Big data og Cyberkriminalitet

En litteraturstudie om hvordan Big Data kan brukes for å bekjempe cyberkrimialitet

HÅKON BERGEM OG ØYSTEIN TRASKJÆR

VEILEDER
Dag Håkon Olsen

Universitetet i Agder, 2019
Fakultet for Samfunnsvitenskap
Institutt for Informasjonssystemer

Forord

Denne masteravhandlingen er et avsluttende produkt av en studie gjennomført i faget IS-501 Masteroppgave i Informasjonssystemer ved Universitet i Agder, våren 2018. Formålet med studien er å belyse nåværende status på forskningsområdet Big Data og cybersikkerhet, samt avdekke trender i nyere forskning. Bakgrunnen for studien er temaets høyaktuelle status hvor cyberangrep stadig øker i omfang og kompleksitet, samt utviklingen av Big Data og dens bruksområder. Denne kombinasjonen fant vi veldig interessant og ønsket å lære mer om. Studien er utarbeidet av Håkon Bergem og Øystein Traskjær som en del av deres mastergrad i Informasjonssystemer ved Universitet i Agder.

Vi vil gjerne takke vår veileder, Professor Dag Håkon Olsen, ved Universitet i Agder, for kontinuerlig støtte og veiledning gjennom hele prosessen. I tillegg retter vi en takk til Anette Cecilie Bergem og Eivind Bergem for et kritisk, eksternt blikk på vår masteroppgave, samt hjelp til korrekturlesing.

Kristiansand, 03.06.2019

Håkon Bergem

Øystein Traskjær

Sammendrag

Cyberkriminalitet er et økende problem i samfunnet og hackerangrep blir stadig mer komplekse og sofistikerte. Bruken av Big Data som et forvarsverktøy mot angrep er et revolusjonerende steg i utviklingen av sikkerhetssystemer og har enormt et potensial for å oppdage angrep og trusler mot et data- eller nettverkssystem.

I denne masterutredningen er det utført en litteraturstudie som tar for seg aktuell tidligere forskning om temaet Big Data og cyberkriminalitet for å kartlegge hvor langt forskningen har kommet på akkurat dette området. Studien ønsker å bidra med å belyse sentrale trender innen Big Data og cyberkriminalitet de siste seks årene, samt avdekke eventuelle forskningshull hvor ytterligere forskning er nødvendig.

Vår problemstilling er følgende:

"Hva sier litteraturen om bruken av Big Data for å bekjempe cyberkriminalitet, og hvilke trender fremkommer i nyere forskning?"

Bakgrunnen for valget av problemstilling skyldes masterstudiets fokus på Big Data, samt dagsaktuelle nyhetssaker hvor store aktører opplever at deres datasystemer blir angrepet og skadet. Denne typen angrep forårsaker skader for flere milliarder årlig. På bakgrunn av dette ønsket vi å se nærmere på Big Data i et sikkerhetsperspektiv og hvordan Big Data kan bli brukt for å bekjempe cyberkriminalitet.

Studien identifiserte 37 relevante artikler om Big Data og cyberkriminalitet publisert etter 2013. Studiens funn har blitt delt opp i tre hovedkategorier: Utfordringer, foreslåtte løsninger og trender. Totalt 13 utfordringer og 9 foreslåtte løsninger ble identifisert i studien, samt trender som preger forskningen de siste 6 årene.

Studien har avdekket at det eksisterer trender innen nyere forskning. Da spesielt IDS som dominerer forskningsfeltet, men også litt mindre markante trender som visualisering av Big Data systemer, redusering av data og bruken av rammeverk og systemdesign. Dette er alle trender innen foreslåtte løsninger.

Videre viser funnene i studien en rekke utfordringer som blir nevnt hyppig i litteraturen. Av utfordringer er det verdt å nevne blant annet "zero-day attacks", Big Data prosessering, identifisering av avvik/anomalier og konfigurering av maskinlæringsalgoritmer.

Innholdsfortegnelse

Figurliste

Tabelliste

1 Introduksjon

1.1 Bakgrunn

Big Data er et emne som har vekket interessen vår i løpet av vårt masterstudium i informasjonssystemer, og dermed et forskningsområde vi ønsket å se nærmere på. Bruksområdene og potensialet for teknologien gjør det i våre øyne til et meget interessant og spennende felt hvor vi ønsket å tilegne oss mer informasjon og kunnskap. Samtidig er IT-sikkerhet et dagsaktuelt tema hvor store skandaler preger nyhetsbildet som for eksempel WannaCry viruset (Sarmadawy, 2017), hackingen av Hydro (Tomter & Gundersen, 2019) eller skandalen hvor norske politikere ble rammet av et hackerangrep, og personlig passord og brukernavn ble spredt åpent på nettet (Johannessen & Åsebø, 2017).

Med nåtidens digitaliseringstrend hvor "alt" skal over på nett og bort fra penn og papir, er bedrifter og organisasjoner ekstra utsatt for angrep på deres nettverk og systemer, og fokus på IT-sikkerhet er større en noensinne (Bronson, 2018). Cyberkriminalitet er under rask og voksende utvikling og forsvar mot dette krever nye komplekse metoder for å holde følge. Dette ga oss ideen om å forske på nye metoder for videreutvikling av sikkerhetsløsninger for å bekjempe og forsvare mot cyberkriminalitet med bruk av Big Data.

1.2 Problemstilling

Da vi i utgangspunktet ikke hadde noen utfyllende erfaring og kunnskap om kombinasjonen Big Data og cyberkriminalitet ble det utfordrende å definere en spesifikk problemstilling med en konkret teori. Vi valgte derfor å velge en utforskende studie hvor hensikten var å etablere en oversikt over nyere forskning innen Big Data og cyberkriminalitet, samt hvilke trender som fremkommer i litteraturen. Vår problemstilling ble som følger:

"Hva sier litteraturen om bruken av Big Data for å bekjempe cyberkriminalitet, og hvilke trender fremkommer i nyere forskning?"

For å besvare problemstillingen har vi i denne studien benyttet oss av en litteraturstudie, nærmere bestemt en systematisk litteraturgjennomgang, hvor målet var å kartlegge forskningen på området de siste seks årene. Denne metoden ble valgt på

bakgrunn av tilgang til data da studien ble gjennomført. En detaljert forklaring av metoden blir presentert i kapittel 3.

1.3 Motivasjon

Big Data har vært et sentralt tema gjennom hele vår studieperiode på Universitetet i Agder innen IT- og informasjonssystemer, både på bachelor og masternivå. Vi har derfor begge fattet interesse for teknologien og hvilke bruksområdet som er aktuelle for Big Data. I den seneste tiden har det kommet frem flere tilfeller hvor cyberkriminelle har kommet seg forbi eller rundt sikkerheten til store organisasjoner. Nyere tilfeller er lekking av bilder fra snapchat (Kleinman, 2014), eller løsepengeangrepet på Hydro i 2019 (Tomter og Gundersen, 2019). Det virker ganske tydelig at dagens standard innen cybersikkerhet ikke er et godt nok forsvar mot den stadig voksende cyberkriminaliteten. Dette i kombinasjon med fokuset på cybersikkerhet de seneste årene, både i skolesammenheng og nyheter/media, gjorde det interessant for oss å se nærmere på bruken av Big Data satt opp mot cybersikkerhet.

1.4 Hensikten med studien

Denne litteraturstudien tar for seg aktuell tidligere forskning om temaet Big Data og cyberkriminalitet for å kartlegge hvor langt forskningen har kommet på akkurat dette området. Studien ønsker å bidra med å belyse sentrale trender innen Big Data og cyberkriminalitet de siste seks årene, samt avdekke eventuelle forskningshull hvor ytterligere forskning er nødvendig.

1.5 Begrepsavklaringer

I dette kapittelet vil vi forklare en del ord og begreper som fremkommer i litteraturen for å gjøre det enklere å forstå innholdet som blir presentert videre i denne masteravhandlingen.

1.5.1 Hva er Big Data?

Big data er teknologi og analysemetodikk knyttet til datamengder som er for store og komplekse for tradisjonelle databehandlingssystemer. Big Data karakteriseres ved de 5 V'ene, hvorav de 2 siste har blitt lagt til i senere tid*: volume, variety, velocity, veracity,*

value(BBVA, 2017). Det varierer hvor mange av Véne som blir brukt i litteraturen. Noen forsikningsstudier forholder seg kun til 3 av Véne, mens andre bruker opp til 7. Disse 5 V'ene representerer de ulike aspektene ved Big Data, slik som store datamengder, forskjellige formater og strukturer, hyppigheten av data, nøyaktigheten av data, samt verdien data kan tilby.

I lang tid har Big Data vært forbundet med kundesegmentering og markedsføring. Begrepet har vært i vinden lenge, og det strides enda om en enhetlig definisjon av begrepet. Big Data er en ting for noen, og en annen ting for andre.

Det finnes ikke en enstydig definisjon av begrepet Big Data. Definisjonene som finnes benyttes om enten en eller flere aktiviteter, og betydningen av begrepene er vage. Den hyppigste brukte definisjonen av Big Data er at den referer både til data i seg selv, og aktiviteten knyttet til å samle inn, lagre og analysere den (Datatilsynet, 2013).

Én definisjon som ofte går igjen er at "... *Big Data er en samling av datasett som er så store og komplekse at de vanskelig lar seg lagre, håndtere og analysere av tradisjonelle databasesystemer",* (Grodzinski, 2013) mens en annen definisjon lyder følgende: "*Big Data er en samling av data fra tradisjonelle og digitale kilder i, og utenfor et firma, som representerer en kilde for pågående oppdagelse og analyse."* (Arthur, 2013)

EU - kommisjonens rådgivende organ i personvernspørsmål, Artikkel 29 - gruppen, definerer Big Data slik: "*... Big Data refererer til den enorme økningen i tilgang til, og automatiserte bruk av, opplysninger: det refererer til gigantiske mengder digitale data som er kontrollert av selskap, myndigheter og andre store organisasjoner, og som gjøres til gjenstand for omfattende analyse ved bruk av algoritmer. Big Data kan bli brukt til å identifisere generelle trender og sammenhenger, men kan også bli benyttet slik at det berører enkeltindivider direkte*." (Datatilsynet, 2013, s. 7). Med utgangspunkt i denne definisjonen legger vi til grunn at begrepet Big Data omfavner både prosessen med å samle inn data, og analysedelen hvor maskinlæring og kunstig intelligens ofte blir brukt for å gjøre nytte av data.

En av de store fordelene med Big Data er muligheten for å håndtere både strukturert, ustrukturert og semistrukturert data. Ved hjelp av algoritmer blir data lagret og kategorisert slik at data kan utnyttes til analyse og gi verdi til dataeier i form av ny innsikt. Big Data brukes blant annet til å utføre prediksjonsanalyser, studere brukeroppførsel, identifisere mønster, fremtidig trender, overvåke IT-systemer osv.

1.5.2 Cyberangrep og cybersikkerhet

Et cyberangrep referer til et skadelig angrep som potensielt kan skade en datamaskin eller et datasystem som fremkommer på bakgrunn å ha skaffet seg uautorisert nettverkstilgang, skadelig data eller kode injeksjon (Theoh et al., 2018). Den vanligste

formen for cyberangrep er såkalt "*malware*", eller *skadevare* som kommer i mange forskjellig former. De vanligste er virus, trojanske hester, bakdører og "rootkits".

Et *virus* er et tilsynelatende harmløst program som er i stand til å lage kopier av seg selv og injisere disse kopiene inn i andre programmer og filer for å forårsake skade. En *trojansk hest* er programvare forkledd som godartet kode som venter på at et offer skal installere programmet den er forkledd som. Den trojanske hesten inneholder noen skjulte funksjoner som oftest er destruktiv mot datamaskinen eller datasystemet så lenge applikasjonen kjører. En *bakdør* er en metode for å omgå en autoriseringsprosedyre eller -system, som oftest for å få uautorisert tilgang til et nettverk. Når først en skadevare har infiltrert en datamaskin eller et system er det viktig for den å forbli ubemerket. Et "*rootkit*" blir da brukt for å modifisere systemets *fastvare* ("firmware") slik at skadevaren fremstår som godartet. Slike angrep kan identifiseres ved å for eksempel bruke maskinlæring for å skanne systemlogger og lete etter anomalier, men dette kommer vi nærmere tilbake på i kapittel 4.

Cybersikkerhet referer til oppgaven med å beskytte seg mot nevnte angrep gjennom å kontrollere fysisk maskinvare eller programvare.

