concepts we have adopted! Thanks for your attention!

A peculiarity of this software, being the low-level messaging libraries the same as our private cloud platform, companies and individuals can use the cloud software router to pass messages between users, creating an internal private messaging circuit, in the which nothing between hosts and external datacenters, as for example instead happens with telegram and whatapp. In any case, everything has been engineered so as not to make it feasible to implement backdoors by us who manage the data communication infrastructure.

It is a project composed of several layers to create a complete messaging software, which can represent the maximum in security and privacy, for this purpose see the technical documentation and the description of the underlying libraries.
The project includes several software layers which technically consist of multi-platform libraries (Linux, Android, iOS, and Windows).
In the lowest state we have the CommunicationClannel Library, a socket-type communication protocol that has sophisticated mechanisms that recover communication even in the case of mobile users where the phone can unexpectedly change the IP and cell to which it is connected, and in the libraries there's also a sophisticated packet spooler and everything needed to re-establish the precarious connection. Technically the CommunicationClannel can be replaced with other compatible ones that instead of the internet connection use the GSM modem network, or serial transmission or other means of communication, in order to use the messaging software with different hardware means of data communication.
At a slightly higher level we have the EncryptedMessaging, the low-level binary encrypted communication library that deals with the encrypted sending of packets, the management of contacts and everything needed to create a complete and

sophisticated security-oriented messaging software information technology, the only thing missing is the graphical interface that will have to be created by the designers in order to customize the user experience according to one's needs. The idea behind this library was to create an encrypted binary messaging platform useful for any need and functioning in any circumstance and on any data transmission medium by replacing the CommunicationClannel which deals with the physical transmission of the packets. The EncryptedMessaging library is so universal that in addition to being used for encrypted communication software, we have also used it as a cloud underlying system for synchronizing data between clients and servers.
Finally, at the top level we have the multi-platform messaging interface (Android, Linux, iOS, Windows), which in fact is only a graphical interface that allows the user to interact with the software, and developers to create a messaging completely customized in terms of graphics and ergonomics.
Messaging software also has crypto wallet functions, and other experimental stuff.

- **Messenger Storage**

  The library for Messenger Cloud (GUI)

  This here is Anonymous Messenger helper software, it adopts trustless security. It offers an encrypted cloud storage where devices encrypt their contact list and other data and send it for safekeeping. This allows the recovery of the contacts, when the messenger account with the passprase is recovered. The device encrypts the data before sending it and therefore the cloud has no way of being able to see it unencrypted (trustless).
  Both this project and the messaging software are open source and inspectable, no aspect of privacy and security has been overlooked, this work reaches military security levels.

  You may also be interested in:

  - Anonymous messenger, messaging software with military-grade security: This project has three open source dependencies for security and functionality. These dependencies are implemented here in the form of Nuget packages, and here are the sources on GitHub (you can replace the nuget packages with the source projects if you want):

  - Secure storage: it is a powerful data safe, the cryptographic keys and data that would allow the software to be attacked are kept with this tool.

  - Encrypted messaging: it is a powerful low-level cryptographic protocol, of the Trustless type, which manages communication, groups and contacts (this software will never access your address book, this library is the heart of the application).

  - Communication channel: is the low-level socket communication protocol underlying encrypted communication.

Preamble

The data produced and managed by a company represents an important part of the company's assets, they are often the result of research and development, let's think, for example, of companies that carry out technological innovation or operate in the field of pharmaceutical research. Even your customer list, contacts, and internal documentation should end up in the hands of competing or ill-intentioned companies could represent serious economic and image damage to your business. Keeping your data private is the ABC of good corporate security practice, all the major non-private cloud service providers have in the past been indicted for privacy violations and therefore are not credible subjects as data custodians corporate. Some of the major public competitors in the cloud sector are also advertising marketing companies and use the stored data to profile their users, explaining their behavior and habits, a role this is incompatible for those wishing to manage a corporate cloud, since the cloud according to all forecasts is one of the major businesses of the future, companies that are technically not credible with regard to respect for privacy, however enter this business trying to create a different image from the real one with refined marketing strategies, however the less naive user does not is deceived, preferring not to transfer the custody of their data to third parties.

- **Amazon – $877m (2021)**

  In July of 2021, European regulators in Luxembourg fined Amazon Europe a whopping $877m fine for data breaches and failing to comply with general data processing principles under GDPR. Officials also tasked Amazon with unspecified ‘practice revisions.’ Google – $391.5m (2022)

- **Google – $391.5m (2022)**

  Google has agreed to a $391.5m settlement over allegations by 40 US states that the tech titan illegally tracked users’ locations. On top of paying the fine, Google is also required to be more forthcoming and transparent when it comes to tracking users’ location and provide more detailed information about location-tracking data on a dedicated web page. The decision came after an investigation led by state attorneys was opened in 2018.

- **France fines Google $57 million for European privacy rule breach**

  France’s data protection watchdog fined Alphabet’s Google 50 million euros ($57 million) on Monday for breaching European Union online privacy rules, the biggest such penalty levied against a U.S. tech giant.
  Source: Reuters

- **The Spanish DPA (also known as AEPD) has fined Google LLC with EUR 10 million**

Two data subjects had filed complaints to the DPA that Google had previously disclosed their personal data to several third parties without their consent. During the lengthy investigation, the DPA discovered that Google had sent the personal data of the data subjects to the Lumen Project. Lumen is a project that's managed and run by the Berkman Klein Center for Internet & Society of the Harvard University. This project began in 2002 for the official purpose of collecting requests related to the removal of content from websites both within and outside of the US. Researchers and other interested parties may then access this data for studies. However, users of the YouTube, Google Drive and other Google-operated platforms could request that the content related to themselves be deleted from these platforms. To this end, Google has provided several complaint and contact forms. However, the data of the people who filed out these forms was automatically transferred to the Lumen Project. The users were not given the chance to object to this data transmission because the process was automatic, and it was a hardwired condition for completing the forms. Consequently, the DPA concluded that Google had no valid legal basis to process the data subjects' data because of this lack of consent regarding the transfer of data to Lumen. In this context, the DPA also discovered that Google did not sufficiently enable the data subjects to exercise their rights of erasure of their data. When analyzing the fine, the DPA took into consideration several aggravating factors: the data was disclosed and transferred to a third-party country without giving the data subjects a chance to object to the transfer. Moreover, this deprived the data subjects of control over their personal data and its transfer. Additionally, the DPA discovered that this transfer had taken place over a long period of time. Another aggravating factor was that a very large number of individuals were affected by this data transfer, and in some cases, sensitive data had been processed.

- **Back on the 31st of December, 2021, the French DPA (also known as CNIL) fined Google Ireland Ltd. with EUR 60,000,000**

  The CNIL received several complaints about the manner in which google.fr and youtube.com approached the manner in which users could refuse cookies on these websites. The CNIL did an online review of these websites and discovered that, despite there being a button to accept the cookies instantly, there was no such button to reject them. To reject the cookies, you had to go through several options, as opposed to one option for accepting the cookies. The CNIL concluded that, in most cases, users accepted the cookies out of convenience rather than because they agreed to it. It also concluded that the way these cookie deposits were designed is an interference with the freedom of consent of internet users, violating Art. 82 of the French Law on Informatics and Freedoms. When determining the fine, the CNIL took into consideration the large number of people who were affected in such an aggravating manner. Additionally, the CNIL also considered the significant profits that the companies could make from advertisements generated indirectly from the data collected through these cookies. The CNIL also pointed out the fact that the authority had previously notified the Google companies of this breach in February 2021. Aside from the fine, the CNIL also issued an order that required the companies to provide all internet users in France with a simple way of rejecting cookies, just as simple as accepting them, within three months of receiving this notification. Otherwise, both

companies would have to pay a fine of EUR 100,000 per day of delay.

- **The DPA authority in Luxembourg fined Amazon Europe Core S.a.r.l. with EUR 746,000,000 ($887,000,000) because the US subsidiary did not process personal data according to the GDPR regulations**

  Apparently, Amazon Europe Core had misused its customer data for targeted advertising. But the company defends itself, saying that there was no data breach and at not time was customer data exposed to other unauthorized third parties. The fine enforced by the Luxembourg DPA came as a result of a 2018 complaint by French privacy rights group, La Quadrature du Net. They argued that Amazon, among other big companies, manipulate customers through targeted content and advertising. They further argued that this was against the principles or privacy and information freedoms of all Europeans. Whether Amazon's defense wins the case remains to be seen.

- **Microsoft menaced with GDPR mega-fines in Europe for 'large scale and covert' gathering of people's info via Office**

  Microsoft broke Euro privacy rules by carrying out the "large scale and covert" gathering of private data through its Office apps.
  That's according to a report that was commissioned by the Dutch government into how information handled by 300,000 of its workers was processed by Microsoft's Office ProPlus suite. This software is installed on PCs and connects to Office 365 servers.
  The dossier's authors found that the Windows goliath was collecting telemetry and other content from its Office applications, including email titles and sentences where translation or spellchecker was used, and secretly storing the data on systems in the United States. That's a no-no.
  Those actions break Europe's new GDPR privacy safeguards, it is claimed, and may put Microsoft on the hook for potentially tens of millions of dollars in fines. The Dutch authorities are working with the corporation to fix the situation, and are using the threat of a fine as a stick to make it happen.
  The investigation was jumpstarted by the fact that Microsoft doesn't publicly reveal what information it gathers on users and doesn't provide an option for turning off diagnostic and telemetry data sent by its Office software to the company as a way of monitoring how well it is functioning and identifying any software issues.
  Other companies typically give users the option to decide whether to send data on their software's functioning to them.
  Source: theregister.com
  Report: https://regmedia.co.uk/2018/11/16/microsoft-office-gdpr-fail.pdf

- **Enterprise giant Oracle is facing a fresh privacy class action claim in the U.S.**

  The suit, which was filed Friday as a 66-page complaint in the Northern District of California, alleges the tech giant's "worldwide surveillance machine" has amassed detailed dossiers on some five billion people, accusing the company and its adtech and advertising subsidiaries of violating the privacy of the majority of the people on Earth.
  The suit has three class representatives: Dr Johnny Ryan, senior fellow of the Irish

Council for Civil Liberties (ICCL); Michael Katz-Lacabe, director of research at The Center for Human Rights and Privacy; and Dr Jennifer Golbeck, a professor of computer science at the University of Maryland — who say they are “acting on behalf of worldwide Internet users who have been subject to Oracle’s privacy violations”. The litigants are represented by the San Francisco-headquartered law firm, Lieff Cabraser, which they note has run significant privacy cases against Big Tech.
Source: Tech Crunch

- **Dropbox security Issues**

  Dropbox is no stranger to embarrassing and harmful data breaches and missteps. In 2011, an update Dropbox pushed to its software allowed anyone to access Dropbox accounts with only an email. Dropbox quickly pushed a patch to fix it, but not before an uproar and some damaged accounts.
  Another Dropbox security breach in 2012 saw Dropbox as the victim of a data leak that exposed the emails and passwords of over 68 million users. It took four years before Dropbox admitted the leak impacted more than just users’ emails.
  In 2017, a programming mistake led to deleted files reappearing in some users’ accounts, including data from over six years prior. Last year, hackers gained access to 130 of Dropbox’s code repositories.
  Source: cloudwards.net

The Secret Global Surveillance Project

Edward Snowden, one of the most famous whistleblowers of our times, brought to light the many surveillance programs and other snooping activities of the U.S. government. This former intelligence officer revealed top secret documents to Glenn Greenwald of The Guardian and Laura Poitras, a freelance journalist, in May 2013 at a hotel in Hong Kong.

