Kryptoteknologi

Kan det være måten å realisere en drøm om å gi eierskap av egne data tilbake til kunden?

Av:
ANDERS REKVE
M.Phil Teknologi, Innovasjon og Kunnskap UiO, Ansatt Turner & Townsend. Utleid til europeisk kunde som prosjektleder for implementasjon av nytt designkonsept i Norden.

ANTONIO MARCUS LAAKE
MSc Finance (Cass Business School), Master I Risikostyring og analyse UIS, Diplomøkonom BI (økonomi og administrasjon), Senior Analytiker/Manager Risikostyring Konsern i Gjensidige med over 13 års arbeidserfaring fra finans, risikostyring, risikomodellering og governance

Forberedelser til innføringen av GDPR (det nye personvernsdirektivet) har det siste året ført til tildels omfattende gjennomganger av bedriftens rutiner for å sikre etterlevelse av det nye regelverket. Parallelt har det i løpet av det siste året også skjedd en utvikling i bruk av kryptovalutaer som til eksempel Bitcoin, Ethereum, m.fl. Siden kryptovalutaer går for å være en hel del sikrere enn andre lignende løsninger, finnes det noen gode løsninger på GDPR problematikk innenfor kryptoteknologi? Er det for eksempel mulig å nyttiggjøre seg av kryptorelaterte løsninger for å kunne sikre sensitive kundedata?

Maidsafe

Det amerikanske sikkerhetsselskapet Identillect Technologies tror at det er mulig å anvende kryptoteknologi for å tilfredsstille GDPR-kravene. I mars 2018 inngikk Identillect Technologies en lisensieringsavtale med det skotske selskapet Maidsafe der de sammen tar sikte på å utforske bruken av Maidsafe sin teknologi for å løse problemstillinger relatert til GDPR.

Maidsafe sitt produkt er et nytt *autonomt* nettverk «SAFE Network». Et autonomt nettverk styrer og administrerer seg selv uten mulighet for menneskelig påvirkning. Det finnes ingen tredjeperson som kan hackes, påvirkes eller kompromitteres for å få ulovlig tilgang på data. Data du har lastet opp er kryptert og distribuert over nettverket med avansert kryptering. Nøkkelen som dekrypterer dataene har aldri forlatt enheten du lastet dataene opp fra. Det er ingen som kan tyvlytte eller hacke tredjepersoner på internett på leting etter tilgang til dine data. Det er som et nettverk lagd for GDPR: Ingen kan få tilgang til dataene med mindre du eksplisitt har gitt noen tilgang til den.

Maidsafe er en forkortelse av ordene *Massive Array of Internet Disks, Safe Access For Everyone.* Målet til Maidsafe er å lage et nettverk, «SAFE Network», som nyttiggjør seg av ledig lagringskapasitet på allmenhetens internett-oppkoblede elektroniske enheter. Hvis Maidsafe:

1. Finner en måte å koble enhetene sammen til et stort nettverk
2. insentiviserer folk til å stille enhetene sine til disposisjon til fellesskapet

– da har man i praksis oppnådd et fungerende *Massive Array of Internet Disks.*

Hvis Maidsafe i tillegg:

3. lager en løsning som er teknisk sikker som gjør at folk er villig til å lagre dataene sine på andre mennesker sine enheter - da har de også oppnådd *Secure Access For Everyone.*

Maidsafe er allerede på god vei til å gjennomføre dette. De har arbeidet over 10 år med FoU; neste iterasjon av testnettverket (Alpha 3) er ventet snarlig, og de har sikret seg flere defensive patenter på teknologien sin, samtidig som de skalerer opp organisasjonen for økt produksjon av datakode og tilrettelegging for eksterne applikasjonsutviklere.

Fordeler ved bruk av Massive Array of Internet Disks

Et hav av ledig kapasitet

Hvis du tenker deg om, hvor mange elektroniske enheter har du hjemme som er

INSPIRASJON TIL TV-SERIE

Richard Hendricks (Thomas Middleditch) i den amerikanske situasjonskomedien og tv-serien Silicon Valley. Teknologien i forretningsideen til Richard sitt fiktive selskap «Pied Piper» er basert på SAFE Network.

