## Cloud Client desktop

Funzioni

1. Sincronizzazione in real time delle cartelle con il Cloud remoto
2. Backup giornaliero (il PC necessita di un HD aggiuntivo per evitare che la rottura del disco provochi anche la perdita del backup)
3. Backup per il versioning  (avviene in automatico quando un file viene modificato, il backup viene creato nell'HD aggiuntivo)
4. Creazione di identità digitale, firma digitale di documenti PDF e validazione della firma.
5. Mirroring su percorso di rete. Il path Cloud può essere mantenuto in copia in real time su un percorso di rete in maniera analogo ad un sistema RAID 1, con la differenza che il mirroring essendo in rete mette in sicurezza l'azienda contro la perdita di dati dovuta al furto del computer.
6. Account decentralizzato: Salvataggio e recupero dell'account tramite passphrase, con tecnologia derivata dai wallet Bitcoin

## Private Cloud home consumer

Dispositivo per la sincronizzazione dei file in remoto, crea un sistema analogo a OneDrive o DropBox ma privato, ovvero i dati non sono in mano a terze aziende, ma custoditi nel proprio device in quale è collegato al client con criptazione di livello militare tramite 2 possibili protocolli: Socket criptato, o una nostra implementazione Rest API alla quale è stato aggiunto un livello di criptazione alla request HTML che non è presente nel protocollo standard.
Ci si può collegare al Cloud tramite:

- Applicazione desktop che fa la sincronizzazione in real time
- Applicazione mobile che consiste in un file explorer che permette di salvare e scaricare i file in Cloud
- Pagina web statica (file explorer per il browser, con funzioni di "drag & drop" per la gestione dei file nel cloud).

## Cloud enterprise

Si tratta di un Cloud stand alone, con sistema operativo e installato su server dedicato, con funzioni di scalabilità dedicato alle aziende. In particolare:

1. È possibile creare e montare on fly da 0 a N Cloud (con il limite dello spazio delle unità di disco).
2. Creare on fly dei sotto Cloud di area, ad esempio, se una azienda ha al proprio interni dipartimenti diversi (marketing, ricerca e sviluppo, commerciale e vendite), è possibile creare per ciascun dipartimento un Cloud posizionato in un ramo del Cloud principale in modo che i membri del dipartimento siano circoscritti in un area ristretta rispetto al Cloud principale, mentre invece il management aziendale ha accesso tramite la connessione al Cloud principale

posto alla radice. I sotto Cloud a loro volta possono avere dei sotto Cloud per creare delle aree ristrette di lavoro.

3. Funzione di backup giornaliero dei dati.
4. È possibile fare il parring di due cloud enterprise posti in località geografiche differenti (esempio Europa e Usa): In tal caso i Cloud accoppiati avranno gli stessi dati sincronizzati in real time: Funzione utile per il disaster recovery in caso l'azienda in cui è custodito il cloud venga distrutta da una inondazione o incendio che fisicamente andrebbe a distruggere il server e tutte le copie di backup dentro l'azienda.
5. Mirroring dei dati su percorso di rete.
6. Creazione on fly di PIN usa e getta per dare accesso al Cloud: Il PIN generato permette la creazione di una identità digitale per connettersi al Cloud, alla quale l'amministratore di rete assegna un nome. Il proprietario della identità digitale, la può esportare su un'altra macchina tramite passphrase (in maniera analoga di come avviene con i wallet Bitcoin, la tecnologia sottostante è la stessa).
7. Funzioni avanzate di auto diagnostica risoluzione dei problemi: Il Cloud enterprise necessita di un sistemista per la messa in funzione, il mantenimento e assistenza: Siccome l'infrastruttura può avere diversi modelli di configurazione, il Cloud al suo interno ha già tutti i test di auto diagnostica per individuare tutte le tipologie di problemi che potrebbero insorgere a causa della configurazione della infrastruttura.

## Proxy criptato

E una implementazione proprietaria di un sistema proxy che supporta un livello di criptazione per il quale il proxy non diventa trustless: A differenza del proxy o della VPN tradizionali, I dati transitano criptati in maniera nativa e continuano in criptato fino al cloud senza che la macchina su cui è installato il proxy abbia la possibilità di vedere la trasmissione in chiaro. In una VPN tradizionale I dati sono criptati fino alla macchina che fa da VPN poi da li in avanti viaggiano comunque in chiaro.
L'idea è quella di tenere tutta l'infrastruttura Cloud all'interno di una intranet aziendale, senza che sia direttamente esposta all'esterno (ad internet), ed esporre solamente il proxy che funge così da macchina sicura come gateway trustless per il traffico di dati proveniente dall'estero e permetta quindi la connessione di client alla infrastruttura con un alto livello di sicurezza.

## Router di messaggistica

Il router di messaggistica è una macchina logica che permette di gestire il traffico dati in maniera trustless (tutto il traffico è criptato dalla sorgente al punto di destinazione e il router non ha modo di vedere in chiaro il traffico passante). Il router permette anche l'instradazione di messaggi a gruppi logici di macchine, dispositivi su rete precaria mobile, e verso dispositivi con IP dinamico, È stato creato per gestire comunicazioni per applicazioni equivalenti a Telegram, o Signal, una sola macchina può gestire centinaia di migliaia di dispositivi client e il traffico da essi generato, la particolarità di gestire anche pacchetti a livello binario (oltre a audio, testi, immagini), lo ha reso lo strumento cardine per collegare fra loro client e server e instradare il traffico generato in ogni condizione.

Il Router può lavorare in simbiosi con il Proxy criptato dato che quest’ultimo è un device client per il router.
A livello logico è possibile personalizzare qualsiasi infrastruttura collocando più di un router e proxy all’interno in base alle esigenze infrastrutturali, La soluzione Cloud enterprise nella stessa macchina unisce Cloud server, Router e Proxy in modo da avere una soluzione già pronta, ma sono possibili soluzioni ad hoc per adattarsi a progetti differenti e policy di sicurezza aziendali personalizzate.

## Acquisizione di dati telemetrici

Abbiamo creato delle library di basso livello che possono essere integrate su piccoli device ARM low cost (~20€), per connettere l’internet delle cose al router o per effettuare l’acquisizione acquisire il flusso di dati telemetrici dalle apparecchiature industriali.

I dati telemetrici vengono criptati e vengono instradati in real time presso qualsiasi tipo di dispositivo o gruppo logico, come ad esempio verso il Cloud, verso dispositivi mobile, verso altri Device, anche con condizioni precarie di connessione, o IP dinamico, e persino tramite differenti tipologie di connessione (TCP, radio, GSM, RS232, ecc), uno spooler interno si preoccuperà di far giungere dati a destinazione indipendentemente dalla qualità della rete e presenza di connessione al momento della acquisizione.
Il livello sicurezza adottato, per quanto riguarda la privacy della comunicazione è di tipo militare.