1.5.3 Maskinlæring og kunstig intelligens

I Store norske leksikon skriver Elster & Tidemann (2017) at begrepene maskinlæring og kunstig intelligens blir ofte brukt om hverandre. *Kunstig intelligens* omfatter alle intelligente systemer.

Maskinlæring er en underart, eller subkategori av kunstig intelligens. I det siste er synonymet dyp læring blitt mer populært.

Maskinlæring er en type kunstig intelligens som bruker statistiske metoder for å finne mønstre i store mengder med data. At maskinen lærer vil si at det trenes opp en modell ved bruk av data. Vanligvis deles data som brukes til læring opp i treningssett og testsett. Data i treningssettet blir brukt for å trene modellen opp til det den skal brukes til. Testsettet blir så testet på den opplærte modellen for å se om den har lært riktig. Data i testsettet er ukjent for modellen. Maskinlæring blir brukt til blant annet selvdrevne biler, epost-filtrering og bildegjenkjenning.

Maskinlæring blir delt opp i forskjellige kategorier:

- Veiledet læring
    - "Maskinen finner en ukjent funksjon fra eksempler. Den lærer å forstå at inngangsverdiene *forutsier* utgangsverdiene.

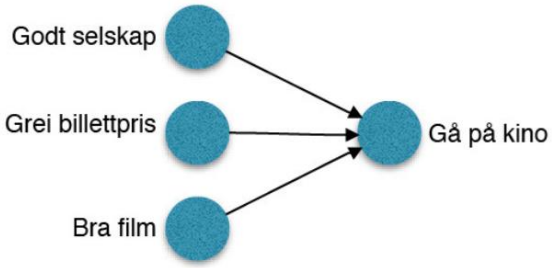
Et enkelt eksempel vil være å skille hunder fra fugler. Hunder har fire ben, mens fugler har bare to. I tillegg har fuglene vinger. Når modellen ser et dyr med fire ben, så kan den være sikker på at det er en hund. Likeledes, har dyret to ben og to vinger, er det mest sannsynlig en fugl. Dette kalles *klassifisering*. Hvis man i stedet prøver å forutsi lengden på dyret, altså et tall, kalles det *regresjon*" (Elster & Tidemann, 2017).

- Ikke-veiledet læring
    - "I dette tilfellet har maskinen ikke tilgang til utgangsverdier for gitte inngangsverdier. I stedet forsøker algoritmen selv å finne strukturen i inngangsverdiene, ved for eksempel å gruppere dem i klynger. Vi mennesker er ekstremt gode på dette, og på dette feltet har maskinlæring langt igjen for å nå menneskelig ytelse" (Elster & Tidemann, 2017).

Det finnes en tredje kategori kalt forsterket læring, men denne er ikke veldig relevant for de metodene av maskinlæring som blir brukt i våre utvalgte artikler og konferansepapirer.

1.5.4 Nevralt nettverk

"Et nevralt nettverk er en samlebetegnelse for datastrukturer, med tilhørende algoritmer, som er inspirert av måten nervecellene i en hjerne er organisert på." (Dvergsdal, 2019). Disse datastrukturene brukes for å finne sammenhenger hvor det kan være vanskelig å finne klare matematiske sammenhenger. For eksempel hva slags matvarer en person kommer til å kjøpe ut ifra hvordan været er. Nettverket tar beslutninger på samme måte som vi gjør det. Det blir satt inn variabler som er med på å danne argumenter og motargumenter. Hva man ender opp med til slutt er et resultat basert på dette. Figuren under viser et veldig enkelt nevralt nettverk for ett spørsmål om man skal på kino eller ikke.



Figur 1 Enkelt nevralt nettverk med argumenter for å avgjøre om man skal på kino eller ikke. (Dvergsdal, (2019).

1.6 Studiens struktur

Innledningsvis har introduksjon blitt presentert i form av bakgrunn, problemstilling, motivasjon, hensikten med studien og begrepsavklaringer. Videre vil vi redegjøre for studiens begrensninger, for deretter å presentere studiens metode og hvordan vi har utført søket etter litteratur. Videre følger presentasjon av artiklene som ble identifisert i studien, hvor vi tematisk legger frem utfordringer og løsninger som kommer frem i litteraturen. Deretter følger presentasjon av studiens funn hvor trender som fremkommer i litteraturen blir presentert, samt forskningshull. Avslutningsvis vil vi diskutere rundt funnene som ble gjort og deretter oppsummere resultatet av studien i en konklusjon, samt potensielle fremtidige-forskningsområder.

2 Tidligere forskning

I dette kapittelet vil vi kort presentere tidligere forskning på området Big Data og cybersikkerhet.

Basert på en tidligere litteraturgjennomgang fra 2013 har vi fått et godt innblikk i hvor langt forskningen har kommet på området. Litteraturgjennomgangen, skrevet av Mahmood & Afzal (2013) oppsummerer bruken av Big Data analyse i et sikkerhetsperspektiv og identifiserer trender, teknikker og verktøy innenfor litteraturen.

Artikkelen presenterer hvilke trusler og angrep som blir ansett som mest vanlig og som det er stort fokus på å beskytte seg mot. Dette inkluderer:

- Spamming
- Search poisoning
- Botnets
- Denial of Service (DoS)
- Phishing
- Malware
- Webside trusler (Sql injection, malwarereklame osv)

Tradisjonelle systemer baserer seg på signaturer for å gjenkjenne angrep. Med utviklingen innen cybertrusler og muligheten for komplekse angrep, som ikke tidligere er blitt brukt eller oppdaget, faller slike signaturbaserte systemer akterut. Fokuset har skiftet fra å fokusere på ondsinnede signaturer, til ondsinnede handlinger.

Mahmood & Afzal konkluderer med at cybersikkerhet er nå blitt et Big Data problem, hvor store mengder data av ulike formater og forskjellige kilder må analyserer og overvåkes for trusler og angrep. Tradisjonelle systemer er ikke egnet for denne oppgaven da dataene er for store og komplekse. Disse problemene fremheves gjennom fire punkter (Mahmood & Afzal, 2013):

- Bedrifter og organisasjoner utvider datanettverket deres for å tillate partnere og kunder å aksessere data på forskjellige måter for å legge til rette for samarbeid. Dette bidrar til å gjøre nettverk mer utsatt for cyberangrep. I tillegg har den utstrakte bruken av sky- og mobile løsninger også generert nye måter å utføre cyberangrep på.
- Big data er et attraktivt mål for angripere på jakt etter sensitiv informasjon. Dette har ført med seg en utvikling innen kompetansen til cyberkriminelle når

det kommer til å skaffe seg adgang og unngå tradisjonelle sikkerhetssystemer som signaturbaserte "*Intrusion Detection Systems"* (IDS) . Denne typen system er utdatert.

- På grunn av Big Data og utfordringene det medbringer vil det i noen tilfeller kun være mulig å hente ut en liten del av sikkerhetsinformasjonen. Eksempler på slik informasjon kan være nettverkslogger, *SIEM* (Security Information and Event Management) varsler, tilgangslogg osv. Det vil si at skade påført av et angrep kun kan bli oppdaget i etterkant av angrepet.
- Big Data hindrer det meste av sikkerhetsdata fra å bli analysert på grunn av kompleksitet og mengde. Data kan for eksempel komme fra forskjellige kilder i forskjellige formater eller generert i en hastighet og mengde som gjør det umulig å analysere for tradisjonelle analysemetoder, maskinvare eller programvare.

Introduseringen av Big Data analyse til bruk innen sikkerhet har revolusjonert måten man kan håndtere store mengder data og gjør det mulig å holde følge med Big Data problemene. Dette medfører følgende unike fordeler og egenskaper (Mahmood & Afzal, 2013):

- En mer agil tilnærming rundt beslutningstakning for nettverksledere med muligheten for overvåkning og monitorering og datastrømmer i sanntid.
- Dynamisk identifisering av både kjente og tidligere ukjente trusler og avvik i form av mistenkelig oppførsel, bruk av ressurser, tilgangsmønstre, transaksjon eller nettverkstrafikk osv.
- Effektiv identifisering av mistenkelig eller skadelig oppførsel (Lavest mulig falsk positivt sats).
- Muligheten til å håndtere og behandle skadelig oppførsel i sanntid.
- Passende dashboardbaserte visualiseringsteknikker for å tilby et helhetlig bilde av nettverket og problemer i sanntid.
- Passende maskinvare og programvare innen Big Data for å håndtere og leve opp til nevnte fordeler og egenskaper.

Sammenlignet med tradisjonelle analysemetoder tilbyr Big Data analyse et fyldigere bildet i form av kontekst ved å separere det "normale" fra det "unormale". For eksempel forskjellen i atferd fra en skadelig, kompromittert bruker til en vanlig bruker.

Big Data kilder kan kategoriseres som passive eller aktive. Eksempler på passive kilder er:

- Maskinbaserte data, for eksempel IP-lokasjon, tastaturtrykk, WAP data osv.

- Mobil basert data, for eksempel GPS-lokasjon, nettverkslokasjon, WAP data
- Fysisk data om bruker, for eksempel tid og lokasjon ved fysisk aksessering til et nettverk.
- HR (Human resources) data, for eksempel organisatorisk rolle og tilgang/autorisasjon til brukeren.
- Reisedata, for eksempel reisemønstre og reiseruter.
- SIEM data, for eksempel nettverkslogger.
- Data fra eksterne kilder, for eksempel ukjente IP adresser eller andre eksterne trusler

Eksempler på aktive kilder, relatert til sanntid, er:

- Brukerdata, for eksempel passord og brukernavn
- Engangspassord, for eksempel til bruk for tilgang til et nettverk
- Digitale sertifikater
- Kunnskapsbaserte spørsmål, for eksempel "Hva er din typiske aktivitet på Lørdager fra 15-18"?
- Biometrisk identifikasjonsdata, for eksempel fingeravtrykk, ansiktsgjenkjenning, stemmegjenkjenning, håndskriftsgjenkjenning.
- Sosiale medierdata, for eksempel Twitter, Facebook, interne kontornettverk e.l.

Analyse på både passive og aktive kilder fører til et 360 graders overblikk over nettverkstraffiken som gjør det mulig å oppdage og hente ut unormal oppførsel basert på eksisterende mønster til en bruker.

Mamhood & Afzal (2013) nevner et sett sentrale egenskaper for en sikkerhetsanalysemodell. Dette innebærer blant annet:

- Ulike datakilder
- Overvåkningssystemer
- Interaktive dashbord
- Avansert sikkerhetskontroll
- Robust sikkerhetsinfrastruktur
- Big Data Analytics motorer

De største bruksområdene for Big Data som et sikkerhetssystem ligger i å identifisere og overåke trusler samt hendelsesetterforskning. Fokuset ligger på å oppdage og kartlegge/lære både kjente og ukjente trusler for å bedre kunne identifisere skjulte trusler og predikere angrep med vesentilig høyere nøyaktighet. Bruksområder for et

slikt system er for eksempel å overvåke nettverkstrafikk, web transaksjoner, servere og brukerkontoer for å oppdage anomalier eller avvik som kan tyde på angrep.

3 Metode

Vi har valgt å følge Kitchenham & Charters metode for litteraturgjennomgang hvor prosessen består av tre hovedsteg med tilhørende understeg (Kitchenham & Charters, 2007):

- Planlegging
    - Identifisere behov
    - Utvikle en protokoll
- Utførelse
    - Samle studier
    - Velge ut studier
    - Vurdere studier på bakgrunn av et sett predefinerte kriterier
    - Datainnsamling fra studier
    - Datasyntese
- Evaluering

Planlegging - Identifisere behov

Vi startet med å diskuterer ulike temaer og teknologier som vi selv fant interessante for å finne en aktuell problemstilling for vår masteroppgave. Big Data har vært et sentralt tema gjennom hele utdanningen, så det falt naturlig å velge dette som utgangspunkt. Kombinasjonen med cyberkriminalitet oppsto etter å ha lest nyhetsartikler om WannaCry viruset og hvordan det utnyttet både tekniske og menneskelige svakheter for å infiltrere et nettverk. Første steg var å sjekke om det tidligere var gjort lignende litteraturstudier på området og om det eventuelt var hensiktsmessig for oss å velge denne kombinasjonen til en oppgave. Vi brukte både Google, Google Scholar og Scopus som søkemotorer for å finne litteraturstudier innen big data og cybercrime. To studier ble identifisert. Den første hadde en annen vinkling enn hva vi hadde planlagt, hvor fokuset var på hvordan Big Data ble utnyttet for cyberkriminalitet, altså å stjele sensitiv informasjon fra store datakilder som sosiale nettverk eller lignende. Vår vinkling var annerledes og fokuserte på hvordan Big Data kan forhindre eller bekjempe cyberkriminalitet. Den andre litteraturstudien tok for seg nøyaktig dette. Dog var denne

publisert i 2013, noe som ga oss muligheten til å gjennomføre en litteraturstudie begrenset til de siste seks årene.