Figure 1: https://spectrum.ieee.org/view-from-the-valley/telecom/wireless/a-2-million-contest-seeks-a-real-world-pied-piper

koblet opp mot internett? De fleste av oss har kanskje en smarttelefon, bærbar PC, lese-/nettbrett, stasjonær datamaskin, en smartTV, osv. Estimatene spriker litt, men ett estimat sier at det innen 2020 vil være over 30 milliarder oppkoblede enheter. Alle estimater viser en enighet om at antallet vil øke betydelig de neste årene. Det er dette som er *Internet of Things (IoT)*, på norsk Tingenes internett.

Felles for alle enhetene er at utnyttelsesgraden av disse er forholdsvis lav. De fleste bruker kanskje bærbar PC og mobil flittig. Men om natten, ca. en tredjedel av døgnets 24 timer, så ligger begge oftest ubrukt. Og selv om de er i aktiv bruk, belastes ikke enhetene 100% hele tiden. Så hva hvis delingsøkonomien kunne bli brukt for å utnytte denne ressursen? Aggregert vil de utgjøre en betydelig reserve i form av lagringsplass og prosessorkraft. Dette er ressurser som kan stilles til nettverkets disposisjon til en marginal kostnad for den enkelte som er tilkoblet nettverket. Dette fordi enheten er allerede:

1. betalt for, så det innebærer ingen innkjøpskostnad som må nedbetales
2. skrudd på, så den konsumerer bare marginalt mer strøm ved økt utnyttelsesgrad
3. koblet til internett som i de fleste tilfeller har en fast kostnad uavhengig av bruk.

Enheter som er koblet sammen i «SAFE Network» vil dermed kunne yte tjenester til brukere av nettverket for en kostnad lik den økte kostnaden et marginalt høyere strømforbruk representerer. Sett i kontrast med kostnaden ved å lagre data i datasentrene der

1. Det må investeres i bygging av datasenteret, infrastruktur og maskinvare
2. Driftskostnader inkluderer kostnader til sikkerhet, redundans, kjølingskostnader osv.

så er merkostnaden i form av høyere strømforbruk på eksisterende digitale enheter beskjeden i forhold. På en annen side blir eierne av enhetene kompensert i form av «SAFE Network» sin kryptovaluta «safecoin». Så lenge denne kompensasjonens kroneverdi tilsvarer eller er høyere enn den økte strømkostnaden, så er individet insentivisert til å stille enhetene sine til disposisjon.

Data lagres én gang

Det finnes millioner av duplikater av filer lastet opp på nettet. Se for deg en liten videosnutt som går viralt. Etter kort tid ligger denne videoen lagret på servene til flerfoldige nettsteder; Facebook, blogger, osv. En fil på 10MB duplisert 1.000 ganger ender opp med å oppta 10GB med total lagringsplass. Ifølge Åse Dragland i Sintef ICT ble 90% av verdens data produsert de siste 2 årene (i 2013). Hvor mye av dette er lagret i duplikater på internett?

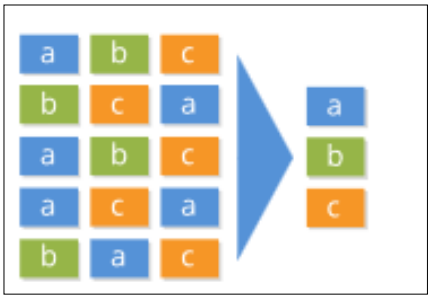
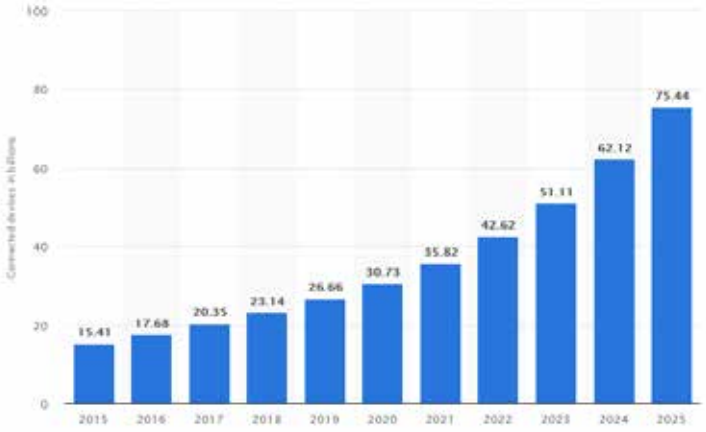