The many documents that he gathered from U.S. intelligence agencies like the NSA show the depth and breadth of surveillance programs that have been in place since 2007. It also showed the role of corporations, governments of other countries and lawmakers in furthering and legitimizing these surveillance programs.

Since 2013, we have learned a great deal about the inner workings of the surveillance state of the U.S. and its allies in the Five Eyes (Canada, New Zealand, the UK, and Australia). Through Edward Snowden’s leaks to the press, hundreds of classified National Security Agency (NSA) documents have been made available to the public online. Perhaps most importantly, the Snowden leaks have uncovered relationships between the corporate empire of digital communications platforms and Western intelligence agencies. For example, one internal NSA document demonstrates that Silicon Valley giants such as Google, Facebook, Apple, Yahoo, Microsoft and Skype have shared access to their servers with the NSA through the PRISM program for almost a decade. PRISM and related programs have allowed the Five Eyes to collect and store unprecedented troves of information on their own citizens, including massive amounts of e-mails, text messages, online chats, status updates, phone calls,

videos, cellphone location data and search engine history despite constitutional protections against unwarranted searches. As state-run initiatives collect personal data on hundreds of millions of people on an untargeted basis, this thesis questions the scope of their reach in the U.S. and Canada. Has increased public awareness resulted in significant policy reform or have intelligence agencies and corporations continued running the same patterns? This work questions the future of the internet and digital privacy as various entities collect user data for the ultimate purpose of predicting and manipulating user behaviour, both online and in “real life”. As we enter unchartered realms of technological capability, the use of strong encryption and alternative software programs are offered as temporary solutions for securing communications online.

As digital communication technologies become increasingly popular and accessible across the globe, various organizations have been quietly collecting and storing unprecedented amounts of personal information from its users. Put simply, two major motivations guide data collection programs, “one for intelligence, the other for money” (Wasserman, 2015:15). As a result, run-of-the-mill internet activities such as personal e-mails, Google searches and private Facebook messages are being simultaneously commodified by corporate actors (Zuboff, 2015) and intercepted by government intelligence agencies (Schneier, 2015; Greenwald, 2014; Fuchs, 2014).

As revealed by the now-famous National Security Agency (NSA) contractor, Edward Snowden, the personal communications of hundreds of millions of internet users around the world are being collected and stored by their own governments. Evidently, the NSA’s post 9/11 strategy to “collect it all” (Greenwald, 2014:89) employs untargeted-surveillance programs to scrape as much user information from the web as possible. As of 2012, billions of text messages, e-mails, phone records, search engine history and location data, were being processed by the NSA on a daily basis through various programs (Greenwald, 2014; Schneier, 2015; Goldfarb, 2015). According to Geist & Wark, these findings serve as tangible evidence of what digital privacy advocates had suspected for years, “that fears of all-encompassing network surveillance and data capture that were envisioned as worst-case scenarios have become a reality” (Geist & Wark, 2014:1).

Further, Snowden’s leaks revealed that the NSA had publicly lied to Congress about the capabilities of these programs on numerous occasions. In a 2012 congressional hearing, when NSA Director Keith Alexander was asked whether the NSA collected data on US citizens, he issued the following statement: "wére not authorized to do it nor do we do it" (Cate, 2015). Likewise, a few months before Snowden’s initial disclosures, Senator Roy Wyden asked James Clapper, the Director of National Intelligence (DNI) the following question: “Does the NSA collect data on millions, or hundreds of millions of Americans”, to which he responded “No sir... not wittingly” (Wyden, 2013). Despite the overwhelming evidence rendering these claims blatantly false since the Snowden revelations, Clapper has yet to be reprimanded. As articulated by a member of the US Homeland Security Council, “I

am still waiting for the attorney general to indict him for a clear-cut case of perjury" (Hamilton, 2015:47). Snowden, on the other hand, faces a potential sentence of 30 years in prison under the Espionage Act should he choose to return to the United States (MacAskill, 2015).

Still, these disclosures have resulted in fierce political debates surrounding state surveillance and individual privacy rights (Fidler, 2015), further classified by Laura Lynch as "a vigorous and sustained discussion about security, privacy and the citizen's right to know in the United States and around the world" (Lynch, 2016:15:05). Out of the tens of thousands of classified NSA documents Snowden passed along to Glenn Greenwald, the public only has access to the few hundred that have been released through The Guardian and other media outlets. They have also been made available online through the Snowden Archives. As leaked documents continue to be released, we have gained significant insight into the surveillance industrial complex, which traditionally operates behind a thick wall of secrecy. The released documents revealed some of the secret ways in which the Five Eyes (FVEY), (US, Canada, New Zealand, Australia, the U.K,) and their loosely affiliated partners (such as the Netherlands, Norway and Sweden) work together to secretly collect and share massive amounts of digital data on their own citizens and foreigners alike (Fidler, 2015).

The information disclosed pertains to secret court rulings concerning the scope of NSA surveillance, internal briefing documents outlining the capabilities of many data-mining programs, and breaches of international law by intelligence agencies in the Five Eyes. Civilians aren't the only targets of these programs, as the documents also demonstrate the NSA has spied on the communications of government officials and world leaders of allied countries including German chancellor Angela Merkel (Ball, 2013b). They have also used spy programs to target humanitarian non-profits like UNICEF, the World Health Organization (WHO) as well as the offices of the United Nations (Ball & Hopkins, 2013). Other documents show that Canadàs Communications Security Establishment (CSEC) have been collecting the location data of Canadians who log on to airport Wi-Fi for weeks after visiting the airport, as part of a trial experiment for the NSA. Under this program, the CSE also gained retroactive access to cellphone data generated in the weeks leading up to visiting the airport (Wetson, Greenwald & Gallagher, 2014).

Due to the lack of transparency within intelligence agencies as well as internet corporations, the fine points of mass surveillance can be challenging to investigate. Without whistleblowers like Edward Snowden or AT&T technician Mark Klein who alerted the public about a secret NSA data collection splitter room in AT&T's San Francisco office years' prior, some government surveillance tactics have been speculated on but never confirmed with tangible evidence. Intelligence programs operate under their own secret laws and secret courts such as the Foreign Intelligence Surveillance Court (FISC) in the United States. Because of their confidential nature, their programs and the rulings that pertain to them are kept private and are not typically subject to congressional debate or public scrutiny. The joint efforts of the Canadian Security Intelligence Service (CSIS) and Communications Security Establishment

(CSE) are even less transparent in Canada, as they operate without an external oversight board. In the words of University of Toronto professor Ron Deibert: “The Canadian checks and balances just aren’t there.

We have no parliamentary oversight of CSE, no adequate independent entity to watch the watchers and act as a constraint on misbehaviour. It just doesn’t exist now” (Geist, 2015:228-229). In an interview with Canadian Journalists for Free Expression (CJFE), Snowden cautioned that the surveillance state may only be getting stronger in Canada:

> Canadian intelligence has one of the weakest oversight frameworks out of any western intelligence agencies in the world and when they're trying to expand their powers, you know it’s pretty amazing that we have the Canadian government trying to block the testimony of former Prime Ministers who have had access to classified information...who are warning the public broadly saying ‘this is something we really need to talk about, this is something we really need to debate, this is something we really need to be careful about’ (CBC News, 2015: 0:02-:034).

On the topic of expanding powers, Geist has also argued that since Snowden, recent Canadian legislation has “adopt[ed] lower thresholds for standard warrants” through Bill C-13 as well as “expand[ed] information sharing” and policing power of Canadian intelligence and the RCMP through Bill C-51 (Geist, 2015:226). Furthermore, Geist argues that new trade deals such as the Trans Pacific Partnership (TPP) threaten Canadian privacy rights as well:

> The TPP features several anti-privacy measures that would restrict the ability of governments to establish safeguards over sensitive information such as financial and health data as well as information hosted by social media services... As countries begin to embrace restrictions on data transfers solely to countries with adequate privacy protections, the TPP could restrict the ability of the 12 member countries to do so (Geist, 2015a).

While the datafication of society continues to expand, and circumscribe our social, political and educational experiences, the implications of data mining become a highly significant area for research and inquiry. Ubiquitous surveillance performed for intelligence, law enforcement and commercial gain is shaping both the future of the internet and democracy as we know it. If political sociology is to reflect on contemporary power dynamics between democratic states and citizens, then government surveillance should be a core focus of study within the discipline. As will be explored in the literature review section of this paper, Christian Fuchs has shown how theorizing surveillance from a Marxist perspective can help to untangle the relationships between big business and government in the digital world (2014). Alongside Shoshana Zuboff’s theory of “surveillance capitalism” (2015, 2016), which elaborates on massive scale data collection for the sake of profit under the Google empire, this paper utilizes Fuchs’ perspective to explore invasive government and corporate surveillance efforts as well as counter initiatives that subvert them.