Utførelse

Ved å følge de 5 stegene beskrevet under utførelse av Kitchenham & Charters (2007) har vi gjennomført en systematisk litteraturgjennomgang for å kartlegge nåværende status på forskningsområdet Big Data og Cyberkriminalitet. *En systematisk litteraturgjennomgang* brukes for å systematisk samle og oppsummere bevis knyttet til en problemstilling (Kitchenham, 2004), men kan også brukes for å identifisere potensielle gap i forskning, såkalte forskningshull, som illustrerer behov for videre forskning der det er nødvendig.

Samle studier

Å identifisere studier relatert til vår problemstilling var første steg i Kitchenham & Charters (2007) metode under utførelse. Vi valgte å begrense oss til artikler publisert de siste seks årene, dette for å oppfylle kravet om behov, med fokus på relevante teknologier og ulik bruk av Big Data for å bekjempe cyberkriminalitet. Dette inkluderer blant annet maskinlæring/kunstig intelligens. Vi valgte å bruke Scopus som hoveddatabase da dette ble anbefalt fra foreleser i faget IS-420 Aktuelle tema og forskningsområder innen informasjonssystemer, og ansees som en anerkjent database med publikasjoner fra de mest renommerte journalene og konferansene. Et utvalg søkeord ble brukt for å finne relevante artikler, denne prosessen er beskrevet i detalj i kapittel 3.1.

Velge ut studier

I litteraturstudier er det helt sentralt å vurdere relevansen til studier som er identifisert (Kitchenham, 2004). På bakgrunn av dette gjorde vi et grovutvalg av artiklene identifisert i forrige steg. Ved å lese tittel, underoverskrift og abstrakt ble artikler med relevans til problemstilling valgt med videre, mens de artiklene som ble vurdert til å ha lite relevans ble valgt bort.

Vurdere studier på bakgrunn av et sett predefinerte kriterier

For å sikre ytterligere relevans og kvalitet på artiklene ble en mer grundig gjennomgang utført. Artiklene ble lest i fulltekst for å få fullstendig oversikt over hva de ulike artiklene omhandlet, og deretter filtrert med et sett predefinerte kriterier. Artikler som

ikke oppfylte kriteriene ble valgt bort. Denne prosessen sikret at samtlige gjenstående artikler var av høy kvalitet og relevans.

Datainnsamling fra studier

Kitchenham (2004) anbefaler en metodikk hvor mengde, type og intervaller av data som hentes ut defineres på forhånd. Vi har ikke vektlagt dette i stor grad i vår oppgave, men heller fokusert på trendene som kommer frem i data. For å identifisere slike trender ble samtlige artikler analysert for tema, problemstilling, løsninger/utfordringer, og deretter plottet inn i en konseptmatrise. Kategoriene i konspetmatrisen ble opprettet dynamisk etterhvert som vi leste gjennom alle artiklene. Samtlige artikler har derfor vært like viktig i prosessen med datainnsamling, mens vi i neste steg har vektlagt de artiklene som omhandler de største trendene de siste seks årene innenfor Big Data og cyberkriminalitet.

Datasyntese

Det siste steget av utførelse består av å oppsummere funn og resultat fra hele prosessen (Kitchenham, 2004). Dette ble gjort ved å presentere artiklene tematisk, samt trekke sammenhenger mellom artiklene for å eventuelt oppdage nye funn, for eksempel forskningshull. Trender ble som tidligere nevnt vektlagt, men også mindre "populære" forskningsområder og vinklinger blir omtalt. Resultatet av datasyntesen er en komplett konseptmatrise samt omfattende oppsummering av funn i litteraturen. Konseptmatrisen ble utviklet dynamisk etterhvert som vi jobbet oss gjennom listen med artikler, og kategorier ble lagt til eller fjernet etter behov. Matrisen ble delt inn i 3 hovedkategorier. "Cyberkriminalitet" viser til hvilken spesifikk cyberkriminalitet som blir fokusert på i studiene. "Utfordringer" presenterer hvilke utfordringer som kommer frem i litteraturen, og "foreslåtte løsninger" viser til hvilke løsninger som blir brukt i studiene, eller som blir foreslått til videre forskning. Slik føler vi å ha konstruert en oversiktlig og presentabel matrise hvor all nødvendig informasjon kommer godt frem. Matrisen ligger vedlagt som vedlegg 1, 2 og 3.

3.1 Oppsummering av søk i Scopus

Søkeord, antall treff og begrensninger som ble brukt er presentert under i tabell 1. Kolonnene "søkeord" og "sekundært søkeord" inneholder termer eller søkeord som ble brukt i søket vårt. Dette står også i rekkefølge etter hva vi søkte på først og sist. Kolonnen "Begrensninger" inneholder de begrensningene vi satt i Scopus under søk. Til slutt viser kolonnen "Treff" antall treff på de forskjellige søkene. Det første søket ga oss

55 treff, noe som er for lite stoff å basere seg på. Søk nummer to ga oss 5980, dette er store mengder med artikler og det er ikke gjennomførbart for oss å gå gjennom alle disse. Vi satte så sammen disse søkene for å spesifisere og filtrere slik at vi treffer artikler og konferanser med mest mulig fokus på både cyberkriminalitet og sikkerhet. Dette søket samsvarer også bedre med vårt forskningsspørsmål.

Vi brukte derfor følgende søkestreng i Scopus:

TITLE-ABS-KEY("big data" AND cyber AND crime AND security) AND DOCTYPE(ar OR cp) AND PUBYEAR > 2013

Med denne søkestrengen fikk vi totalt 149 treff. Resultatet fra søket ble som følger:

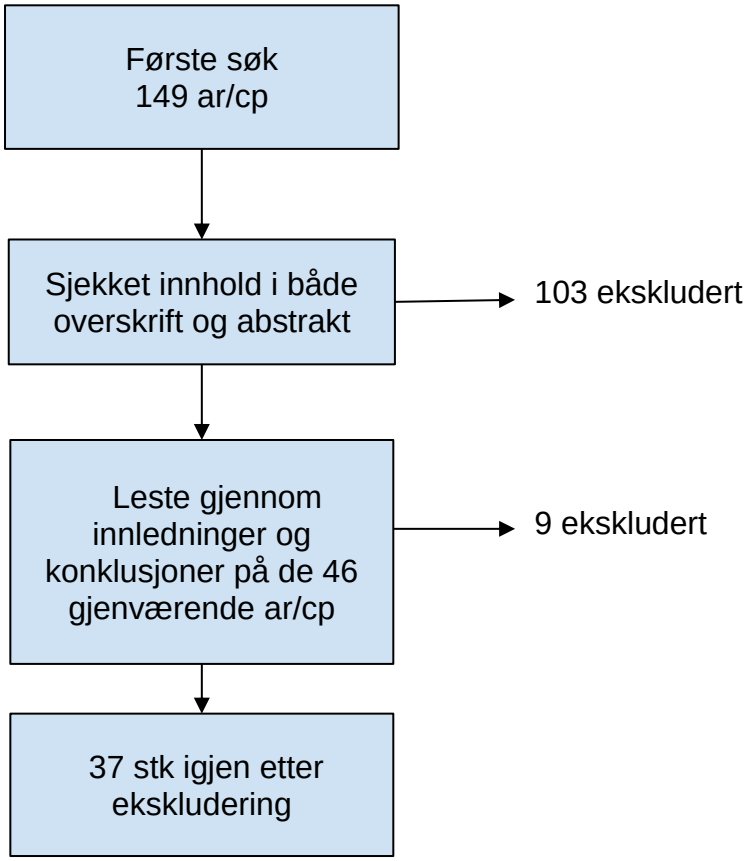
Tabell 1: Søkeord

NR	Søkeord	Sekundært søkeord	Database	Begrensninger	Treff
1	Big-data	AND cybercrime	Scopus	Peer-reviewed, engelsk, ar/cp, år 2013 til i dag	55
2	Big-data	AND security	Scopus	Peer-reviewed, engelsk, ar/cp, år 2013 til i dag	5980
3	Big-data	AND cybercrime AND security	Scopus	Peer-reviewed, engelsk, ar/cp, år 2013 til i dag	149

Vi begrenset søkeordene til tittel, abstrakt og nøkkelord, slik at vi ikke fikk opp artikler med lite relevans til vårt tema. Som dokumenttype begrenset vi oss til artikler og konferansepublikasjoner. Prosessen med å filtrere ut lite relevante artikler startet med at vi leste gjennom abstrakt til hver enkelt artikkel for å få en oversikt over hva de ulike artiklene tok for seg. Hvis innholdet oppfylte våre inkluderingskriterier, lagret vi artikkelen. Denne prosessen ble repetert til vi hadde gått gjennom hele listen med artikler.

3.2 Vurdering av studier

Vi ønsket å ytterligere forbedre litteraturgrunnlaget vårt og sørge for god kvalitet og relevans. Derfor gjennomførte vi en kvalitet- og ekskluderingsvurdering basert på Kitchenham (2004). Denne vurderingen fungerer som en utvalgsprosess hvor vi tar artiklene gjennom flere steg med kriterier. Denne prosessen er fremstilt i figuren under.



Figur 2 Ekskluderingsprosess

Når vi startet kvalitetsvurderingen tok vi utgangspunkt i alle treff vi hadde i starten av utvelgelsesprosessen. Dette var 149 artikler og konferanseartikler. Siden vi gikk ut fra et søk som gav oss 149 treff var dette en håndterbar mengde med artikler og konferanseartikler. Vi gikk derfor gjennom overskriftene og abstraktene til alle artiklene og konferanseartiklene for å sjekke relevans. I tilfeller hvor det var usikkerhet ble introduksjon og konklusjon sjekket allerede her. Denne fasen ekskluderte 103 artikler hvor 46 ble tatt med videre. Etter en nøyere gjennomgang av de 46 gjenstående artiklene satt vi til slutt igjen med 37. Et lite antall av artiklene vi fant kostet penger og ble derfor utelukket da vi ikke fikk tilgang til fulltekst, kun abstrakt. Denne prosesessen er illustrert i tabell 2

Tabell 2. Utfyllende kriterier. Bergem & Traskjær (2018, s. 8)

Kriterier	Begrunnelse
Tilgang til fulltekst	For å kunne lese hele artikkelen var vi avhengig av å ha tilgang til fulltekst. De artiklene som lå bak betalingsmur grunnet manglende lisenser hos UiA, ble valgt bort. Prosessen ved å ekskludere slike tilfeller besto av to steg: Sjekket tilgjengelighet gjennom Scopus. Søke etter artikkelnavn på Google/Google scholar. Hvis artikkelen ikke ble funnet gjennom disse to stegene ble den ekskludert fra studien.
Peer/reviewed artikler og journaler med fokus på informasjonssystemer	Vi ønsket å finne artikler eller konferanseartikler fra forskere eller journaler med fordypning i informasjonssystemer. Vi passet også på at disse var peer-reviewed. Innholdet på Scopus er peer-reviewed og passer derfor til dette kriteriet.
Tittel med relevans til søkeord.	Effektiv metode for å identifisere artikler med relevans til vårt forskningsspørsmål. Artikler med relevant eller interessant tittel ble inkludert.
Abstrakt med god relevans til forskningsspørsmålet.	Artikler med god relevans til vårt forskningsspørsmål ble valgt ut for å dekke det litteraturområdet vi ønsker å se nærmere på.
Innledning, resultater og konklusjon samsvarer med vårt forskningsspørsmål.	Artikler og forskningsartikler må ha som utgangspunkt å gå i dybden på ett eller flere tema som vi ser på som relevante for forskningsspørsmålet.