Figure 2: https://maidsafe.net/features.html

På «SAFE Network» lagres unike filer kun en gang. Når brukere lagrer en fil som allerede ligger på nettverket, så vil brukerne bli referert til filen som allerede ligger på nettverket. Dette skjer ved at nettverket tar et fingeravtrykk, «hash», av filen



Tingenes internett (IoT)

Wikipedia beskriver IoT som «et nettverk av oppkoblede fysiske enheter, kjøretøy, husholdningsapparater og andre ting som inneholder elektronikk, programvare, sensorer, aktuatorer og nett-oppkobling som muliggjør at enhetene kan kommunisere og utveksle informasjon».

Figur 1: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

du ønsker å lagre på nettverket – og sjekker om fingeravtrykket allerede ligger på nettverket.

Effektivitet

SAFE Network tar i bruk *delingsøkonomien* for å skaffe tilgang til ressurser og utnytter ubenyttet kapasitet til enhetene i Tingenes Internett. Samtidig sørger teknologien for at data ikke blir lagret i duplikater - som effektiviserer lagring ytterligere. Resultatet er ett nettverk som kan stille nettverksressurser til disposisjon til en langt lavere ressurskostnad enn dagens arkitektur som er avhengig av store datasentre.

I tillegg til mindre ressurskrevende lagring, bidrar SAFE Network med mindre ressurskrevende sikkerhetsopplegg for den enkelte bedrift som må etterfølge GDPR. Datasikkerhetsfunksjonene som muliggjør etterlevelse etter GDPR er en sentral egenskap av nettverket. En kan tenke seg at spesielt for nykommere vil det være interessant å se hvordan SAFE Network kan senke inngangskostnadene til å tilby tjenester innenfor etablerte segmenter – der konkurrentene har gjort betydelige organisasjonsmessige og materielle investeringer.

Sikkerhet: Blokkjede vs. SAFE Network

Sikkerhet og lagring i blokkjede

SAFE Network og blokkjede er ikke direkte sammenlignbart. De utfører forskjellige funksjoner. Ved hjelp av blokkjede kan man etablere en uforanderlig historikk over hendelser uten å være avhengig av en sentral autoritet som verifiserer at hendelsene tok sted (som en bank ville gjort med transaksjoner). Den iboende *sikkerheten* i blokkjede er at ingen skal kunne endre historikken om hva som har hendt. For eksempel er det svært vanskelig å endre på transaksjonshistorikken til Bitcoin.

Blokkjede er «en voksende liste med databaser kalt «blokker» som er lenket sammen ved hjelp av kryptografi» ifølge Wikipedia. Forenklet består den kryptografiske lenken i at hver blokk inneholder et «hash» av den foregående blokken.

Det er svært vanskelig for en uærlig aktør å endre på data som er skrevet inn i blokkjeden. Hvis en uærlig aktør ønsker å gjøre en endring på transaksjonene som ligger i databasen til blokk #32, så vil «hashen» av blokk #32 som ligger i blokk #33 ikke lenger stemme. Da vil heller ikke «hashen» av blokk #33 som ligger i blokk #34 stemme. Og så videre. Se tekstboksen i denne artikkelen for et inntrykk av hva selv den minste forandring i den underliggende dataen betyr for den assosierte «hashen».

HVA ER EN HASH?

En hash kan fungere som et fingeravtrykk av data, uten å avsløre hva slags data det er snakk om. Dette skjer ved hjelp av spesielle hash-funksjoner som til eksempel Secure Hash Algorithm (SHA). I eksemplene under blir setningene «hashet», og vi får en «hash» (et fingeravtrykk av setningen) representert med tall og bokstaver. Legg merke til endringen i «hashen» (fingeravtrykket) der kun en bokstav endres i setningen.