Snowden's whistle-blowing has served to reengage a public debate over internet control and privacy rights that has been ongoing since the 90s. However, further awareness and activism is still needed to reduce the various ways internet users are exploited in the information age. The purpose of this work is to help raise awareness through the critique of blanket surveillance programs in the post-Snowden era. This thesis explores the question of whether significant changes have taken place in the surveillance states of US and Canada since Snowden made his public debut in June of 2013. Here, changes can be achieved through official channels via policy or legal reform.

They can also be made possible through corporate initiatives such as non-compliance with the government or promoting applications that use encryption by default. Alternatively, change can also come from internet users, which may avoid certain programs or take extra steps to secure or obfuscate their data (Brunton & Nissenbaum, 2015).

In order to deepen the investigation of Western surveillance from a critical sociological perspective, this work utilizes a wide variety of sources including the Snowden documents themselves, subsequent journalistic reporting from Greenwald and others from 2013-2016, interview videos from Snowden himself, and academic work by experts in the field of law, digital studies, cryptography and surveillance. Because the Snowden story is ongoing, this work can be considered as part of the first wave of scholarly work using these resources. My investigation has also been guided by four semi-structured interviews with relevant researchers in the Montreal area.

The purpose of this study is to add to the academic discussion on digital privacy, security, and civil liberty as we grapple with the new challenges and opportunities made possible by budding computer technologies and the corporatization of the web. If sociology is to stay relevant and on top of current affairs, there is a need for a critical account of this story and its subsequent outcomes.

My goal is to contribute to that effort. The outline of this project proceeds as follows: Chapter One consists of a brief overview of the literature and methodology used to inform this writing; Chapter Two: The Robin Hood of the Information Age, explains Snowden's motivations in his lifechanging decision to leak an unprecedented amount of classified documents to the press; Chapter Three: Intelligence Programs, Effectiveness, Exploitation and Legality, dives deeper into the capabilities of civilian spy programs, the policies that protect them and their general effectiveness;

Chapter Four: Activism and Encryption, looks for solutions to digital privacy invasion by elaborating on alternative strategies for secure communications. Chapter Five: Social Change, concludes with thoughts on the unequal distribution of risk associated with modernized surveillance tactics alongside the future of the internet and predictive analytics.

Data Espionage in the Age of Global Surveillance

This chapter reviews relevant literature on internet surveillance as well as the aftermath of the Snowden documents. Much of the literature referenced here sheds light on the data surveillance culture of companies such as Facebook and Google, and outlines their motivations for setting up business models in this way. Understanding the corporate side of the web is useful for understanding how law enforcement and intelligence agencies gained access to the data they have today. For example, if those companies had not relied on the collection and sale of user data as their primary modes of profit, or if they had nothing to share with intelligence agencies, the surveillance capabilities of the NSA would be gravely weakened. Moreover, this review sheds light on the Snowden revelations as a crucial component to debates on several political topics, including freedom of the press, journalism ethics, whistleblower rights, the future of the internet, as well as surveillance states at large. Although much of the significant scholarly discussion surrounding this topic has been written before 2013, these works can still be used effectively to theorize or explain what we now know is happening behind closed doors of the Western intelligence community, as well as with the corporatization of the web.

David Lyon, a known expert in surveillance studies, is helpful for explaining what exactly the Snowden documents mean for democracy. In his 2015 article, “The Snowden Stakes”, Lyon insists the future of the internet is the most important question raised by these disclosures: "If there is a key issue raised by the Snowden revelations, it is the future of the internet. Information and its central conduits have become an unprecedented arena of political struggle, centered on surveillance and privacy. And those concepts themselves require rethinking" (2015:139). Due to the public’s general lack of knowledge about government and corporate surveillance over the past four decades, Lyon calls for fresh and accessible research that accurately reflects the new data collection capabilities that come along with new ways of communicating online. In the contemporary context, more research is needed on everyday social media practices such as the circumstances under which users share data and with whom. The analyses of bulk surveillance practices are fundamental to the future of digital communications and human rights to privacy and free speech (Lyon, 2015). However, even though inner workings of surveillance are notoriously elusive and difficult to capture, the limited information we have about secretive intelligence programs is enough to form a baseline critique. Lyon coins the term “liquid surveillance” to capture its omnipresence in today’s culture of smartphones and data mining:

> Surveillance is no longer highly specific and [is] going down very discrete conduits, it’s flowing everywhere. It flows within organizations, it’s everywhere. Personal data especially flows within and between organizations in unprecedented ways and so therés less of an obvious relationship going on. It becomes very fluid and moveable...therefore, it becomes quite difficult to know where those personal data are flowing if something that began in a commercial context, consumer surveillance, ends

> up going through data brokers and is being used for policing or government purposes, you don't know where it's gone (Council of Europe, 2016, 0:39).

the public's general lack of knowledge about government and corporate surveillance over the past four decades, Lyon calls for fresh and accessible research that accurately reflects the new data collection capabilities that come along with new ways of communicating online. In the contemporary context, more research is needed on everyday social media practices such as the circumstances under which users share data and with whom. The analyses of bulk surveillance practices are fundamental to the future of digital communications and human rights to privacy and free speech (Lyon, 2015). However, even though inner workings of surveillance are notoriously elusive and difficult to capture, the limited information we have about secretive intelligence programs is enough to form a baseline critique. Lyon coins the term "liquid surveillance" to capture its omnipresence in today's culture of smartphones and data mining:

Surveillance is no longer highly specific and [is] going down very discrete conduits, it's flowing everywhere. It flows within organizations, it's everywhere. Personal data especially flows within and between organizations in unprecedented ways and so therés less of an obvious relationship going on. It becomes very fluid and moveable...therefore, it becomes quite difficult to know where those personal data are flowing if something that began in a commercial context, consumer surveillance, ends up going through data brokers and is being used for policing or government purposes, you don't know where it's gone (Council of Europe, 2016, 0:39).

Here, the boundaries between state surveillance and corporate data mining have blurred, as subcontracted security and tech companies work together with government intelligence agencies in Western countries. Making reference to his previous work, Lyon stipulates that a loose network of government authority and technical professionals have created a complex surveillance community. Data collection methods previously reserved for military personnel are now being used by an increasing number of agencies. As a result, it becomes difficult for outsiders to tell who exactly is conducting mass or targeted surveillance (Bauman in Lyon, F2015). For Lyon, "The Snowden Stakes" are high, shining a new spotlight on age old questions of human rights and freedoms: "The revelations have rightly remained buoyant in the headlines, just because so much is 'at staké not merely for Surveillance Studies or the future of the internet, but more significantly, for privacy, human rights, civil liberties, freedom and justice" (2015:144).

Lyon notes that clumsy metaphors for explaining data storage and movements are detrimental to policy reform as well as active discussion (2015). He explains that while 'the cloud' is an expression used to refer to online data storage, the physical locality of data and the way it flows is important for critical discourse on the infrastructure of the Internet (Lyon, 2015:145).

Likewise, Clement and Obar insist that the metaphor of the cloud obstructs effective political discussion about surveillance, as the physicality of what is actually happening is rarely discussed or even understood (2014). The idea of data invisibly floating through the air gives it a mystical quality which makes it difficult to pin down in terms of legal boundaries. This makes it harder to subject data flows to territorial laws (Clement & Obar, 2014). Lyon (2015) and Clement and Obar (2014) have both argued that the precision of metaphorical language can be crucial to progressive discussions around policy formation and legal decisions surrounding Big Social Data. Thinking about data as physical matter that flows through fiber-optic cables in data packets helps us to compare online messages to letters in the mail. This makes it easier to discuss what is happening to digital data as it flows through cyberspace. Letting go of the 'cloud' metaphor becomes important when discussing major issues surrounding constitutional protections when data crosses national borders. Once online data leaves one country and travels through another, the user who generated the data no longer enjoys their home country's constitutional rights to privacy.

Currently, even efforts to keep data localized are being subverted by new international trade deals.

For example, Geist explains how the TPP threatens to reverse recent Canadian initiatives to keep sensitive data within the country in response to US surveillance: "provinces such as British Columbia and Nova Scotia have enacted laws to keep government information (such as health data) within the country. The TPP is designed to counter these efforts by restricting the ability of governments to mandate local data storage" (Geist, 2013a). For reasons such as this, understanding ways in which data is transmitted through networks is crucial for debating government and corporate policy that concerns digital life.

As discussed by Clement and Obar, Snowden has shown that the NSA intercepts internet data from all over the world while it transits through major US cities through splitter operations that copy and store the information (2014). In the tech world, this movement of data across national boundaries is referred to as "boomerang routing" and makes Canadian internet users vulnerable to NSA surveillance, even when both parties are communicating from within Canada in close proximity (Clement & Obar, 2014). As shown in one internal NSA PowerPoint slide from the Snowden documents, data packets of information move through fibre-optic cables through the cheapest route before reaching their final destination. As a result, much of Canadian data goes through the United States where it is intercepted and stored, before being bounced back to its final destination in Canada (Lyon, 2015; Clement & Obar, 2014). While investigating the paths of thousands of Canadian data routes, Geist and Wark found that almost 25% of Canadian data flowed through the United States before coming back to Canada, each time passing through cities with NSA splitters (2014). Because of the ways in which data flows across borders, national laws concerning data collection are easily evaded. This poses a threat to digital privacy rights:

> Once the data flows beyond the border, it no longer enjoys Canadian constitutional and other legal safeguards. This means the NSA or other US agencies can legally intercept and analyze it without warrants or other judicial oversight. Furthermore, Canadians have no legal basis to challenge or remedy any abuses (Clement & Obar, 2014: 27).

What is at play here is a larger force that extends beyond the legal rights of citizens of any given nation. In their book Empire, Hardt and Negri have commented on these forms of globalized power and the significance of mass surveillance within them. They argue that the globalization of surveillance is crucial for the functionality of contemporary forms of imperialism to flourish (2000). Thinking deeper about the role of government and corporate actors in 21st century politics, contemporary politics distort the boundaries of transnational corporations in collaboration with state efforts of control: “The concept of Empire is characterized fundamentally by a lack of boundaries: Empirés rule has no limits. First and foremost, then, the concept of Empire posits a regime that effectively encompasses the spatial totality, or really that rules over the entire ‘civilized’ world” (Hardt & Negri, 2000: xiv). Later, in Commonwealth, Hardt and Negri continue by asserting that biopolitical control (or governance over bodies and minds) relies on surveillance practices in order for authorities to maintain a dominant role in order to “primarily divide and segment the common field of productive cooperation” (Hardt & Negri, 2009:144), thus discouraging political organization and action against capitalism.