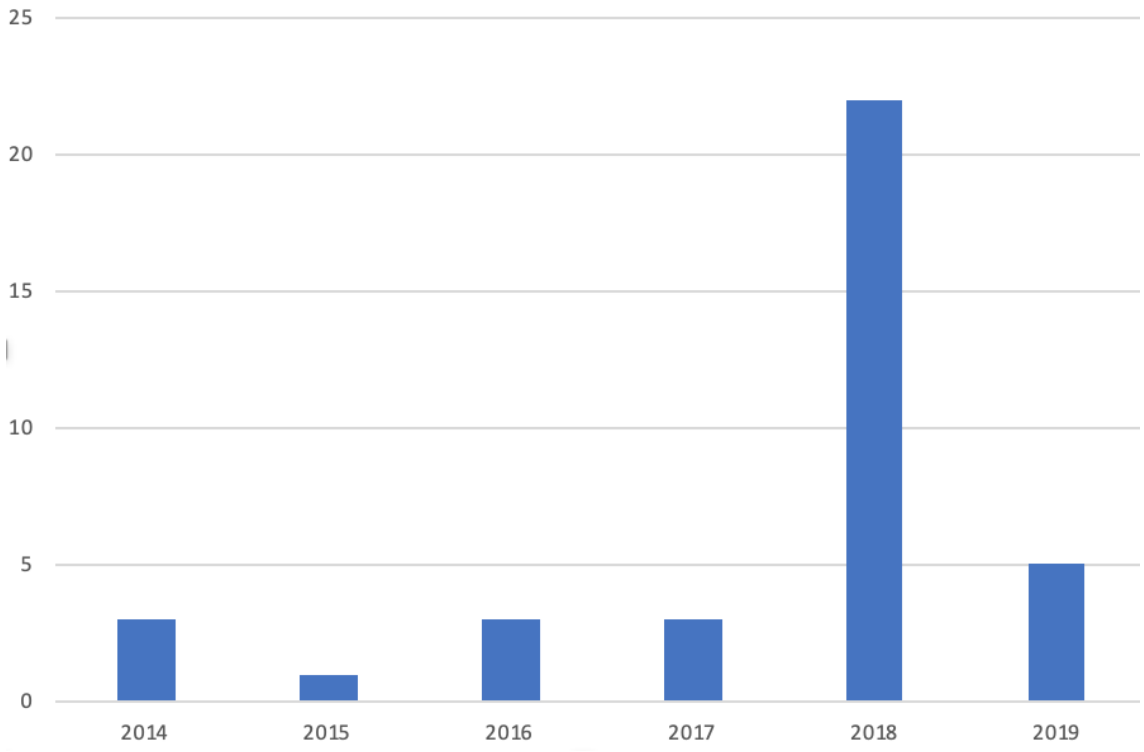
4 Presentasjon av artikler

I dette kapittelet har vi gjennomført en meta-analyse av artiklene i studien for å få et overblikk over hvilke data artiklene gir oss.

Vi stilte sprøsmål som for eksempel; “Hvilke universitet publiserer mest innen Big Data og cyberkriminalitet?” og “Ser vi en utvikling i antall publikasjoner de siste årene?” m.m. En meta-analyse kan hjelpe med å besvare slike spørsmål og på den måten vise om temaet er aktuelt, i utvikling eller opplever en nedgang innen forskningen. Videre presenterer vi hva Big Data er og hvilke bruksområder teknologien har samt andre teknologier som ofte blir brukt i denne sammenhengen og noen begrepsavklaringer. Deretter tar vi for oss de ulike artikkelen tematisk hvor trender som fremgår i litteraturen blir vektlagt. Delkapitlene tar utgangspunkt i kategoriene brukt i konseptmatrisen for å danne en sammenheng mellom denne og teksten.

4.1 Metaanalyse

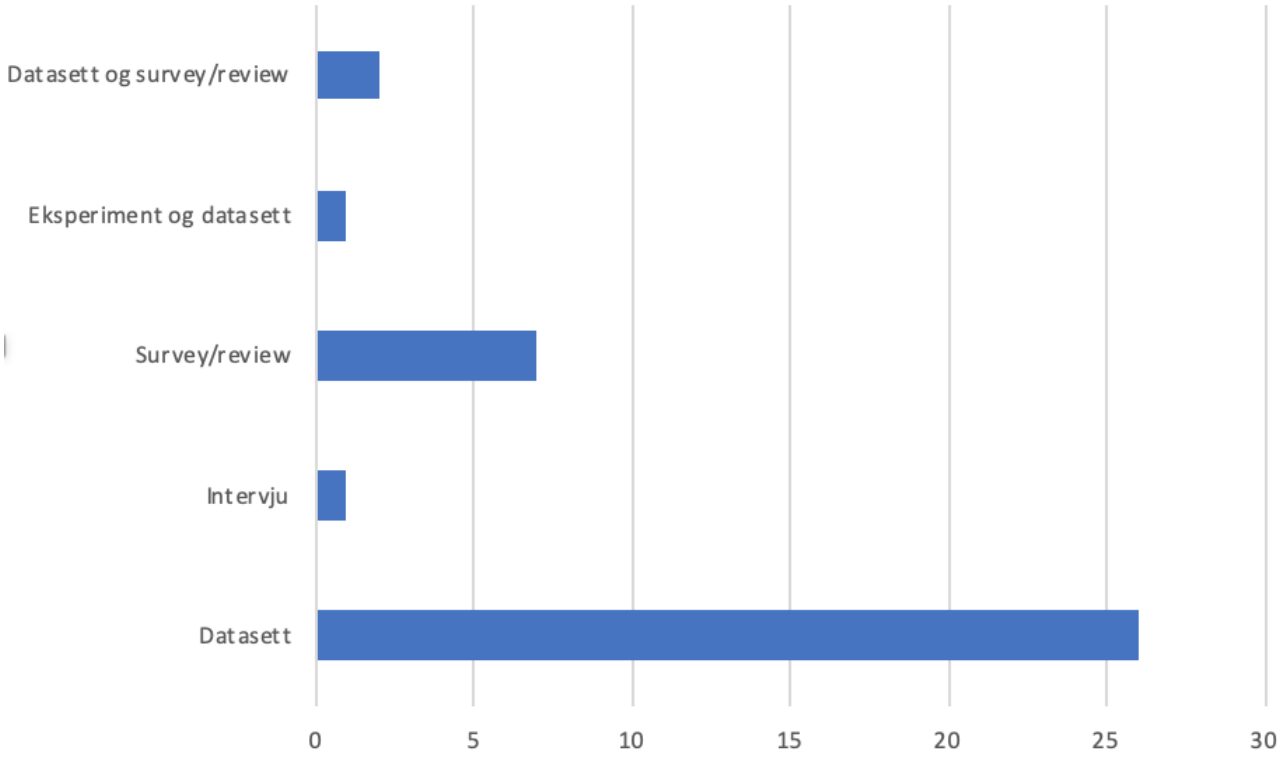
For å få en oversikt over hva slags artikler vi har plukket ut, i henhold til publiseringsår, publiseringsland og metode har vi utført en metaanalyse som belyser disse punktene. Vi har ikke fordelt artiklene basert på database da vi kun har artikler fra Scopus. Figur 2 viser hvordan artiklene er fordelt med utgangspunkt i publiseringsår. Artikler publisert før 2014 oppfylte ikke våre inkluderingskrav og er derfor utelukket fra dette studiet. Ut i fra diagrammet ser vi tydelig at vår oppfatning av at dette temaet er høyaktuelt stemmer, og samsvarer med forskningsfeltet. Totalt 22 av 37 artikler er fra 2018 og under vårt søk etter forskning fant vi fem som foreløpig er publisert fra 2019. De resterende ti er fra 2014-2017. Dette viser en stor økning innen forskning på temaet innen de siste årene.



Figur 3 Publiseringsårstall

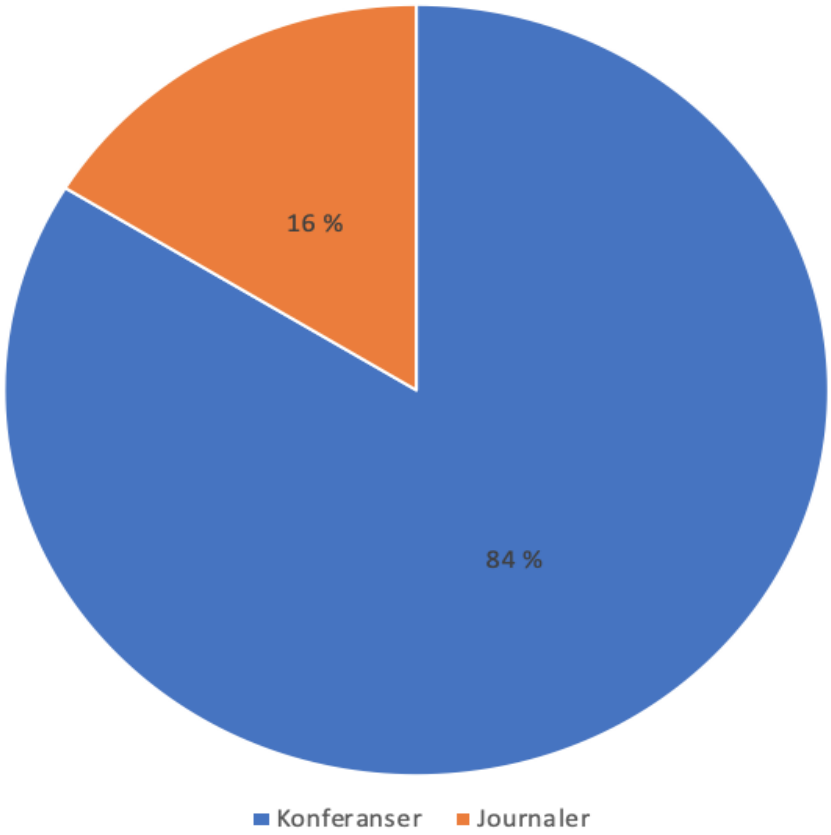
Videre delte vi opp artiklene basert på hvilke datakilder artiklene eller konferanseartikler baserer seg på, herunder datasett, intervju, survey/review, datasett sammen med survey/review og eksperiment sammen med datasett. Alle studiene vi har gått gjennom i vår litteraturstudie baserer seg på kvalitative metoder i form av utforming av modeller, rammeverk, systemer eller intervjuer. Vi har derfor valgt å ikke dele opp denne delen av metaanalysen i forskningsmetoder som kvalitativ, kvantitativ eller litteraturstudie. Et fåtall av studiene kombinerer datakilder.

To studier kombinerer datasett og survey/review. En kombinerer eksperiment og datasett. Et eksperiment vil i dette tilfellet si at det hentes informasjon ut i fra en test som har blitt laget av forskerne selv. Flertallet av artiklene baserer seg på datasett eller survey/review. Det ble også funnet et intervju gjort av en journalist som baserer seg på sikkerhet og big data eksperter. Oversikten vises i figur 4.