SHA1(«The quick brown fox jumps over the lazy dog»)
= 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12

SHA1(«The quick brown fox jumps over the lazy cog»)
= de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3

Eksempel hentet fra Wikipedia, https://no.wikipedia.org/wiki/SHA-sjekksumsfunksjoner, 25.04.2018

> «Blockchain´s killer app is bitcoin, the rest is mostly pure marketing»
>
> *-David Irvine, Maidsafe*

Blokkjede er uovertruffen til å skape en uforanderlig historikk. Men den fungerer dårlig til lagring av data. Databasen til hver blokk i blokkjeden har kun kapasitet til en veldig begrenset mengde informasjon. Det er ikke realistisk å lagre et bilde til en blokk i en blokkjede, men noen tusen linjer med tekst går fint.

Det siste året har det vært en «hype» der blokkjede har vært løsningen som lette etter problemer å løse. Det kan være greit å opplyse om at kypto-sfæren består av mer enn kun blokkjede. Blokkjede er en fantastisk teknologi for å skape desentraliserte og sikre betalingsløsninger, men dårlig på svært mye annet.

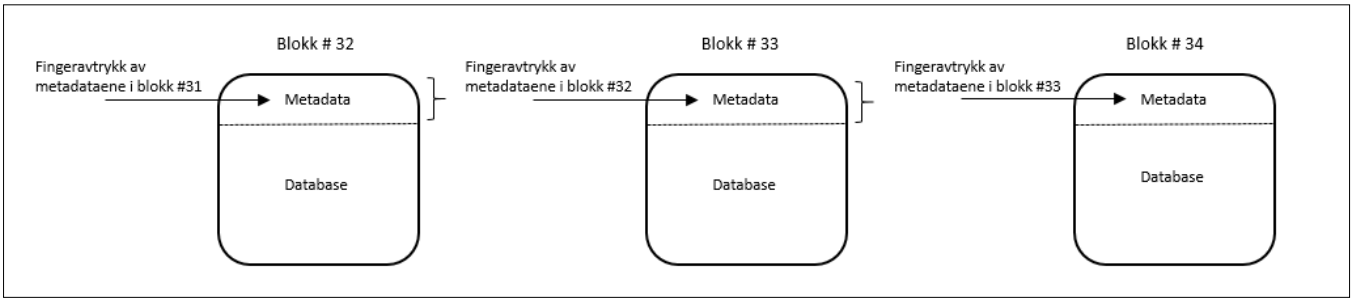


Figure 3: inspirert av https://www.pluralsight.com/guides/software-engineering-best-practices/blockchain-architecture

Sikkerhet og lagring i SAFE Network

SAFE Network er et autonomt nettverk, der nettverket styrer og administrerer seg selv. Det er et desentralisert nettverk uten et sentralt sted som en uærlig aktør kan angripe for å påvirke nettverket. Det regulerer selv hvor, hvordan og når data blir lagret. Det regulerer selv prisen den kompenserer enhetene i nettverket slik at det alltid er et tilstrekkelig tilbud av ressurser i reserve. Ingen kan vite hvilke enheter og hva slags data ligger lagret, selv ikke nettverket selv. Datasikkerhetsmessig fjerner dette kanskje den største kilden til at data kommer på avveie: Det er ingen mennesker til å begå feil, kompromitteres eller ødelegge med vilje.

Hvis du tar et bilde med telefonen din og ønsker å lagre dette på nettverket, så deles bildet først opp i flere mindre biter. Deretter krypteres det med to svært sikre krypteringsmetoder, der nøkkelen for å dekryptere bildet aldri forlater telefonen din. Etter dette blir de krypterte bitene av bildet lastet opp til tilfeldige enheter på nettverket.

Siden passordet ikke forlater telefonen, betyr det at passordet ikke er lagret et annet sted. Dette betyr igjen at:

1. Ingen kan tyvlytte på kommunikasjonen din for å finne passordet
2. Ingen kan hacke stedet der passordet ditt er lagret
3. Ingen har nøklene til dataene utenom personen som lastet opp dataene.

I 2012 ble Linkedin hacket, og rundt 6.5 millioner passord ble stjålet av hackere. Disse passordene sammen med brukerinformasjon kan igjen åpne opp for at uvedkommende får tilgang til brukerkontoer andre steder. Slike scenarioer er ikke mulige på SAFE Network, da det ikke finnes et sentralt mål for hackere å angripe. Passord og brukerinformasjon er ikke lagret noe sted unntatt på enheter kontrollert av brukeren. Hvis passord kommer på avveie, så er det sannsynlig som følge av brukerfeil.