Likewise, Christian Fuchs notes that digital risks of exploitation and privacy invasion come not only from state governance but from corporate power (2014). Fuchs points to capitalism as a form of domination and control and a force that contradicts democratic freedom. Using the harsh state sanctions on whistleblowers in the United States as an example, he characterizes capitalism as a system in which alternative media cannot flourish or effectively disseminate information:

“The economic, political, and ideological repressions that WikiLeaks faces are characteristic of the fact that the freedom of the media and information does not and cannot exist in capitalism” (Fuchs in Fuchs 2014: 11). For Fuchs, the resistance alternative media outlets face is one reason why political movements should aim to disarm structural power imbalances: “progressive struggles have to be directed against capitalism and power asymmetries” (2014:11). More generally, he offers privacy law reform as a solution to one form of corporate exploitation: “given the right kind of government, states can also pass legislation that protects consumers’ and employees’ privacy from surveillance that serves corporate interests” (Fuchs, 2014:13). Fuchs supports Edward Snowden’s actions as part of a larger movement of organizations and actors working to critique the commodification and surveillance-enabled structure of the internet:

> The actual practices of data commodification, corporate media control and corporate and state surveillance limit the liberal freedoms of thought, opinion, expression, assembly and association. These movements and groups are the negative dialectic of

> the enlightenment of the 21-st century informational capitalism. They show the difference between the proclaimed essence and the actual existence of liberalism (Fuchs, 2014:11).

As Fuchs enunciates this critique of liberalism, he believes more effort is needed in this direction, calling for a "society of equals, a participatory democracy" (Fuchs, 2015:11) as a solution to repressive state and corporate control over both the internet and society at large. As many discussions surrounding mass surveillance and civil liberties in the digital age touch upon the dynamics of corporate and government power, this has recently inspired some academics to rethink the exploitation of internet user activity through a Marxian analytic framework (Andrejevic, 2014). Fuchs differentiates between political and economic surveillance, noting that each operate by placing citizens under the threat of violence, albeit in different forms: "In the case of political surveillance, individuals are threatened by the potential exercise of organized violence (of the law) if they behave in certain ways that are undesired, but watched by political actors (such as secret services or the police)" (2013:7). In describing economic surveillance, Fuchs writes:

"individuals are threatened by the violence of the market that wants to force them to buy or produce certain commodities and helps reproduce capitalist relations by gathering and using information on their economic behaviour. Violence and heteronomy are the ultimo ratio" (Fuchs, 2013: 7). For Fuchs, both economic and political surveillance are about securing behavioural control of the masses by any means necessary, including the threat of violence in various forms.

While Fuchs recognizes that Marx's analysis of capitalist society alone cannot account for all the complexities of the modern surveillance state, his writing illuminates the significance of Marx's work for theorizing this type of research. Fuchs exposes the main goal of these combined activities as a means of maximizing surplus value through the exploitation of the labour force:

"capital employs surveillance to control and discipline the workforce. Economic surveillance helps minimize the risk of making losses and maximizes the opportunities for profits" (Fuchs, 2013:9).

He explains further by pointing to various ways in which surveillance works under the cycle of capital accumulation. To name a few examples, surveillance works to enhance capitalist relations through targeting future employees for background checks, using electronic or human supervision to evaluate workplace performance and protect private property, or following the data trails of consumers or market competitors (Fuchs, 2013: 8). Fuchs argues that the general logic of capitalist accumulation can be applied to support population management and control under capital:

> Marx's notion of accumulation as a central process of contemporary society plays an important role in unifying different approaches because modern society is based on the

> competition between actors accumulating ever more money capital, political power and ideological power and controlling the resulting resources. Marx is therefore not only important as a critical theorist of capitalism, but also in a more general sense, because he has pointed out a general law of movement in modern society originating in the capitalist economy that shapes all subsystems so that relatively autonomous subsystems have emerged based on the logic of accumulation. That is, modern surveillance is a competitive and instrumental process oriented towards accumulating money, power and hegemony (Fuchs, 2013:3).

While understanding surveillance as a core aspect of capitalism, Marx and Engels have elaborated on how the state monitors the population in various ways to maintain its power: "[The State] enmeshes, controls, regulates, superintends, and tutor's civil society from its most comprehensive manifestations of life down to its most insignificant stirrings" (Marx & Engels, 1968:123 in Fuchs 2013). As characterized by Ogura (2006), the five forms of capitalist surveillance deal with population management, workplace surveillance, consumer behavior, control of the human mind, and digitalized surveillance (Ogura 2006 in Fuchs, 2013). Again, each form is concerned with monitoring and collecting information on bodies and minds in order to influence, predict, control or dissuade behaviour under capitalism, making it very difficult for individuals to discuss alternative politics or potential activist projects privately.

Following Manuel Castells' theory of informational capitalism, whereby technological advancements facilitated the switch from material labour to immaterial labour and resulted in the restructuring of western capitalism from the 1980's onward1 (2009), Shoshana Zuboff has used the logic of accumulation to explain the undercurrents of modern surveillance under capitalism.

"Surveillance capitalism" is a new form of capitalizing on the activity of others whose main purpose is to ultimately predict and manipulate consumer behaviour for profit" (Zuboff, 2015:75).

Using the motivation of capital accumulation to collect as much data on internet users as possible, information on peoplés every move can be digitized, commodified, and sold to third-parties (Zuboff, 2016). Here, Zuboff's three laws of surveillance capitalism are also of relevance to explain the expansion of the surveillance state alongside the recent progress of the digital age:

> First, that everything that can be automated will be automated. Second, that everything that can be informated will be informated... [and third, in] the absence of countervailing restrictions and sanctions, every digital application that can be used for surveillance and
>
> control will be used for surveillance and control, irrespective of its originating intention

(2013).

Mark Andrejevic also expresses the need for a critique of political economy to explain the intersection between surveillance and capitalism, as privacy-based arguments alone are inadequate to explain the full level of exploitation at play: “privacy-based critiques do not quite capture the element of productive power and control at work in the promise of monitoring-based marketing...

the critique of exploitation addresses this element of power and control" (2012:86). He also challenges readers to think about the future of society in the context of extensive digital surveillance methods that effect hundreds of millions of internet users:

> It is time to move beyond the question of whether or not we want targeted advertisingthe real issue is whether or not we want to create a world in which every detail of our behaviour and communications with one another feeds into giant databases that are used to sort and evaluate us in ways that remain totally opaque to us, by a range of institutions whose imperatives are not necessarily our own (Andrejevic, 2013:189).

While various scholars have pointed out the ways in which internet users give up rights to their personal data in exchange for the use of so-called free services (Trottier, 2012; Schneier, 2015; Zuboff, 2015), Fuchs (2016) and Andrejevic (2013) have both drawn parallels between Marx’s alienation of labour and alienation involved in social media activity. Although the alienation of labour has traditionally underlined the exploitative experience of wage-labourers (Marx, 1844), this theory can be loosely applied to social relations of the digital era in that internet users lose ownership and control over their own online activity, which alienates them from this activity and its products. That is, they often have no knowledge of where their data goes, or for what purposes it is used thereafter. User-created content is handed over as a new form of free raw material (data) to big businesses who then use it to create new value through sorting, analyzing, and selling this data. At the same time, the same users who created it go uncompensated for their activity (Fuchs, 2016, Andrejevic 2013). Platforms such as Facebook and Google collect user data to provide a more intuitive browsing experience, which is reflected in the algorithmic sorting of data that ensures the most relevant information appears first. They also sell this data, such as demographic information, (sexual orientation, religious affiliation, age, income levels, behaviour patterns, location data, friend lists, shopping habits, etc.) for profit, as third-party companies pay large sums of money for this information. As pointed out by cybersecurity expert Bruce Schneier, “Location data is so valuable that cell phone companies are now selling it to data brokers, who in turn resell it to anyone willing to pay for it” (2015:8), and these sales are taking place unbeknownst to users who are being tracked by GPS technology for these purposes. Outside of programs like AdBlock, internet users also have very limited options of the types of targeted advertisements they are subjected to, which puts their online experiences out of their control at yet another level (Fuchs, 2016).

In this form of exploitation, third-parties use this data for analytics and marketing purposes meant to predict, manage and control consumer behaviour. In the words of Zwick, Bonsu and Darmody, social media platforms rely on user generated data to "expropriate the cultural labour of the masses and turn it into monetary value: each in their own specific way but all according to the same general logic" (Zwick, Bonsu & Darmody in Andrejevic, 2012:72). Here, Andrejevic asks us to recognize “the importance of considering the components of exploitation (the capture of unpaid surplus labour, coercion, and alienation) [that] operate within the context of technologically facilitated forms of commercial surveillance” (2012:87). The concept of alienation as applied to digital age online participation effectively demonstrates another way in which Marx remains relevant for critiquing 21st century surveillance tactics.

Moving forward, reference to Foucault’s ground-breaking work on early forms of surveillance and disciplinary society (1977) is helpful. Of equal relevance to the contemporary context of state power exercised as surveillance is Deleuzés subsequent commentary on societies of control (1992). Deleuze weighs in on new forms of social sorting through technology, as individuals are reduced to their data bodies, which Deleuze refers to as ‘dividuals’, entities to be managed and monitored by companies and law enforcement agencies: “The numerical language of control is made of codes that mark access to information, or reject it. We no longer find ourselves dealing with the mass/individual pair. Individuals have become ‘dividuals,’ and masses, samples, data, markets, or ‘banks’" (Deleuze, 1992:5). As defined by Williams, a "dividual” refers to “a physically embodied human subject that is endlessly divisible and reducible to data representations via the modern technologies of control, like computer-based systems” (2005:2).

Because liquid surveillance (Lyon 2015) has extended far beyond the confines of the institution, it is often argued that the panoptic threat that ultimately controlled bodies within prisons, schools or places of work has transcended that old model. In this view, we have moved away from Bentham’s vision of the panopticon as presented by Foucault (1977), whereby the very possibility of always being visible within institutions forces people to alter their behaviour (Foucault, 1977:200). Through technological means, new age surveillance has seeped into digital devices, exposing our innermost private thoughts, relationships, plans, and conversations. For this reason, according to Simon (2005), this new electronic realm does not signify the death of Bentham’s panopticon, but has only expanded it. Under the reign of “new surveillance” or “dataveillance”, the population is under even harsher scrutiny than previously imagined: “What makes databased selves different from our actual selves is that databased selves are more easily accessible, observable, manageable and predictable than we are. Databased selves actually meet the Benthamite ideal better than the disciplined bodies of the Panopticon” (Simon, 2005:16). In this day and age, the very possibility of being watched at any given time has become a fathomable reality, even within the confines of our own homes.