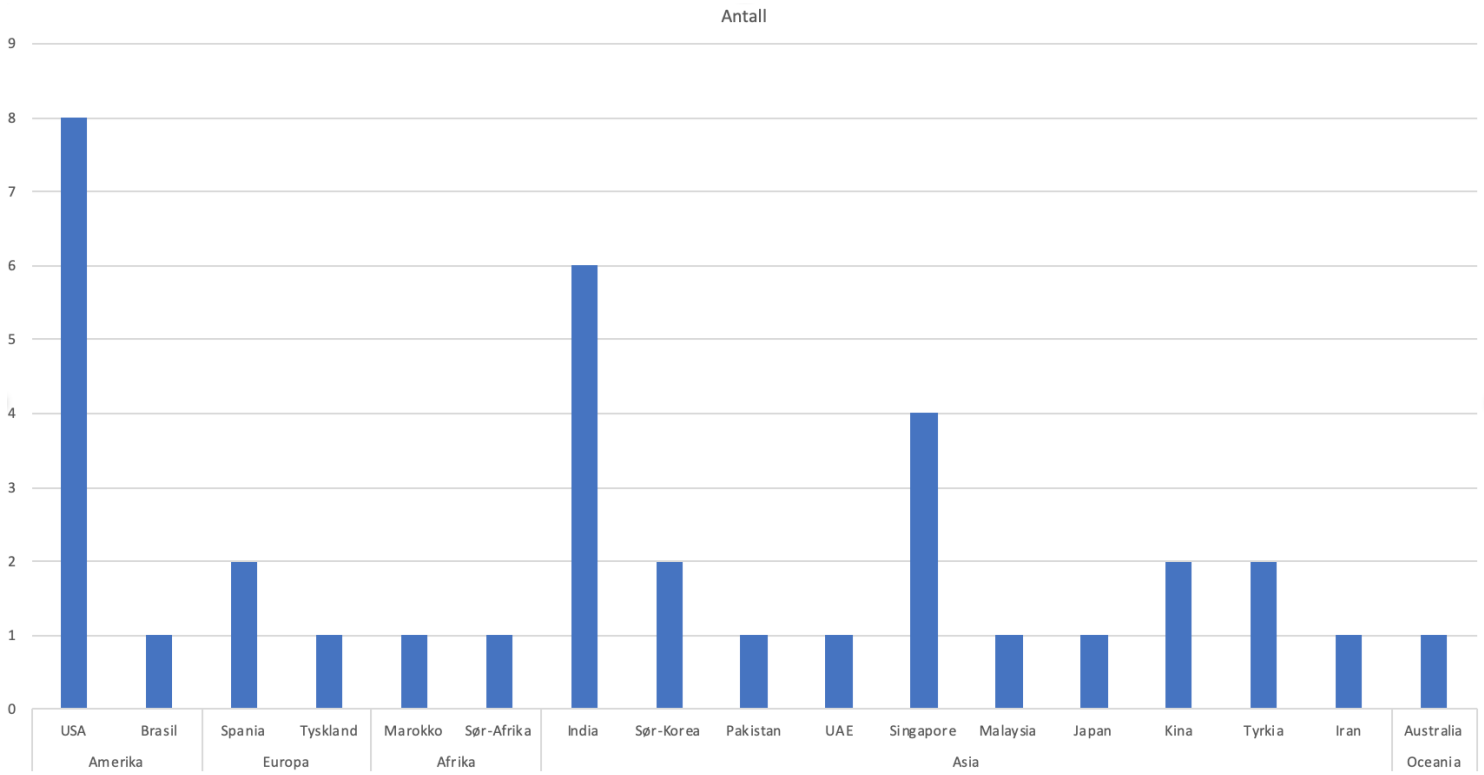
Figur 4 Datakilder

Noe vi la merke til med vår samling av studier er at de fleste er skrevet i konferanserartikler. Det kan tenkes at grunnen til det er at temaet for øyeblikket er veldig aktuelt, og at det derfor gjennomføres mange konferanser med Big Data og sikkerhet som tema. Figur 5 viser fordelingen.



Figur 5 Publikasjonstyper

Det var også interessant for oss å vite hvilke universiteter som som har bidratt mest til forskning innen big data og sikkerhet. Vi så raskt at det var universiteter fra mange av de samme landene som har vært mest aktive de siste seks årene. Figur 6 viser derfor en fordeling av land som har universiteter som er aktive på dette feltet. Slik kan vi se hvor studiene vi har valgt kommer fra og hvilke områder våre studier kommer fra.



Figur 6 Oversikt over våre valgte studier, fordelt på hvilke land og verdensdeler universitetene ligger i.

4.2 Utfordringer

I dette kapittelet fremhever vi de utfordringene litteraturen presenterer i form av Big Data og cyberkriminalitet fordelt på kategoriene vi identifiserte i konseptmatrisen.

4.2.1 Zero-day attacks

En av de største utfordringene innen datasikkerhet er såkalte *Zero-day attacks* (ZDA), hvor angriperen utnytter en svakhet som ennå ikke er fikset av

programvareleverandøren. Det sirkulerer ulike varianter av definisjonen på ZDA, hvor noen mener ZDA er angrep som utnytter en svakhet dagen den blir offentlig oppdaget, mens andre mener ZDA utnytter svakheter som ikke er fikset eller offentlig kjent. Den generelle definisjonen går derimot ut på at ZDA er angrep som utnytter svakheter som er offentlig kjent men ikke fikset av leverandøren i det angrepet inntreffer (Symantec, n.d"). Utfordringen med slike angrep er at svakheten allerede eksisterer i systemet, og med mindre en fiks kommer på plass fort kan skadene potensielt bli store. Forskningen har identifisert dette som en sentral utfordring innen cybersikkerhet og det er blitt gjort store framsteg på området maskinlæring og kunstig intelligens for å oppdage ZDA.

4.2.2 Seksuell grooming

Harms (2007) definerer *seksuell grooming* slik; "En kommunikasjonsprosess hvor en gjerningsmann bruker tiltrekningssøkende strategier samtidig som de engasjerer seg i seksuell desensibilisering og innhenting av informasjon om målrettede ofre med sikte på å utvikle relasjoner som resulterer i oppfyllelse av behov. Denne formen for cyberkriminalitet er et voksende problem på internett. Barn med mangel på venner eller sosial aktivitet er spesielt utsatt da overgriperen ofte kan bli deres nærmeste "venn". Å identifisere forsøk på grooming før de inntreffer er derfor viktig. Slike faremoment er forstyrrende for samfunnet som helhet. Men mest for mindreårige som blir eksponert for internett og som ikke alltid er klar over disse farene. (Ngejane et al, 2018). På grunn av at sosiale medier stadig vokser og gir flere plattformer for denne typen cyberkriminalitet er det nødvendig å ha systemer og rutiner som kan være med på å redusere dette.

4.2.3 Distribuerte angrep

Ifølge Feng, Akiyama, Lu & Sakurai (2018) er distribuerte cyberangrep som iverksettes samtidig fra mange ulike verter vel kjent som den typen angrep som har forårsaket mest skade i nyere tid. *Distributed denial-of-service* (DDoS) angrep er et eksempel på et slikt angrep hvor angriperen oversvømmer en nettverkstjeneste med forespørsler for å hindre tjenesten i å fungere normalt (Weisman, n.d). Målet med angrepet er at tjenesten eller serveren blir utilgjengelig eller ubrukelig. Slike angrep kan også fungere som en avledningsmanøver hvor angriperne forsøker å for eksempel plante skadevare eller stjele informasjon mens offeret er opptatt med å håndtere DDoS angrepet (Weisman, n.d).

4.2.4 Kredittkortsvindel

Svindel gjennom kredittkorttransaksjoner utgjør store tap for kunder og banker årlig. Kredittkort spiller en stor rolle i banksystemer, og i dag finnes det flere forskjellige metoder for å hente og "mine" informasjon og data ut fra korresponderende kredittkorttransaksjoner. En utfordring er at angripere kan hente informasjon fra kredittkortet og bruke dette på nettet for å enten utgi seg for å være offeret eller gjennomføre transaksjoner. (Kazemi & Zarrabi 2018)

4.2.5 Big Data prosessering

En stor, hvis ikke den største utfordringen innen big data og sikkerhet, er prosessering av all data som hentes inn. Analyse av nettverkstrafikk, logger og systemhendelser for å oppdage forsøk på inntrengninger har vært ett av de viktigste temaene innen cybersikkerhet. Analyse av Big Data forbedrer cybersikkerheten gjennom analyse av datastrømmer, etterforske hendelser, identifisering av anomalier i nettverksbruk, oppdage inntrengere, o.l. Kjennetegnene på big data kan bli beskrevet med de syv v-ene som er; "*Volume, Variety, Velocity, Variability, Veracity, Valence og Value*". De tre v-ene som er mest relevante satt opp bruk innen sikkerhet er "*Variety*", "*Valence*" og "*Veracity*". "*Variety*" er heterogeniteten til datatyper, formater, representasjon og semantisk tolkning. "*Valence*" referer til koblingen mellom datatyper. "*Veracity*" handler om data nøyaktighet, sannferdighet og pålitelighet. Wang & Jones (2018 s. 117). Dette stemmer bra med basis i systemer og modeller som vi har gått gjennom i litteraturen. Vi har sett flere utfordringer rundt heterogenitet til datatyper som analyseres for bruk innen sikkerhet. Ustrukturert og strukturert data som ofte blir representert på forskjellige måter må kunne bli satt sammen og gi et resultat som er nøyaktig og pålitelig. Dette krever mye datakraft og kompetanse samt systemer og modeller som er utformet med tanke på disse problemstillingene. Maimo, Clemente, Perez & Perez (2018) tar opp problematikken rundt utviklingen av det nye 5G nettet, hvor mengden data vil mangedobles så fort nettverket er ferdigstilt og implementert. For at slike datastrømmer skal kunne overvåkes og sikres mot trusler og angrep kreves det enorme mengder datakraft, samt smarte løsninger knyttet til design og arkitektur.

4.2.6 Oppdage anomalier/avvik

Terzi, Terzi & Sagiroglu (2017) sier at cyberangrep tidligere ble gjennomført med enkle og tilfeldige metoder. I dag blir angrep gjort mye mer systematisk og over lengre tid. I tillegg til dette øker datavolumet samtidig som data og informasjon kontinuerlig endrer seg seg fra angrep til angrep. På grunn av dette er det vanskeligere å gjøre gode og pålitelige analyser for å oppdage unormal oppførsel i et nettverk. Dette er en stor

utfordring som big data kan være med på å løse. De fleste studiene bruker dette som utgangspunkt for hvordan big data skal bli brukt i integreringen med sikkerhet. Anindya & Kantacioglu (2018, s. 1-8) sier også at de tradisjonelle regelbaserte IDS systemene begynner å bli utdatert og er svake forsvar mot nye, omfattende og sofistikerte angrep. Å ta i bruk Big Data sammen med dyp læring for å videreutvikle IDS'er som kan oppdage anomalier og proaktivt jobbe mot cyberangrep er blitt forsket på mye de siste årene da dette er en stor utfordring.

Anomalier i et nettverk kan være unormale mengder med data som sendes mellom brukere eller pakker som sendes inn eller ut fra helt ukjente IP-adresser. Et annet eksempel kan være at en bruker jobber inhouse på arbeidsplassen, samtidig som remote pålogging skjer via *VPN* (Virtual private network) på samme bruker. Dette vil være et avvik fra normal oppførsel på nettverket.

4.2.7 Kompromitterte brukere

Shah et al., (2019) tar opp utfordringen med kompromitterte brukere, "*compromised user credential*" (CUC), ettersom cyberangrep blir mer og mer utspekulerte og avanserte. I slike tilfeller blir en bruker med tilgang til et nettverk, for eksempel en administrator eller annen type bruker, misbrukt av andre personer enn hva brukerkontoen var tiltenkt og kan potensielt forårsake stor skade på nettverket. Utfordringen til bedrifter og organisasjoner er å oppdage slike tilfeller hvor en bruker blir misbrukt av andre på bakgrunn av at brukerinformasjonen er blitt lekket eller stjålet. Shah et al., (2019) presenterer en rekke metoder som cyberkriminelle bruker for å få tak i brukerinformasjon, for eksempel:

- *Lekkasje av brukerinformasjon* - Refererer til tap av passord og brukernavn hvor en annen enn tiltenkt bruker får tilgang til nettverket og dens rettigheter.
- *Phishing kits* - Scripts som distribuerer phishingmateriale for å lure til seg passord og brukernavn
- *Keyloggers* - Små scripts med skadelig innhold som registrerer blant annet tastetrykk, informasjon fra "clipboard" og opptak fra skjermen.

4.2.8 Konfigurering av ML algoritmer

Litteraturen presenterer maskinlæring og kunstig intelligens som gode metoder for å beskytte seg mot cyberkriminalitet, men det kreves ekspertkompetanse og mye prøving og feiling for å konfigurere en velfungerende maskinlæringsmodell (Sabar, Yi & Song 2018). Dette taes opp i flere artikler som vi har identifisert i vår studie og fremheves som en utfordring som må overgås skal maskinlæring og kunstig intelligens bli en solid

og sikker løsning innen cybersikkerhet. Apurva, Ranakoti, Yadav, Tomer & Roy (2018) poengterer også at slik kompetanse er vanskelig å innhente da teknologien fortsatt er i en utviklingsfase, og slik spesialisert og utfyllende kompetanse om Big data i et sikkerhetsperspektiv er ettertraktet.

4.2.9 Kostnader

Effektiv bruk av big data er ekstremt ressurskrevende for selskap å ta i bruk. Everett (2015) gjennomførte intervjuer med flere sikkerhetseksperter rundt bruken av Big Data. Her sies det at Big Data er essensielt for forebygging av cyberkriminalitet. Kostnader blir poengtert som et av de større problemene for denne typen løsning. Apurva et al., (2018) setter også kostnader som en stor utfordring. Selv om big data analyse har mange positive sider, er det ikke kommet langt nok på noen områder. En av nøkkelutfordringene som burde bli fokusert på er; "High Solution Cost" - Bygging og oppsett av slike big data analyse infrastrukturer har veldig høye finansielle krav. Å opprettholde "*return on investment*" (ROI) er vanskelig oppgave for mindre prosjekter eller selskaper. Bruk av skyløsning blir foreslått som en metode for å senke kostnader.