«SAFE Network» og GDPR – En mulig løsning

Grunntanken er at kundens sensitive data hele tiden ligger på «SAFE Network» og aldri er i bedriftens kontroll. Bedriften tilrettelegger for at kunden kan legge til sine data til «SAFE Network» og gi bedriften midlertidig lesetilgang til denne. Dette gjøres ved hjelp av en applikasjon som bedriften har utviklet ved hjelp av utviklerverktøyene til Maidsafe. Bedriftens applikasjon abstraherer vekk kompleksiteten ved SAFE Network for kunden. Den sørger for at kunden innehar reelt og faktisk eierskap til dataene sine. Den sørger også for å strukturere informasjonen som bedriften er interessert i, på samme måte et hvilket som helst skjema ville gjort.

Når det er nødvendig for å fullføre en gitt forretningsprosess etterspør bedriften lesetilgang på relevant data fra kunden. Det er kunden som kontrollerer informasjonen hele veien, og det er kundens ansvar å administrere tilgangskontroll til denne informasjonen. Når forretningsprosessen er overstått sitter bedriften igjen med produktet av forretningsprosessen, men ikke dataene som inngikk i den.

En kan spørre seg om ikke dette ville latt seg gjøre uavhengig av «SAFE Network»? Kan ikke bedriften be om at kunden oppbevarer dataene sine hos en ekstern leverandør av skylagringstjenester? Begge tilfeller resulterer i at kundedata er lagret utenfor bedriftens systemer. Og på samme måte som i eksempelet ovenfor, så etterspør bedriften lesetilgang til kundens data når den trenger det.

Forskjellen ligger i at kundedata lagret hos underleverandør er data i bedriftens kontroll, og dermed også ansvar for med tanke på datasikkerhet. Kundedata på «SAFE Network» ligger innenfor kundens kontroll.

Utvikling fremover

Personene bak «SAFE Network» har store ambisjoner. Det er spennende å se systemer som knytter sammen såpass mange utviklingstrekk i dagens samfunn: Generelt fokus på eierskap og kontroll av data; et autonomt og desentralisert nettverk; *kryptografisk* sikret data; nyttiggjøring av *delingsøkonomien* for å skaffe til veie ressurser i *Tingenes Internett* (IOT) samt nye metoder for å lagre data uten duplikater som igjen adresserer den massive økningen i dataproduksjon. Den fiktive COO til «Pied Piper» Jared Dunn i den amerikanske situasjonskomedien og tv-serien *Silicon Valley* uttrykte det på en veldig bra måte – se boksen.

Konklusjon

I disse tider blir Facebook beskyldt for å lagre for mye av våre data og selge de videre til tredjepersoner. Vi leser om nettsteder som blir hacket og sensitiv kundedata som kommer på avveie. Personlige data er blitt en ettertraktet ressurs for legitime og illegitime aktører. Gitt denne bakgrunnen er det spennende å få øynene opp for alternative måter å organisere data på slik at individet – kunden - du selv - eier og forvalter egne data. I sammenheng med innføringen av GDPR blir det spennende etter hvert å se hvordan kryptoteknologier kan utvikle seg til å være en løsning av utfordringer - med en tilsvarende stor mulighet for innovasjon av varer og tjenester. Kanskje vil dette ikke være den første og siste gangen du hører navnet «SAFE Network» og utnyttelsen av kryptoteknologi i personvernsammenheng?

I AM SURE YOU ARE AWARE OF THE GREAT LONDON HORSE MANURE CRISIS OF 1894?

In the 1890s the industrial revolution had people flocking to the city. And more people equals more horses and more horses equals manure. And it was predicted that by the middle of the next century there would be 9 feet of manure covering the streets. But what no one saw coming was a new technology that would completely obliterate those concerns - the car. Overnight the manure problem vanished.

And the internet as we currently know it is rife with identity theft and SPAM and hacking - so it is manure. And we believe that in success, our new entirely decentralised internet will be just as significant as the car.

«Pied Piper» sin COO Jared Dunn (Zach Woods)