On the topic of data bodies and data trails, Snowden advocates for the important possibility to remain anonymous online, as the fear of being surveilled breeds self-censorship and hinders education. In CITIZENFOUR, a documentary about his meeting with reporters in Hong Kong to discuss and hand over the leaked NSA documents, Snowden asserts that the very knowledge of being potentially surveilled online “curtails intellectual freedom” and “limits the boundaries of intellectual exploration” where people are afraid to write or research on certain topics out of fear of ending up on a government watch list (Poitras, 2014:26:55-27:20). We can interpret this fear using Foucault’s concept of governmentality, whereby entire populations are socialized to conform and govern their own actions and thinking through various institutional and cultural norms alongside the implicit threat of fear-based policing (2007). The existence of mass surveillance can be harmful to social movements and political progress; in Greenwald’s words: “history shows that the mere existence of a mass surveillance apparatus, regardless of how it is used, is in itself sufficient to stifle dissent. A citizenry that is aware of always being watched quickly becomes a compliant and fearful one” (2014:3). In this case, governmentality describes the situation when users avoid using the internet in certain ways, self-policing their own internet research and social connection due to fear of being targeted for extra surveillance. Pew Research has indeed shown that at least 34% of Americans have made some attempt to privatize or change their internet habits since learning of the Snowden revelations (Rainie & Madden, 2015).

Next, the subject of whistleblower protection is an important aspect within literature on the Snowden files. While media controversy surrounding whistleblower Chelsea Manning’s harsh prison sentence is ongoing (Pilkington, 2015), there has been much subsequent debate about what to do with Edward Snowden. As discussed in “Protecting News in the Era of Disruptive Sources” (Wasserman, 2015), members of the press enjoy certain immunities to legal scrutiny that whistleblowers do not. Even though the press needs whistleblowers for serious investigations of questionable government and corporate practices, media organizations often do little to help their sources in terms of legal protection (Wasserman, 2015). Wasserman, a professor of journalism and ethics at Washington and Lee University, argues that the Snowden case can serve as either a deterrent or inspiration for future whistleblowers, depending on how the US handles his capture or release. Snowden has been charged under the Espionage Act2 but due to the valuable information Snowden revealed, Wasserman argues that Snowden should be entitled to a fair trial with a strong legal defense, which is currently not an option. For Wasserman, Snowden’s charges should reflect the significance of his disclosures: “something appropriate to the enormity of the wrong-doing he has exposed, something that helps make the country safe for others who have stories the public is entitled to hear” (2015: 118).

Here, the legal protection of whistleblowers is important to the larger issues of freedom of speech, government transparency, and future of democratic information networks. Wasserman explains that the digital revolution of communications can either result in unprecedented emancipation or suppression. As we have seen with recent “fake news”

scandals following the Trump election, technology alone does not guarantee the sharing of true or high quality information, nor does it guarantee meaningful public dialogue. Wasserman argues that political journalism and whistleblowing can only flourish if sources can enjoy proper protection and fair legal processes:

> People who have information [of public significance] believe it will be heard and welcomed, and if they can step forward with it without fear of punishment. That's why the whole edifice of informational freedom in the digital age depends on creating and environment in which sources can speak (Wasserman, 2015: 119).

Traditionally, because of the thick veil of secrecy safeguarding the secrets of intelligence agencies, whistleblowing has been the only catalyst for reform in the intelligence community (Cullather, 2015:23; Hamilton, 2014). Bruce Schneier (2015) and Glenn Greenwald (2014) have both shared similar sentiments, stating that whistleblowers and journalists need better legal protection to expose serious wrong-doing. Schneier suggests that government whistleblowers should benefit from the same legal protections that corporate whistleblowers enjoy. This does not suggest that anyone should be able to leak any information and call themselves a whistleblower.

The argument is that there should be appropriate legal framework and protocol for leaking sensitive information, by which courts could evaluate leakers on a case by case basis, where the defendants have a chance to defend their actions from a moral standpoint in front of a jury of their peers (Schneier, 2015).

While whistleblower protections are weak, so too are the rights of internet users in general, especially when dealing with governing bodies outside of their own countries. As state and corporate actors work together to maintain control of the internet and its users, Tim Berners Lee, the creator of the World Wide Web, has been calling for a public collaboration on “A Magna Carta for the Web”, as the corporatized internet in its current form is uncoordinated with its true democratic potential of information sharing and non-hierarchical power structures (2014). As stated by Schneier, this effort would “restrict the actions of both governments and corporations, and impose responsibilities on information-age corporations rather than just rights” (2015: 149).

Along these lines, work from the Berkman Center for Internet and Society at Harvard University investigates thirty different web advocacy initiatives working towards an “Internet Bill of Rights” or “digital constitutionalism” between 1999-2015. The authors use this term to categorize a variety of efforts working towards “political rights, governance norms, and limitations on the exercise of power on the internet” that have the potential to change governmental and corporate policies concerning internet use (Gill et al., 2015:2). Gill, Redeker and Gasser map the trajectory of influential organizations, hacktivists, cryptographers, journalists and others that have been taking action towards making the internet a decentralized, democratic space for free speech, anonymity and information

sharing (Gill et. al, 2015). In hopes of pushing public policy and law in the direction of digital constitutionalism, the authors explain how the Snowden documents have positively influenced discourse on privacy rights initiatives:

> In particular, we see marked overall increases in the occurrence of the right to data control and self-determination, the right to anonymity, the right to use encryption, and the right to explicit protection from government surveillance. Our hypothesis, borne out at least in a preliminary way by this data, is that while the perceived importance of privacy rights was not substantially affected, they are now being articulated in much more specific, sophisticated, and nuanced ways than they have been in the past (Gill et al., 2015:17).

Despite the wide range of differences between initiatives to democratize the internet, these efforts are grouped together based on this common goal "and are usefully understood as part of a broader proto-constitutional discourse" (Gill et al., 2015: 2). Activist initiatives to protect the legal use of strong encryption are also of relevance here, as the political and legal landscape is still unfolding in terms of questions of who governs the internet as well as what constitutes legal online activity. Additionally, this article demonstrates the significance of discourse, activism, and academic investigation on digital rights by making reference to the International Principles on the Application of Human Rights, stating that Snowden's documents have only expedited the significance of these movements: "[n]othing could demonstrate the urgency of this situation more than the recent revelations confirming the mass surveillance of innocent individuals around the world" (Gill et al., 2015:17)3.

As the internet has been exposed to be a risky place for private communication due to pervasive surveillance on multiple levels, the concept of risk itself is worth exploring. Social theorist Ulrich Beck has also commented on Big Data surveillance in lieu of Snowden by expanding on his 1992 theory of risk society. In 2013, he coined the term "Global Digital Freedom Risk" to refer to the heightened risks involved for internet users in the 21st century, where activist groups are heavily targeted as blanket surveillance operations become normative. Beck calls for a "digital humanism" when he writes: "Let us identify the fundamental right of data protection and digital freedom as a global human right, which must prevail like any other human right, if needs be against all odds" (2013)4. Following Beck, digital sociologist and risk studies scholar Deborah Lupton identifies three components of "Digital Risk Society" in a paper with the same title. As activism has become increasingly criminalized with harsher sentences, digital activists also take on the risk of violence perpetuated by the state. More generally, mass surveillance makes private digital communications risky, as users lose track of their own digital movements. In terms of the digital divide, those without internet access face different types of risks in this new age concerning opportunities and life chances (Lupton, 2014). Lupton calls for traditional risk studies to move towards digital sociology and surveillance studies to create a more

comprehensive interdisciplinary understanding of how to grapple with the struggle of the increasingly pervasive risks associated with communications technology (2014).

Published a year before the first Snowden disclosures, Daniel Trottier's book Social Media as Surveillance: Rethinking Visibility in a Converging World investigates the risks of using social media by studying Facebook as a new social dwelling (2012). Trottier explores the ways in which users live and interact online as well as who is watching their behaviour. Facebook, once an exclusive platform for university students to communicate with each other, has turned into a massive network early users no longer recognize. Over the past decade, as parents, grandparents and work colleagues have joined the site, the overall structure and social significance of the dwelling has drastically changed. Thus, users are not only being watched by their own network of "friends" but also their employers (present or future), their universities, the police, government agencies, third-party corporations, and of course, Facebook itself. Most significantly, local law enforcement agencies have gained access to backchannels of social media quite some time ago, and new additions to the platform such as facial recognition have made evidence collection on social media easier for police departments (Trottier, 2012).

Trottier uses the aftermath surrounding the Vancouver Hockey Riots as an example of crowd-sourced surveillance on Facebook, where thousands of people shared images and videos of the riots while others identified them to help police catch rioters on designated Facebook groups.

While Trottier appreciates the many benefits of new communication technologies, he also explores surveillance as "the driving force behind social sorting, the allocation of life chances and business models in the information economy" (2012:7). For Trottier, one of the biggest risks of greater public visibility on social media is giving law enforcement unprecedented access to information it otherwise had no means of legally attaining. As social media sites become dwellings for larger segments of the general population, the convergence of government, corporate, activist, criminal and social interests find a new site of intersection, marking the internet an emerging social space for sociological inquiry (Trottier, 2012).

As mentioned above, Zuboff theorizes on how technology helps to enhance the mass surveillance project, and will continue to do so unless meaningful oversight or limitations of power are imposed on it. As a result of new technological capabilities and a lack of legal regulations to keep up with them, companies who engage in data collection have far more power over their clients than those who do not. In one example, Zuboff points to insurance companies who follow Googlés business model of data mining to collect and sell information on their clients to increase profit.

Car insurance companies are beginning to use GPS technology to collect data on driving habits, which can result in higher insurance rates, time-stamped location data and the

possibility of shutting engines down remotely as a response to late payments or aggressive driving (2015).