4.2.10 Personvern

Ved bruk av Big Data medfører det utfordringer relatert til personvern da store mengder data samles på ett sted. Mishra & Singh (2016) nevner flere eksempler på utfordringer relatert til Big Data og personvern, blant annet:

- Anonymisering av data - Med så store datamengder kan det bli umulig å kontrollere at all data blir anonymisert
- Big Data analyser er ikke fullstendig nøyaktige
- Juridisk beskyttelse, personvern, eksisterer for alle involverte individer
- Uetiske handlinger basert på tolkninger
- Sikkerhetsinformasjons- og overvåkingsrevisjon
- Personvernsbrudd og svindelhendelser
- Diskriminering
- Maskering av data kan bli forbigått eller overvunnet for å avdekke personlig informasjon, såkalt reidentifisering hvor flere datasett satt opp mot hverandre kan avsløre sensitiv informasjon om anonymiserte brukere

- Informasjonssikkerhet er et Big data problem
- Big Data vil sannsynligvis eksistere for alltid
- Bekymringer relatert til e-discovery
- Kan gjøre patenter og opphavsrett irrelevant

4.2.11 "Adverserial"

Prinsippet bak maskinlæring er at algoritmen over tid utvikler seg basert på data som kommer inn, input. På den måten holder algoritmen seg moderne og oppdatert på aktuelle og nåværende trusler og angrep. En "*adversary*" eller motstander av systemet kan på den måten utnytte dette prinsippet ved å "mate" algoritmen med tilpassede data for å degradere ytelsen til modellen da motstanderen i praksis har direkte tilgang til treningsdataen modellen benytter (Duddu, 2018).

Duddu forklarer også hvordan angripere kan utnytte distribusjonen av datapunkter for å yttligere degradere ytelsen til modellen:

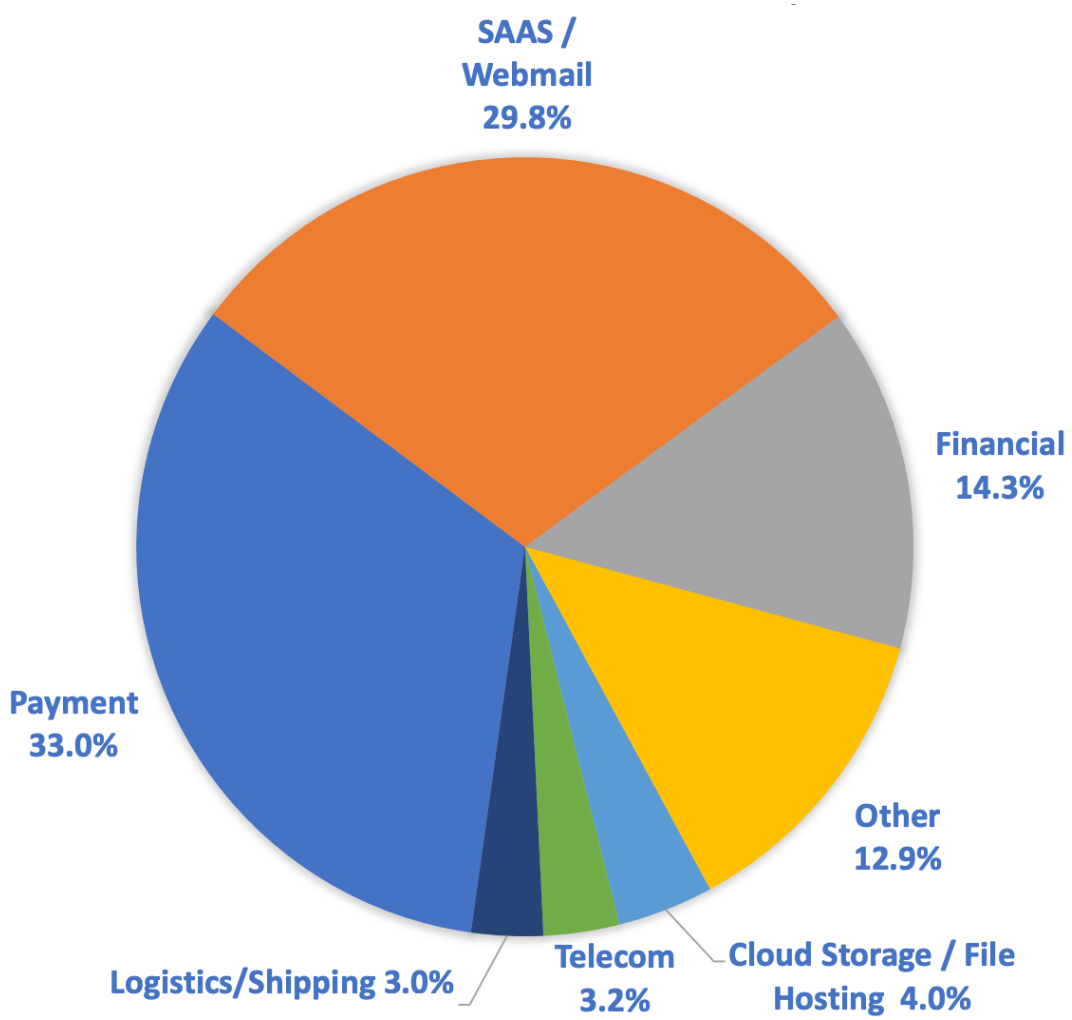
"Different data instances are considered to be independent and identically distributed. Some authors, for convenience and ease of computation, assume that the features are independent of each other. however, an adversary can try to obtain the correlation between different data points and features to introduce instances from different data distribution to degrade the model's performance. One of the major vulnerabilities in ML models is that the models perform well on testing and training data as they are usually drawn from the same underlying distribution. If the data from some other distribution is used as an input, the model will behave differently. This is the basic vulnerability that is exploited by attackers to craft adversarial examples to evade the model or degrade its performance." Duddu (2018, s. 357)

Eksempler på "adverserial" angrep er "poisining attacks, equation solving attack, path finding attack og model invasion attack".

4.2.12 Social engineering (phishing)

Denne utfordringen gjelder spesielt i tilfeller hvor det forekommer forsøk på *phishing* gjennom e-mail eller andre angrep som baserer seg på "social engineering". Pantic & Husain (2019) skriver at phishing e-mailer ofte er et utgangspunkt for cyberangrep hvor psykologien til offeret blir utnyttet. Phishing gjør det mulig for en angriper å omgå sikkerheten til et system ved å få tak i autentisk legitimasjonsbeskrivelser fra legitime brukere av systemet. Hvilke personlighetstrekk en bruker av et system har, vil ha en

påvirkning på hva slags phishing angrep denne personen er utsatt for. Pantic & Husain(2019) skriver også at det mangler forskning på området rundt hva slags innhold i phishing e-mailer som påvirker ulike typer mennesker som innehar like personlighetstrekk. Utfordringen her vil være å gjennomføre forskjellige typer opplæring, ut i fra hva slags innhold man er utsatt for å motta på mail. Statistikk fra "*Anti Phishing Work Group*" (APWG) viser at det er store mengder med phishing sider som operer med "spoofing" av e-mail og falske nettsider. "*Spoofing*" av e-mail vil si å sende mail med en forfalsket avsenderadresse i håp om at kunder eller ansatte vil bli lurt til å gi fra seg privat og verdifull informasjon. Antallet av phishing sider som ble oppdaget av APWG i fjerde kvartal 2018 var 138,328. Dette er mye mindre enn første og andre kvartal som begge lå på 230,000+. Grunnen til at det er en statistisk nedgang i phishingsider i fjerde kvartal betyr ikke at det er en faktisk nedgang. Sidene er heller blitt mer innovative for å unngå algoritmene til APWG som i tur gjør det vanskeligere for dem å oppdage. Dette viser uansett at social engineering, med fokus på phishing er en stor utfordring. Figuren under er fra APWG sin rapport fra fjerde kvartal i 2018. Denne viser at *SaaS*(Software as a Service) og webmail er offer for 29,8 prosent av alle phishing angrep. Figur 7 viser denne fordelingen



Figur 7 Fordeling av phishing angrep rettet mot teknologi og applikasjoner i industri. APWG Trend Report Q4 2018, www.apwg.org (2018)

4.2.13 Domenegeneratorer

Når et ondsinnet program eller skadevare kommer inn på et nettverk eller system er det ofte avhengig av kommunikasjon med en "*command-and-control*" server(C2 server) for å motta instruksjoner, videresende innsamlet informasjon eller engasjere seg i andre skadelige handlinger. Å hardkode en slik serveradresse i kildekoden er en dårlig løsning for angripere, da adressen enkelt kan sperres hvis den oppdages og angrepet nøytraliseres. Derfor implementerer angripere *domenegeneratorer*, *domene generator algorithms*(DGAs), for å generere et stort antall pseudotilfeldige domener hvor skadevaren forsøker å koble seg til. Denne oppførselen er vanskelig å overkomme på grunn av trusselens asymmetriske natur: sikkerhetsfagfolk må nekte tilgang til hele settet av domener som kan genereres av DGA for å begrense angrepet, mens angriperen trenger kun å kontrollere et enkelt domene for å opprettholde kommunikasjon. Det er tidligere blitt gjort lignende forsøk med bruk av maskinlæring for å identifisere domenene som blir generert og resultatet har vært lovende når det gjelder domener

generert av tilfeldige bokstaver og tall. Tidligere forskning kommer derimot til kort mot ordlistebaserte generatorer som setter sammen ulike ord fra en liste for å generere domener. Dette forklarer Koh & Rhodes (2018) med at tidligere forsøk har blitt lært opp til å identifisere tilfeldig rekker med bokstav og tall. For eksempel dhlpcscshdrvpcpp.com (generert av Ramnit DGA) fremstår mer mistenkelig enn middleapple.net (generert av suppobox DGA).

4.3 Foreslåtte løsninger

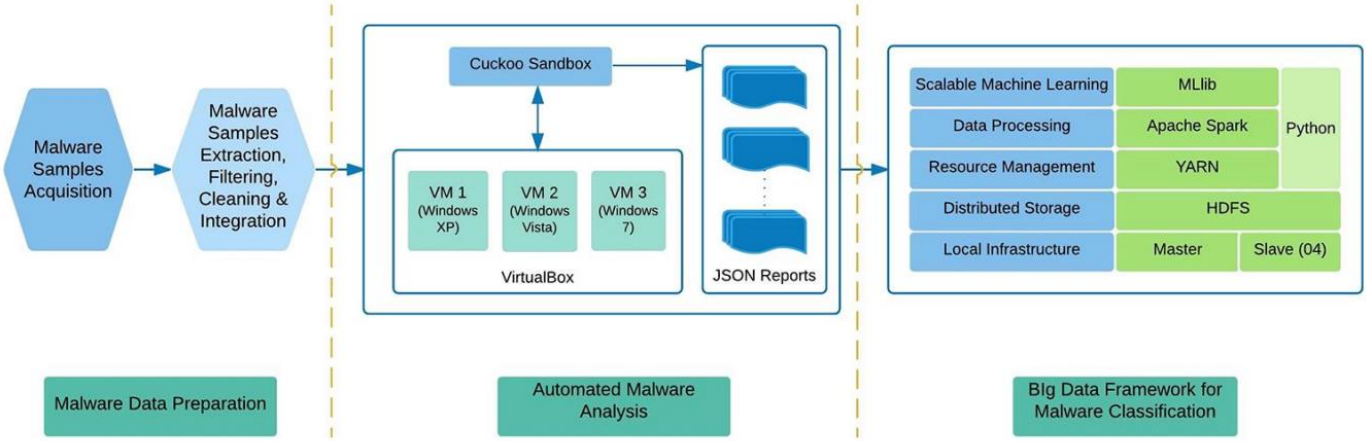
I dette kapittelet vil vi presentere løsninger som har kommet frem i litteraturen som et svar på utfordringene som ble identifisert i forrige avsnitt. Kapittelinndelingen er basert på kategoriene fra konseptmatrisen på samme måte som utfordringene for å skape en sammenheng mellom teksten og matrisen. Vi har valgt å fokusere på de kategoriene som vi ut fra litteraturstdiet opplever har størst betydning

4.3.1 Intrusion detection system

Det mest omtalte temaet i litteraturen IDS, et system som er designet for å fange opp trusler og angrep basert på blant annet signaturer. Britel (2019) beskriver IDS i to hovedkategorier, signaturangrep og atferdsangrep. *Signaturangrep* baserer seg på gjenkjennelse av et angrep eller deler av et angrep basert på signatur satt opp mot en eksisterende database. Systemet er derfor avhengig av at angrepet er blitt oppdaget tidligere og at signaturen er kjent og lagret i databasen. *Atferdsangrep* skiller seg ut ved å studere atferden til enten brukere eller data for å avdekke anomalier eller avvik. Et avvik blir deretter flagget som en potensiell trussel og signaturen til angrepet kan lagres i databasen. Det er denne typen system som dominerer nyere forskning og ansees som en banebrytende metode for å identifisere ZDA's, angrep som utnytter svakheter som ikke er kjent for verken bruker eller leverandør. Slike angrep er ekstremt vanskelig å beskytte seg mot da tradisjonelle signaturbaserte systemer ikke gjenkjenner angrepet som en trussel.