Zuboff's article "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization" (2015), investigates Google as a key perpetrator of surveillance capitalism as the king of Big Data analytics. As the world's most visited website, Google has been the leader in Big Data analytics, paving the way for Facebook and other notable internet firms to collect and store mass amounts data to sell to advertisers (Zuboff, 2015). Google puts innovation before everything else including the legality of its own actions. Zuboff uses the example of Googlés Street View project where Google took the liberty of taking photos of homes across the globe without obtaining any sort of permission, illegally scraping their personal Wi-Fi data along the way (Zuboff, 2015).

Google has taken advantage of a time where both the law and user understanding are perpetually a few steps behind new communications technology. Consequently, once privacy laws are set in place to secure user data, companies like Google will use the same arguments for privacy rights to hide its own activity:

> Surveillance capitalists have skillfully exploited a lag in social evolution as the rapid development of their abilities to surveil for profit outrun public understanding and the eventual development of law and regulation that it produces. In result, privacy rights, once accumulated and asserted, can then be invoked as legitimation for maintaining the obscurity of surveillance operations (Zuboff, 2015: 83).

By extension, the business models and unprecedented data accumulation of these companies are what makes today's extensive state surveillance possible in the first place. Zuboff challenges Googlés Chief Economist, Hal Varian, in his view that predictive analytics will make new social contracts possible in a progressive way, where the Google users will "voluntarily" give up even more of their behavioural data in exchange for high tech services such as digitalized personal assistants that know what you want even before you do. Instead, Zuboff argues that a constantly surveyed reality will result in the end of social contracts and the absence of consumer choice: "In Varian's economy, authority is supplanted by technique, what I have called the 'material dimension of power' in which impersonal systems of discipline and control produce certain knowledge of human behaviour independent of consent" (Zuboff 2015:81). As the White House and Google both fully intend to continue mining as much internet data as possible, Zuboff warns predictive analytics are harmful to the concept of the democratic right to privacy. The way data mining is currently performed under Castells' "information capitalism" (2009) perpetuates power imbalances and damages life changes by "predict[ing] and modify[ing] human behaviour" for the sake of profit (Zuboff, 2015: 75). Under surveillance capitalism, the relationships between producer and consumer or capitalist and labourer have changed. First, Googlés customers aren't its users, but their advertisers (Zuboff, 2015). Second, though Google employs tens of thousands of people, its most valuable material (data) is collected for free, from users who (however unknowingly) provide

massive amounts of personal data to be analyzed and sold to third-parties daily. In a 2009 Wired article, Varian explains that Google offers its services for free because user action holds value for corporations, and more web traffic inevitably leads to more ad sales: “since prediction and analysis are so crucial to AdWords, every bit of data, no matter how seemingly trivial, has potential valué (Levy, 2009 in Zuboff, 2015:79). This, combined with smart technology and wearables, creates a reality where every single human movement is potentially commodifiable by outside forces. Outlining the threat to freedom and social contracts that this type of surveillance culture implies, Zuboff critiques Varian’s optimistic view of the future of behavioural data mining. Googlés ideology does away with the very possibility of privacy as a choice at all. When the inherent trust is taken out of traditional contracts between buyer and seller to be replaced with digital surveillance that renders all human activity ‘certain’, Zuboff argues:

“deception-induced ignorance is no social contract, and freedom from uncertainty is no freedom” (2015:86).

Data mining projects will only get more sophisticated and deeper in breadth. To highlight this point, Zuboff quotes a 2014 White House report: “The technological trajectory, however, is clear: more and more data will be generated about individuals and will persist under the control of others” (White House, 2014: 9 in Zuboff 2015: 75). The future plans of internet giants only seek to expand data mining capabilities alongside their own profitability, capturing anything they can about users’ immediate reality. We see this happening with the rise of “smart” technology, wearable sensors and GPS technology used to share private health data, and patterns of movement to surveillance databases (Zuboff, 2015). Predictive analytics are the next step towards influencing and controlling consumer activity, as insurance rates (Zuboff, 2015), employment opportunities (Schneier, 2015), and bank loans (McCrum, 2015) are becoming increasingly dependent on digital data collection. Schneier likens this level of surveillance to extending the way celebrities and politicians are constantly scrutinized to the general population (2015). Internet users are penalized in ways they may not even be aware of by their own data content. In defense of the NSA after the initial Snowden leaks reached the public, Robert Litt, General Council for the Office of the Director of National Intelligence explained the NSA’s intentions to make use of new technologies to fight crime: “Rather than attempting to solve crimes that have happened already, we are trying to find out what is going to happen before it happens” (Fidler, 2015: 104).

From a critical standpoint, one way predictive analytics are ethically problematic is due to the threat of digitalizing the same racist and classist bias already embedded within some traditional law enforcement practices in the United States and elsewhere. History has shown that regardless of the method, marginalized populations and dissidents are consistently surveyed the most (Greenwald, 2014; Hamilton, 2014; Lynch, 2012). Just as new biometric technologies often discriminate against disabled bodies or people of colour (Magnet, 2011), algorithmic crimeprediction programs may have racial discrimination built into their systems

as well, targeting areas which are already heavily policed to begin with, which are most often communities of color in the United States (Eubanks, 2014; Lynch, 2012). Hewitt argues that while discriminatory targeting is not new, the possibilities of reach have greatly expanded: “certain groups and individuals have long been subjected to more intrusive surveillance, and dramatic consequences as a result of that attention, because of their ideology, race, ethnicity, gender, sexuality, religion, nationality, social class, or some combination of these variables” (Hewitt, 2015:46). The potential outcomes of this type of information access by third parties can be life changing for the individuals involved. As users lose control over their private identities online, information meant to be shared with close friends may be accessed by future employers, family members, the police or national intelligence.

The intimate details of sexual preferences, religious affiliations and medical history are made available to various entities without consent or knowledge (Schneier, 2015). To circumvent this from happening, strong legal protection against the abuse of mass surveillance programs is needed.

As aptly concluded in Zuboff’s analysis: “The question is whether the lag in social evolution can be remedied before the full consequences of the surveillance project take hold” (Zuboff, 2015:85).

PRISM

Probably Snowden’s biggest revelation was concerning a program called PRISM, under which the National Security Agency (NSA) accesses emails, documents, photographs and other sensitive users’ data stored in major companies.

Documents leaked by Snowden show that Facebook, Google, Microsoft, Yahoo, PalTalk, AOL, Skype, YouTube and Apple give the NSA direct access to its users’ information. According to the documents, Dropbox also joined this list.

PRISM was launched from the ashes of President George W. Bush’s domestic surveillance programs, which were abandoned due to lawsuits, disclosures in the media and widespread protest.

Due to past controversies, this program was given the legal go-ahead by the U.S. Congress when it passed the Protect America Act in 2007. Also, the FISA Amendments Act of 2008 gave legal immunity to private companies that cooperated voluntarily with U.S Intelligence agencies.

Microsoft became PRISM’s first partner in 2007 and the NSA began collecting vast amounts of data from its servers. Other companies joined the program in due course. In 2008, Congress gave the Justice Department authority to compel a reluctant company to “comply” with the needs of PRISM. This means that even companies that were not willing to join the program voluntarily had to do so at the behest of a court order.

This gave the NSA access to even more information. Soon, PRISM became a leading source of raw material for the NSA, as it accounted for one in every seven intelligence reports. PalTalk, for example, is much smaller when compared to the other companies on the list, but it provided substantial intelligence during the Arab Spring and the ongoing Syrian civil war.

Wiretapping

A court order shows that Verizon was ordered to provide the details of all calls, on a daily basis, to the NSA. This included calls that were made within the U.S. as well as between the U.S. and other countries.

This order was granted by the secret Foreign Intelligence Surveillance Court to the FBI on April 25, 2013. Under this order, Verizon has to provide the numbers of both parties on a call, location data, call duration, time of the call, International Mobile Subscriber Identity (IMSI) number and any other unique identifiers.

In addition, the court order explicitly forbids Verizon from disclosing to the public the existence of FISA order or this request from the FBI. The terms of this order complies with the “business records” provision of the Patriot Act.

A report in The Wall Street Journal shows that this court order was sent to AT&T and Sprint Nextel too. This arrangement with the country’s three largest phone companies means that the NSA gets a record of almost every call that is made.

To top it, some documents show that the NSA can crack cellphone encryption, so it can easily decode the content of intercepted calls and messages.

The report also states that the NSA made a similar arrangement with Internet service providers to obtain data about emails and browsing history of all individuals. A recent decision by the U.S. Senate will compound this breach of privacy by ISPs, as they will not just be working with the NSA but also with commercial third parties to sell customer data.

Besides wiretapping and ISP spying, credit card transactions are also cataloged and stored in NSA’s servers for analysis.

Tempora

The British intelligence agency, the Government Communications Headquarters (GCHQ) works closely with the NSA in a program called Tempora.

Under this program, GCHQ monitors the world’s phone and Internet traffic to gather information on emails, calls, facebook messages and browsing history by tapping directly into the transatlantic fiber optic cables that land on the shores of the UK. All this data and

intelligence is shared with the NSA. In fact, more than 850,000 NSA employees and private contractors like Snowden had access to the GCHQ database.

A report shows that in 2012 alone, the GCHQ handled 600 million phone calls a day by tapping into 200 cables. Since each cable can carry 10GB of data per second, this agency had access to about 21 petabytes of data every day.

This collection is legal, as the Regulation of Investigatory Powers Act (RIPA) allows the GCHQ to collect information without a warrant. As a result, Tempora gives the British spying agency the “biggest Internet access” among a coalition called “Five Eyes,” which comprises Australia, Canada and New Zealand, besides the UK and the U.S.

Final Thoughts

From the above facts it’s clear that the NSA is keeping a constant watch over your activities. With the help of large corporations and lawmakers, the government knows every little thing you do. Even information you access, store and use is recorded in NSA’s facilities, thereby giving you little to no privacy in your everyday life.

Such programs show how surveillance practices have shifted from individual suspicion in favor of a large and systematic practice of collecting mass data. Given this, the onus is on you to protect your privacy in a methodical way.

Text credits by: Cloudwards & © Jessica Percy Campbell

Public Cloud vs Private Cloud: What is the Difference?

The key difference between public and private cloud computing relates to access. In a public cloud, organizations use shared cloud infrastructure, while in a private cloud, organizations use their own infrastructure. To fully understand which cloud environment organizations should use, it is important to understand each environment in-depth, as well as their advantages and disadvantages.

What is a Public cloud?

In a public cloud model, cloud services and resources are offered through a third-party cloud service provider (CSP) and delivered via the internet through a subscription model, such as platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS) or software-as-a-service (SaaS). In this model, all hardware, software, and other supporting cloud infrastructure are owned, operated and maintained by the cloud provider and shared with other users. Examples of public clouds include Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

The public cloud operates on the principle of multi-tenancy, which means that multiple organizations, or “tenants”, have access to the same cloud infrastructure and computing resources, such as servers and cloud storage.

What is a Private Cloud?

A private cloud, which is sometimes referred to as an on-premises private data center, is a cloud computing model where one organization has exclusive use of the cloud, its services and associated infrastructure. While a private cloud may still be hosted by a CSP, it is dedicated to just one user and resources are never shared.

Private clouds are most often used by organizations that require customizable and highly secure IT environments. For example, private clouds are often used by government agencies, hospitals, or financial institutions, which maintain sensitive data and are subject to strict compliance standards.

Information taken from crowdstrike.com

Benefits of a private cloud solution:

- **Privacy** As the name implies, the private cloud is not shared with other tenants, which means that a single tenant has complete control over the cloud environment.
- **Security:** Because the private cloud is not shared with any other users, this network tends to provide far greater control, privacy and security — as long as the user has adopted a comprehensive security strategy specifically designed for the cloud.

- Customization: In a private cloud model, organizations have complete control of their cloud environment and can customize their network to meet the organization's business needs or comply with regulatory standards.

- **Performance:** Because the private cloud is not a shared resource, most users benefit from higher performance.

- **Flexibility:** As your infrastructure changes based on business needs, a private cloud can keep up with it without an issue.
- **Cost:** Using a private cloud is almost always more expensive than using a public cloud because the organization either has to build and run their own network, or pay a third-party to do so on their behalf.

  IT burden: Most private cloud users require significant IT resources for setup, operation and maintenance of the cloud environment.

  Scalability: Private cloud users cannot scale or shift workloads between cloud environments as easily as public cloud users, which makes it difficult for organizations to introduce new services rapidly. However, the private cloud model offers enhanced scalability as compared to traditional on-premises infrastructure.
- **Remote access:** In most private cloud environments, remote access, as well as mobile access, is limited. Given recent workforce trends, as well as the effects of the COVID-19 pandemic, most private cloud networks do not support the needs of the modern workforce.
- **Mobile Access:** Because there are strong security measures protecting the private cloud, it is hard for mobile users to access it.

Cloud Storage Market Size, Share, Growth & Forecast

Source: *Fortune Business Insights*

Unlike many projects that exist only on paper, the cloud solutions we theorize have also been developed as regards the technical and software part, and IT security, by applying innovative solutions. From an initial analysis of the reports and projections regarding the development of the market, it seemed clear to us that we could not sit idly by, and we embarked on a path to become one of the main players in this market.

The global cloud storage market size was valued at USD 70.19 billion in 2021 and is projected to grow from USD 83.41 billion in 2022 to USD 376.37 billion by 2029, exhibiting a

CAGR of 24.0% during the forecast period. Based on our analysis, the global cloud storage market share had exhibited a higher growth of 13.8% in 2020 as compared to 2019. The global COVID-19 pandemic has been unprecedented and staggering, with the market experiencing higher-than-anticipated demand across all regions compared to pre-pandemic levels.

In the market study, we have considered cloud storage solutions offered by market players such as Amazon.com Inc' Amazon Simple Storage Service (S3) object storage, file storage including Amazon Elastic File System, Amazon FXs for Windows File Server, Amazon FXs for Lustre and Amazon Elastic Block Storage. Similarly, Oracle Corporation's file, block and object storage, archive storage, flash local storage and storage gateway, Google LLC's Filestore, Cloud archival storage, persistent disk, local SSD block storage, and cloud object storage.

The growth of the cloud storage is driven by several factors, such as the growing volume of unstructured data and increased demand for advanced technologies such as the internet of things, artificial intelligence, analytics, automation and others. Cloud storage stores and manages data on the internet and can be delivered on-demand and as per pay and use model. Also, cloud-based storage provides global scalability, agility, remote access and durability to data storage.

In June 2020, as per LogicMonitor's Cloud 2025 survey respondents, 95% of the IT workload will be on the cloud in the next five years. This factor indicates that the market is likely to showcase remarkable growth in the coming years. Also, the global market is to witness significant growth driven by the COVID-19 pandemic.

Market players are providing storage services to businesses to manage their remote employees. For instance, in July 2020, Google Cloud partnered with a cloud content management company, Box, Inc. The partnership aims to support customers to transform their remote workspaces with cloud-based data storage. Such active partnerships and collaboration activities are anticipated to propel the demand for cloud storage.

Adoption of Distributed Work Environment Owing to Spread of Novel Coronavirus to Drive Market Growth

The impact of COVID-19 is expected to result in considerably high market growth during the analysis period. The market's growth is attributed to the significant adoption of storage

services owing to virtual work and the growing volume of data. The market observed a significant growth rate of 13.7% in 2020 compared to 9.3% in 2019.

Cloud-based solutions enable employees to collaborate and stay connected as firms move toward a remote work environment. The COVID-19 pandemic accelerated the adoption of cloud storage with the increased proliferation of collaboration and conferencing applications by the remote workforce.

In August 2020, PWC stated cloud spending grew by 37% in the first quarter of 2020. Further, it stated that spending is expected to rise in the next 12 months across pharmaceuticals and biotechnology industries, forestry and paper products, automobiles, beverages and food, household and personal use products, chemicals, banks, and other financials, constructions, and IT and Telecommunications.

Hence, market players focus on offering scalable and cost-effective storage solutions to tackle increased network traffic and unprecedented data growth. For instance,

- In December 2020, Oracle Cloud-managed the COVID-19 Vaccination program of the U.S. The partnership aims to help the U.S. public health agencies accumulate and evaluate COVID-19 data.

Thus, the partnership and collaborations fuel the market growth during the COVID-19 pandemic. The growing data volume surges the demand for cloud infrastructure. The increasing investment by prominent market players to develop data centers worldwide in response to the COVID-19 pandemic is anticipated to drive the market in coming years.

- For instance, in June 2020 - Microsoft Corporation expanded its data centers in May 2020 across Italy, Poland and New Zealand with the growing demand for cloud services in the wake of COVID-19.
- In April 2020 – Amazon.Com Inc. launched a cloud data center in Italy during the COVID-19 pandemic. The new data center provides support to remote learning and working and empowers research.

Thus, the growing investment by cloud providers to develop data centers is expected to create significant market opportunities for market growth post-pandemic period.

Last trends

Cloud analytics creates ample opportunities for cloud providers due to the increasing demand for analytical insights for decision-making across various industries. The demand for additional data storage to support a massive data volume is growing exponentially due to the

substantial computing power. Enterprises leverage platforms and deliver advanced storage technologies with more accessibility and flexibility.

Similarly, social media analytics encouraged end-users to adopt cloud-based automated data storage services to provide real-time improved customer experience. For instance, in October 2020, Facebook LLC partnered with a Cloud service provider, Backblaze. The partnership focused on transferring the social media videos and images over the cloud-based encrypted storage to maintain security and privacy. These technological trends are expected to fuel the market size in the coming years.

Driving factors

Remote sensing, the Internet of Things (IoT), and improved video quality such as 4K or 8K resolution cameras have resulted in the collection of large amounts of data. As a result, demand for cloud-based storage and networking technology is increasing. Similarly, the growing use of artificial intelligence (AI) is projected to increase storage demand to improve data security.

For example, in February 2021, NextBillion AI, a California-based start-up, collaborated with Google Cloud to improve time-to-market solutions using cloud SQL and storage. The partnership aims to offer data protection and 99 percent uptime for NextBillion artificial intelligence clients.

Additionally, connected devices and autonomous systems such as self-driving cars are likely to drive the adoption of cloud computing services, including data storage for providing real-time assistance.

For instance, in February 2021, Ford Motor Company, a connected car manufacturer, partnered with Google Cloud to improve the customer experience with connected vehicles. The company is moving towards digitalization with automatic and driverless cars. The company aims to offer an enhanced experience by implementing machine learning, automation and cloud across vehicles. Such factors are expected to drive the market towards a higher growth trajectory.

Restraining factors

Stringent Laws and Regulations Associated with Privacy and Data Security May Impede the Market Growth, however, the limiting factor of the invasion of privacy will particularly affect our major competitors who in the past have been guilty of violations on this aspect, and will strengthen our project which, being a private and trustless cloud, proves to be an effective tool for protecting of sensitive data.

Data privacy and confidentiality are the most vital elements of the cloud storage ecosystem. The stringent government laws and regulations on using the cloud are expected to restrict market growth. For example, the Government of India made a provision in the Information Technology Act 2000. According to the provision, any unlawful activities related to the computing models/transactions consisting of confidential data or information will be subjected to a penalty. Such rules and regulations enforced by governments are likely to hamper market growth.

As the data resides outside the company's infrastructure, it is apparent that the company may loss control over data. Even though the concerns are largely psychological and hypothetical, due to the immaturity and lack of awareness of cloud services, especially in developing and underdeveloped regions, consumers may have genuine concerns regarding the service provider's capability and operational processes. Privacy and security concerns are projected to act as barriers to adopting cloud-based storage.

Segmentation

By the component, the market is divided into storage models and services. The storage models, including block storage, object storage and file storage, are projected to hold the maximum market share. Block storage is expected to hold a major market share due to increased demand for reliable and high-performance storage during the forecast period.

The file storage cloud is anticipated to grow with the highest CAGR owing to its increased storage capacity. For instance, in February 2021, Nasuni Corporation, a file cloud data storage provider, collaborated with Google Cloud. The increased demand for enterprise file storage played a vital role in the partnership.

Storage models help organizations tackle fundamental requirements such as availability, data security, and durability. These factors are projected to drive the adoption of cloud-based data storage among enterprises. At the same time, services such as training, installation, support, maintenance and others help maintain connectivity and data flow, which is expected to drive the demand for services in coming years.