Ved hjelp av Big Data, maskinlæring og kunstig intelligens har forskere oppnådd gode resultater i forsøk på å oppdage ZDA's og andre typer angrep som ikke baserer seg på signaturer. Videre vil vi presentere ulike metoder og fremgangsmåter for å utvikle et IDS som kommer frem i litteraturen.

Gupta & Rani (2018) presenterer et rammeverk i sin artikkel hvor Big Data blir brukt for å oppdage ZDA's. Løsningen er skalerbar og bygget på Apache Spark med sitt tilhørende maskinslæringsbibliotek, MLlib. Figur 8 viser et overordnet løsningsforlag i form av et blokkdiagram for hvordan rammeverket fungerer.



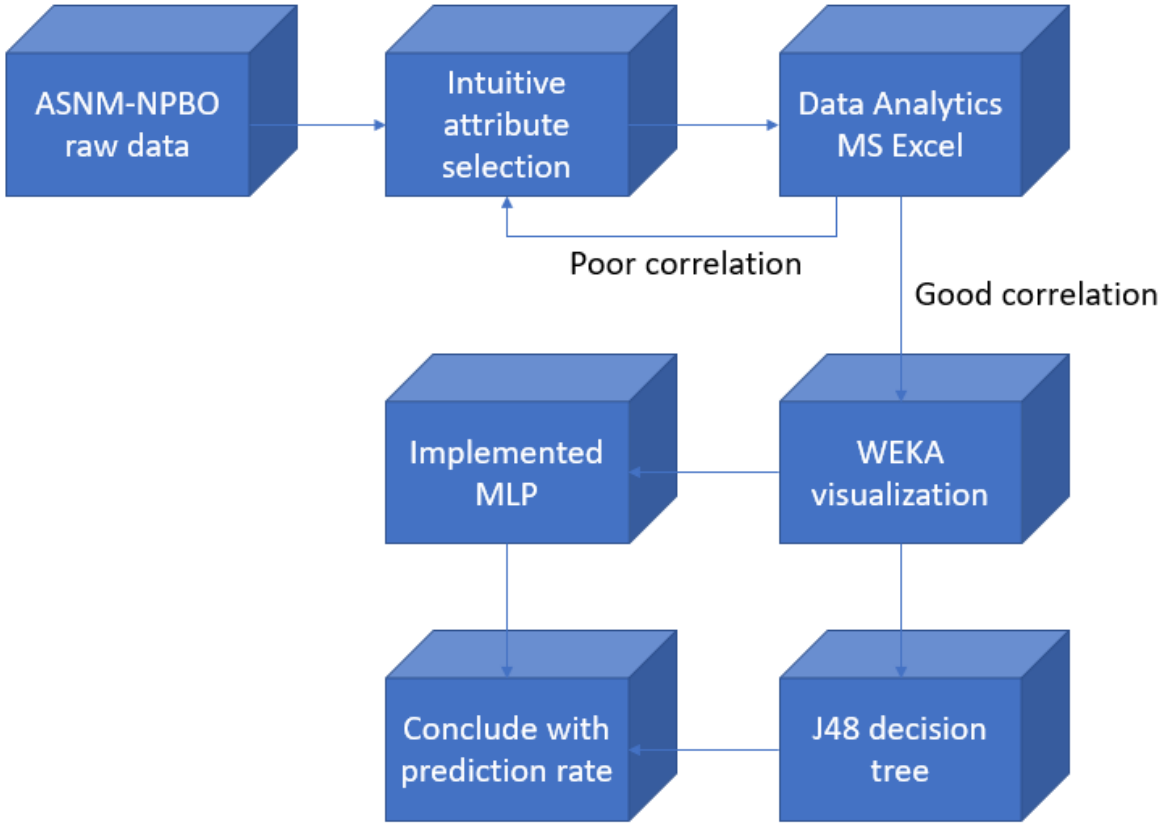
Figur 8 Blokkdiagram som visualiserer et rammeverk fokusert på oppdagelser av ZDA. Gupta & Rani (2018, s. 107)

Gupta & Rani (2018) benyttet seg av tre ulike maskinslæringsalgoritmer: *Naive Beyes* (NB), *Support Vector Machine learning* (SVM) og *Random Forest*(RF). Disse ble brukt for å analysere et datasett bestående av 200 000 datapunkter, hvorav 150 000 av dem inneholdt skadelig kode. Gupta & Rani hevder disse tre modellene er de mest brukte algoritmene i litteraturen når det kommer til å identifisere og klassifisere ZDA. Spesielt SVM går igjen i mange artikler med samme fokus og vitner om en enighet om at denne typen algoritmer er interessante å forske på i denne konteksten. RF skåret høyest med en nøyaktighet på 98%, mens SVM identifiserte 94% og NB 89% av truslene i datasettet.

En artikkel skrevet av Aksu & Aydin (2019) bruker en lignende fremgangsmåte som Gupta & Rani (2018). *Dyp læring* (DL) og SVM algoritmer ble brukt til å lage IDS for å oppdage mulige angrep på porter i et nettverk. IDS modellens oppgave var å fange opp såkalte "*port scan attempts*", forsøk på å scanne porter i et nettverk for å finne åpne porter, svakheter og potensielle muligheter for et angrep. En slik type modell kan erstatte et antivirus eller lignende IDS og forhåpentligvis forbedre ytelsen.

Modellene ble utviklet med utgangspunkt i CICIDS2017, et datasett bestående av ulike typer vanlig angrep. Modellene ble utviklet ut fra testdata som utgjorde 33% av datasettet. De resterende 67% ble brukt til å trene modellene. Resultatet viste en treffprosent på 97,90% for DL og 69,79% for SVM.

Teoh et al., (2018) brukte en lignende fremgangsmåte med DL i form av en "*Multilayer perceptron*" (MLP) modell, som består av et "*feed forward neural network*" med minimum tre noder. Modellen ble brukt til å oppdage potensielle trusler og ondsinnede data i et nettverk, som er en utrolig viktig del av datasikkerhet. Å oppdage slike data kan hjelpe til å forutse samt forhindre et potensielt angrep. I tillegg til MLP brukte Teoh et al., (2018) J48, en annen type klassifiseringsmodell, for å analysere et datasett bestående av trusler og ondsinnede data for å senere kunne identifisere slike data i en nettverksstrøm. Figur 9 viser hvordan data fra datasettet ASNM-NOBD blir brukt for å velge attributter og trene modellene.



Figur 9 Visualisering av treningsmetode ved bruk av data fra ASNM-NOBD datasett. Teoh et al (2018, s. 3)

For et menneske er det nærmest umulig å oppdage slike anomalier da dataen er tilnærmet uleselig, samtidig som det genereres data i en enorm fart og mengde. DL algoritmer gjør derimot denne jobben meget bra. Den analyserte dataen ble tagget med en tallkode som representerte datatype.

1. Godartet data
2. Direkte angrep
3. Ukjent angrep

MLP algoritmen greide å identifisere trusler i nesten alle tilfeller, og oppnådde en nøyaktighet på 99,35%.

Et angrep på "*Information and communication technology*"(ICT) systemet til en flyplass kan potensielt sette liv i fare og må unngås for enhver pris. I en artikkel skrevet av Sezari, Moller & Deutschmann (2018) blir et IDS system basert på DL brukt for å oppdage anomalier i et nettverk. Datasettet DARPA ble brukt for å trene og teste modellen. 494 021 observasjoner ble brukt i datasettet og splittet 80/20 på forholdsvis treningssett og testsett. Totalt 36 features ble brukt for input, mens output kun produserte to utfall, angrep eller ikke angrep. Dette gjorde det lettere i identifiseringsprosessen. Modellen ble målt ut ifra tre faktorer: Nøyaktighet, gjenkjenningshastighet og lav forekomst av falske positiver. Resultatet viser at modellen presterte veldig bra og scoret 99,86% nøyaktighet og 99,83% gjenkjenningshastighet med en lav forekomst av falske positiver på kun 0,16%. Dette resultatet viser at Deep Feedforward network fungerer meget bra til å oppdage anomalier i et nettverk.

Et annet eksempel hvor DL blir brukt for å oppdage anomalier kommer frem i Najada, Mahgoub & Mohammed (2019). I denne artikkelen blir dyp læring (DL) og Big Data brukt for å overvåke kontinuerlige datastrømmer for å oppdage avvik (anomalies), enten enkeltstående eller flere datapunkter som sammen utgjør et avvik, for å predikere potensielle angrep. Artikkelen fokuserer på fem ulike typer angrep:

- DoS
- DDos
- *Brute Force angrep* (En eller flere datamaskiner som forsøker å knekke et passord ved å forsøke så mange passord som mulig før systemet evt. stenger kontoen)
- SSH Brute Force angrep
- Intern nettverksinfiltrering

Resultatet er todelt, hvor del en fokuserer på å utvikle flere ulike modeller per angrep for så å optimalisere den modellen med høyest treffsikkerhet. Del to inkluderer alle angrepene i en og samme modell ved bruk av distribuert random forest og DL med de mest relevante egenskapene. Den endelige modellen kan nøyaktig predikere en trussel og hva slags type angrep som utføres.

For selskaper som bruker cloud for lagring av informasjon betyr det at store mengder med data blir behandlet på forskjellige nettverksenheter og mye informasjon blir lagret på en felles lagringsenhet. Slike systemer er store mål for angrep fra cyberkriminelle. For store organisasjoner og offentlige institusjoner som regjering, bank og sykehus, som lagrer store mengder med personlig data, betyr dette at cybersikkerhet må være på

topp. More, Unakal, Kulkarni & Goudar (2018) foreslår bruken av Big Data analyse for å skape et sanntidssystem for deteksjon av trusler mot cloud nettverk. "Open source" programvare som "Apache Hadoop, Hive og Mahout" blir trukket fram som programvare for bruk innen deteksjon av angrep mot cloud nettverk. Det blir så lagt frem en enkel 8 stegs algoritme som viser den grunnleggende tankegangen bak behandling og analyse av data.

Første steg henter datasett fra de gjeldende cloud tjenerne og lagrer disse. Andre steg viderefører data til en "*sniffing module*" som henter ut den nødvendige informasjonen og sender denne til "*Hadoop distributed file system*" (HDFS) for videre prosessering. Steg tre konverterer all data til en strukturert form. Steg fire definerer et skjema og tabeller samtidig som den strukturerte dataen blir fylt inn her. Steg fem henter ut data fra disse tabellene basert på satte features, altså variabler som blir hentet ut fra tabellen som er viktig for å lære opp maskinlæringsalgoritmen. Steg seks bruker maskinlæringsalgoritmer for å finne ut om data er skadelig eller ikke. I steg 7 blir en treningsmodell brukt for å ta i bruk historiske data ved å sammenligne testdata og treningsdata. I siste steg brukes en classifier for å sammenligne data fra treningsmodell med ny innhentet data for å definere data som skadelig eller ikke.