The market is divided into three types of deployment such as public cloud, private cloud and Hybrid cloud. The public cloud segment is expected to account for a major market share due to growingpublic cloud spending. The growing end-user spending in the public cloud will accelerate market growth in the coming years.

The private cloud is expected to exhibit steady growth during the projected period owing to the improved security offering and protection of confidential data.

The hybrid cloud is projected to gain sturdy growth due to increased demand for hybrid deployment as enterprises can benefit from private and public deployments. Thus, the surge in demand for hybrid cloud storage due to data security, flexibility, and agility will likely foster market growth. Organizations will rely on multiple public clouds, private cloud legacy platforms, and on-premises to fulfill the infrastructure needs. The hybrid multi-cloud provides control and visibility over the infrastructure, which helps to access and secure files. These factors are expected to increase the demand for hybrid cloud-based storage.

Based on the enterprise size, the market is bifurcated into large enterprises and small & medium enterprises (SMEs). Large enterprises are expected to account for a maximum revenue share due to the increased demand for cloud-based storage to manage large amount of remote workforce and data.

The growing adoption of infrastructure as a service, software as a service, and platform as a service by the organizations to manage the virtual work during the COVID-19 pandemic accelerated the demand for cloud-based storage. For instance, in February 2022, as per the EY-Nasscom cloud survey, 67% of the large organizations accelerated cloud adoption, while 38% of small organizations embarked on their cloud journey.

The small and medium enterprises are expected to showcase a higher growth rate during the forecast years. According to Flexera 2021, State of the Cloud Report, 86% of respondents stated that small and medium-sized enterprises adopted the cloud higher than planned during covid-19, likely to drive market growth.

Vertical Analysis

The market is classified into banking, financial services and insurance (BFSI), healthcare and life science, IT and Telecommunication, manufacturing, government and public sector, media and entertainment, retail and consumer goods, and others.

The BFSI industry to gain traction owing to the digitalization of banking and financial services such as online banking, mobile wallets, digital payment, net banking and others. This factor drives the demand for secure storage models. The market players are offering secure storage solutions to the banking and financial institutions, which is expected to surge the partnership

and collaborations between cloud providers and financial service providers. For instance, in February 2021, Global Financial Services partnered with Google Cloud. The collaboration aims to tackle data and security threats of its banking infrastructure using an AI-based platform.

Healthcare and life sciences are anticipated to showcase a remarkable growth rate. Cloud services help get real-time health data insights and minimize the IT complexities with storage solutions. The patient's data stored in the cloud can be accessed from anywhere and at any time. Besides, the growing adoption of advanced technologies such as virtual reality and augmented reality in healthcare generates a huge volume of data per day. Thus, digitalization in the healthcare and life science industry creates a demand for scalable data storage. The key players are focusing on introducing cloud-based services to the healthcare industry to improve the productivity of healthcare professionals.

For instance, in December 2020, Amazon.com Inc. launched a cloud-based storage and data management service, HIPAA-eligible HealthLake, for healthcare professionals. The HealthLake assists in reducing healthcare professionals' time required to transform and analyze health data in real-time. Such a growing introduction of advanced services is expected to drive the market across this industry.

The surge in demand for video streaming and over-the-top services (OTT) accelerated the adoption of cloud-based storage services across telecom service providers. Similarly, government and public sector, manufacturing, retail and consumer goods, among other industries, are actively investing in cloud-based data management services and software, which is expected to fuel the market across these industries.

Geographical areas

The market has been classified into five major regions, including North America, Europe, Asia Pacific, the Middle East and Africa, and Latin America. The regions are further divided into countries.

North America is projected to dominate the market throughout the forecast period. The U.S. holds the major market share attributed to the presence of major cloud providers and a large number of data centers. Further, the growing adoption of smart home devices, connected

devices, video streaming services, and digital payments generates heaps of data every day. These huge volumes of data create the demand for cloud data storage across the U.S.

Canada is expected to grow with the highest CAGR during the forecast period owing to growing investment by organizations to implement cloud-based services and solutions. According to January 2021, CDW Cloud Report, more than half of enterprises (52%) in Canada have already made a plan on making investments in cloud-based infrastructure and services to ensure consistent service delivery. COVID-19, which forced many enterprises to recognize the drawbacks of on-site solutions and data centers, fueled the adoption.

The Asia Pacific is anticipated to showcase the highest growth rate during the projected period. The growing investment by developing economies such as India, Japan, Singapore, South East Asia, South Korea, and others contribute to market growth. The government initiatives to drive digital transformation across the countries fuel the adoption of cloud technology across the region.

For instance, in July 2021, the Deloitte report 'The imperative cloud Asia Pacific's unmissable opportunity, stated that public cloud spending was USD 19.45 billion in 2020 is expected to rise to USD 67.64 billion by 2024 in China. It also stated that the total Asia Pacific annual spending on public cloud is expected to reach USD 116.06 billion in 2024 from USD 43.14 billion in 2020. These factors are expected to fuel the demand for cloud-based storage across the Asia Pacific countries.

Europe is likely to gain a significant market share due to government initiatives to fuel cloud adoption across organizations and governments. In December 2021, as per Eurostat, 68% of the European Union enterprises used cloud computing services to store files 2021, and 42% of the enterprises used cloud computing across the organization.

Besides, 75% of enterprises in Sweden and Finland will adopt cloud computing in 2021. The increased adoption of cloud computing across Nordics is expected to create new market opportunities for the European cloud storage market growth in the coming years.

The Middle East and Africa are projected to show potential market growth in coming years owing to growing investment by cloud providers to establish data centers across the region. For instance, Oracle Corporation launched the cloud region in Saudi Arabia in 2021, Abu Dhabi in 2022, and Dubai and Jeddah in 2020. Similarly, the rising smartphone penetration and improved network connectivity across the region are expected to foster market growth.

South America is expected to witness steady growth owing to growing investment by Brazil, Argentina, Chile, and Columbia governments to improve digitalization across the countries. COVID-19 pandemic surged the adoption of digital technologies, smartphones and digital banking across the region.

For instance, in October 2020, Mastercard stated that 40 million people from Latin America opened bank accounts amid a pandemic. Further, in October 2020, IT spending in Latin

America is expected to grow by 7.7% in 2021, and the IT industry rose by 5.5% in 2020. These factors are anticipated to propel market growth.

Key industry players

Key Market Players to Enhance their Product Offerings and Adopt Partnership Strategies to Achieve Organizational Goals:

Being a fragmented market, key market players such as Amazon.com, Inc., IBM Corporation, Oracle Corporation, Alibaba Group Holding Limited, VMware Inc., and Microsoft Corporation are likely to expand their product offerings. By expanding their product lines, these companies are ensuring to increase the revenue share. Also, it is likely to enable them to take advantage of the market opportunities across different sectors. Strategic partnerships are likely to promote the business expansion of market players. For instance, in August 2019, IBM Corporation enhanced its software portfolio to make it cloud-native and compatible to run on Red Hat OpenShift.

It should be noted that the main actors have almost all been convicted of privacy violations in the past and therefore have little credibility in this area. Their massive advertising investment aimed at creating a clean image makes them believe they can compete on the market using their own logo and brand, currently no one seems to have bothered to create parallel brands that are not easily connected to companies already involved in privacy violations and user profiling, but in reality companies that value their data as extremely important will never rely on a public cloud, and in any case, the corporate security manager is never inclined to share company documents with external companies, becoming the cloud privacy the only acceptable solution in terms of security and privacy.

April 2020 – Microsoft Corporation partnered with Blackrock, Inc., an investment management corporation. The partnership aims to host Aladdin infrastructure provided by Blackrock Solutions on the Azure cloud platform. Blackrock brings improved capabilities to its Aladdin platform using the Microsoft Azure cloud platform.

March 2021: Oracle Corporation launched new Cloud Lift Services to help customers quickly migrate through its tools and engineering resources. The new platform removes critical barriers and offers single contact points, high speed, and more. This development is helping in accelerating customer growth through Google Cloud support.

Worldwide cloud service spend to grow by 23% in 2023

Source: *Canalys, 8 February 2023. Canalys is an independent analyst company that strives to guide clients on the future of the technology industry and to think beyond the business models of the past. We deliver smart market insights to IT, channel and service provider*

professionals around the world. We stake our reputation on the quality of our data, our innovative use of technology and our high level of customer service.

Worldwide cloud infrastructure services expenditure grew 23% year on year in Q4 2022 to reach US$65.8 billion, an increase of US$12.3 billion. For full-year 2022, total cloud infrastructure services spend grew 29% to US$247.1 billion, up from US$191.7 billion in 2021. The quarterly growth rate slowed, down over 10 percentage points from Q1 2022 (34% in Q1 2022 against 23% in Q4 2022). Rising public cloud costs, fueled by inflation, are forcing enterprise customers to optimize public cloud spend after constant IT investment over the past three years in digital transformation. Macroeconomic uncertainties are contributing to a more conservative approach to IT budgets. A growing number of customers are adjusting cloud strategies for greater efficiency and control. That includes assessing the repatriation of certain cloud workloads to private or co-location data centers to reduce costs, driving greater adoption of hybrid and multi-cloud strategies. While enterprise demand for cloud services persists, the growth rate for cloud infrastructure services will continue to slow for the next few quarters. In 2023, Canalys expects global cloud infrastructure services spend to increase by 23% for the full year, compared with 29% in 2022.

The realities of worsening macroeconomic conditions and the looming recession prompted a slowdown in the volume and pace of migration to the cloud in Q4, especially by enterprise customers, which typically have larger workloads. The hyperscalers were inevitably affected, with their growth falling by about 5 percentage points from the previous quarter. The top three in Q4 2022, AWS, Microsoft Azure and Google Cloud, collectively grew 26%, to account for a combined 65% share of customer spend.

“Enterprise customers are responding to higher cloud prices and higher-than-expected operating costs under the tough macroeconomic conditions,” said Canalys Research Analyst Yi Zhang. “Customers that are currently on pay-per-use billing models will optimize cloud activities to reduce cloud consumption and save costs. There will also be a considerable slowdown in the take-up of cloud contracts, which will also result in a decrease in associated cloud revenue.”

“Customers are rethinking how they use cloud in their business operations,” said Canalys VP Alex Smith. “In some cases, there is a natural slowdown in compute demand as core operations see less activity. In addition, conservative budgeting among businesses will lead to less experimentation during the next 12 months.”