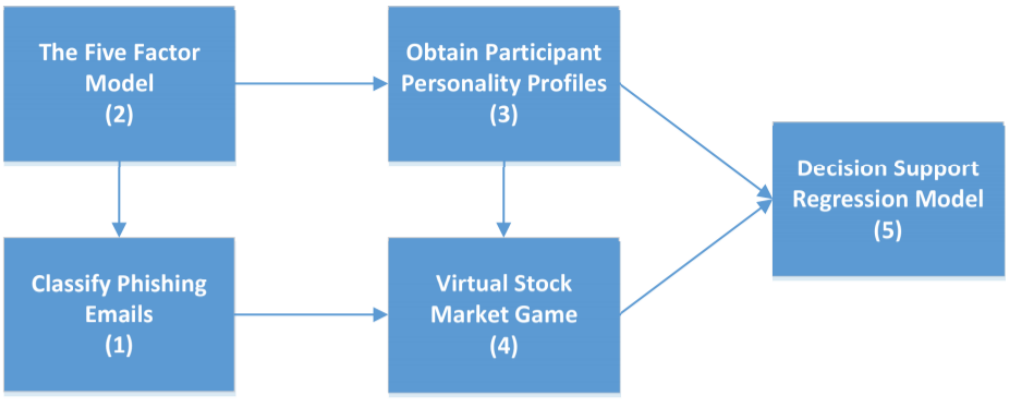
For å kunne ha mest mulig oppdatert informasjon om skadelig programvare, eller smutthull som oppdages, kan det være lurt å oppsøke stedene hvor slik informasjon og programvare deles. Enkelte sider på "darknet" og "deepnet" tilbyr deling av denne typen programvare, samt forum hvor cyberkriminelle kommuniserer seg imellom. Nunes et al., (2016) foreslår å hente data fra nettopp "darknet" og "deepnet". Forskerne presenterer et operasjonelt system for informasjonsinnsamling fra sosiale plattformer på internett som fokuserer på cybertrusler, spesielt fra sider på "darknet" og "deepnet". Det fokuseres på pre-rekognosering av informasjon rundt cybertrusler, det vil si informasjon som blir samlet før en eventuell hackergruppe går til angrep på det forsvarte systemet. Det er brukt "*crawlers*" som fokuserer på å hente inn relevante HTML dokumenter, "parsers" henter informasjon fra spesifikke markedsplasser for å gi "crawler" nettsider som burde sjekkes, eller sjekkes flere ganger. For at "crawler" og "parser" skal få tak i den mest relevante informasjonen, blir det tatt i bruk en maskinlæringsteknikk som forholder seg til et datasett med informasjon om hva man skal se etter på markedsstedene og forumene. Dette kan være ord eller setninger som eksperter på "darknet" og "deepnet" har bidratt med. Det blir brukt både veiledede metoder og semi-veiledede metoder under tilnærmingen av maskinlæring. Veiledede metoder krever mer ressurser i form av at eksperter må bli tatt i bruk for å få til en effektiv klassifisering av ord og setninger. Semi-veiledede metoder bruker klassifiseringsteknikker som RF og SVM. Dette systemet var allerede operasjonelt i 2016 og i ferd med å overføres til en kommersiell partner for bruk.

I februar 2015 ble det oppdaget et sikkerhetshull i windows som brukere ble informert om, men foreløpig var det ingen kjente metoder for å utnytte dette. I april 2015 ble det på "darknet" lagt ut for salg en metode for å utnytte dette sikkerhetshullet. Så sent som i

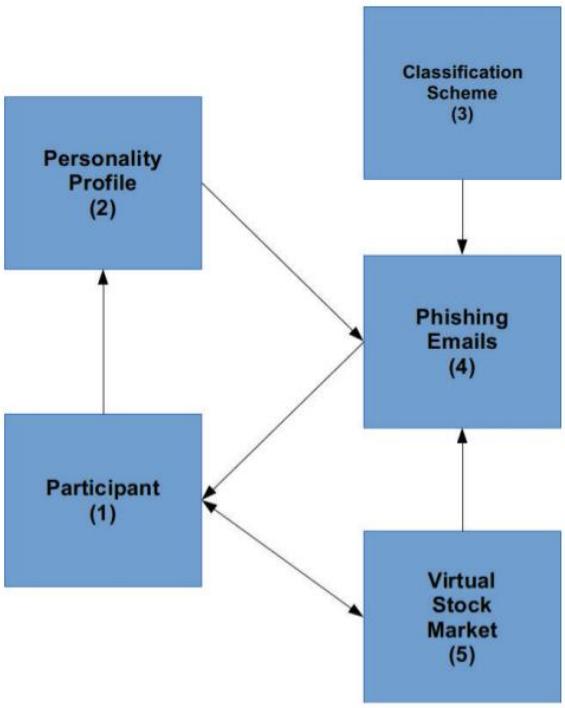
juli 2015 ble det oppdaget av et cybersikkerhetsfirma at en trojansk hest utnyttet dette hullet for å hente kredittkortinformasjon. Da var allerede nesten 6 av 10 organisasjoner på en global skala blitt eksponert. Dette demonstrerer hvor viktig pre-rekognosering av informasjon fra de riktige kildene er for å forbedre et IDS.

4.3.2 Personifisering av opplæring

Som et tiltak for å forbedre motstandsdyktigheten til ansatte i en bedrift mot "social engineering" og da spesielt med tanke på phishing angrep, foreslår Pantic & Husain (2019) å kartlegge personlighetstyper som et hjelpemiddel for å kunne utvikle personifisert opplæring innen phishing angrep. Hovedmålet for deres arbeid er å kunne fastslå hvor mottakelige personer er for phishing angrep basert på deres personlighetstrekk ved bruk av femfaktor modellen, også kjent som "OCEAN" modellen. Dette er et system for profilering av personlighet og som skårer deltakerne på fem forskjellige personlighetstrekk. Her foreslår Pantic & Husain (2019) å bygge et eksperimentelt system som kan korrelere en persons "OCEAN" profil mot hans eller hennes mottakelighet for en eller flere typer phishing e-mail. Under treningsfasen brukes "OCEAN" for å skape personens personlighetsprofil. Deretter må e-mailene som skal brukes som phishing mails senere i treningsfasen kategoriseres etter hvilke av de fem faktorene de utnytter mest. Deltakerne vil så delta i et virtuelt aksjemarked spill. Dette er et kunstig online handlingsmarked laget av Pantic & Husain(2019). For å finne mottakeligheten til de forskjellige deltakerne vil de bli forsøkt phishet med e-mailer som bruker innholdet fra det virtuelle aksjemarkedet som utnytter hver av de fem faktorene. Når det er samlet inn tilstrekkelig med data brukes statistiske slutningsteknikker som multinomial logistisk regresjon for å finne testpersoners mottakelighet for "spear-phishing" angrep basert på personlighetstype. Figurene under viser hvordan treningsmetoden for beslutningssystemet er satt sammen, og hvordan samspillet i det virtuelle aksjemarkedet ser ut.



Figur 10 Beslutningsstøttesystem basert på personlighet for analyse av phishing mottakelighet. Pantic & Husain (2019, s. 3068)



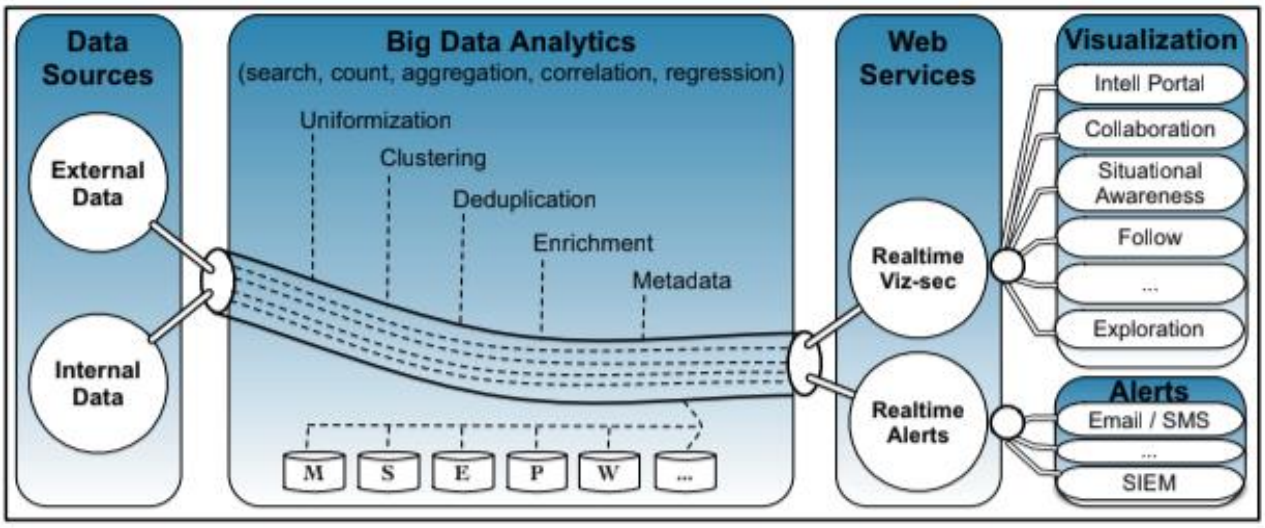
Figur 11 Samspillet i det virtuelle aksjemarkedet. Pantic & Husain (2019, s. 3069)

4.3.3 Big data visualisering

Som en foreslått løsning for demping av cybertrusler presenterer Carvalho, Polidoro & Magalhaes (2016) en cybertrussel plattform med et registreringssystem som opererer i sanntid og visualisering av cybertrusler. Denne plattformen er allerede tatt i bruk av kunder og i 2016 oppdaget den 107 millioner skadavarehendelser daglig på mer enn 2,7 millioner infiserte IP-adresser. Plattformen heter *OwlSight* og ble laget med tanke på at dybden og bredden på cyberangrep har økt de siste årene. Noe som krever mer av systemer og mennesker som jobber mot cyberkriminalitet. Målene for plattformen er:

- Evnen til å jobbe med forskjellige databaser, filtyper og andre systemer sømløst.
- Kunne håndtere mengden, hastigheten og variasjonen av data til sikkerhetsrelaterte hendelser
- Tilby sanntidsregistrering av cybertrusler med minst mulig falske alarmer.
- Tilby innsiktsfull visualisering og analyseteknikker.
- Bidra til å redusere gjennomsnittlig tid til å rette opp skader som er påført som følge av et angrep

OwlSight er bygget med forskjellige blokker. Dette er illustrert i Figur 12.

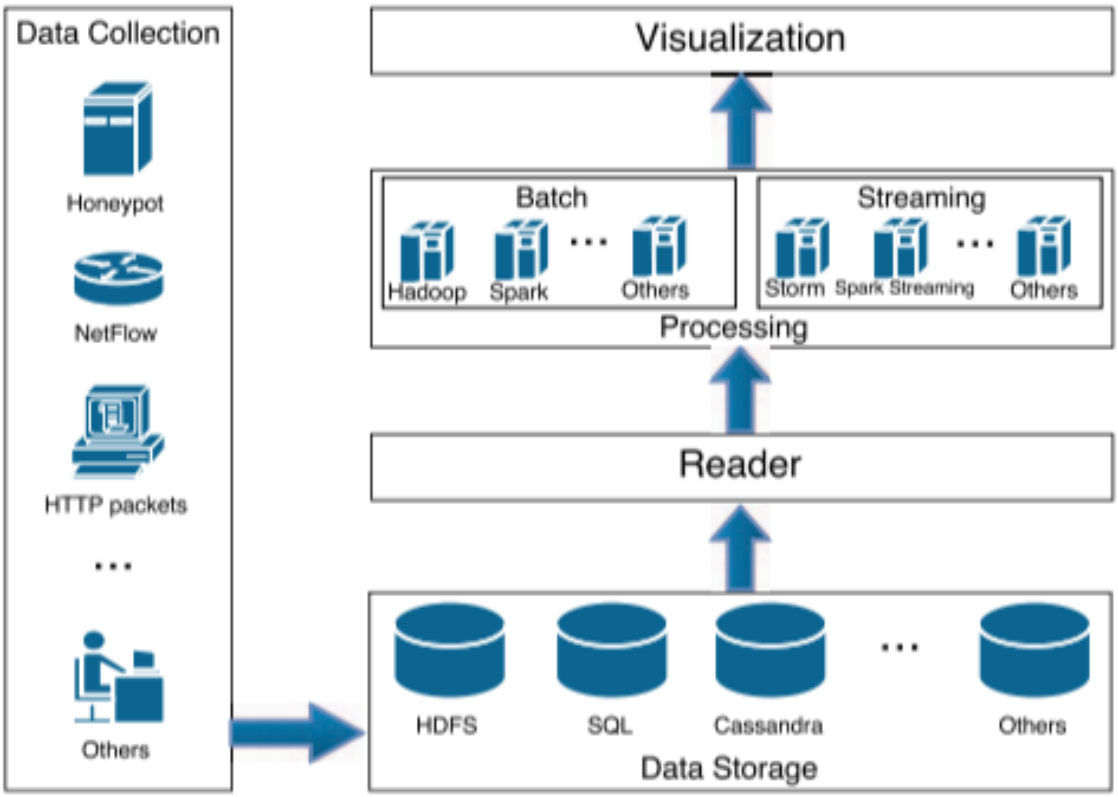


Figur 12 Oppbyggningen av OwlSight. Carvalho et al. (2016, s. 63)

Fra figuren kan vi se at OwlSight samler inn data fra forskjellige kilder. Ekstern data er data som hentes på en ikke-inntrengende måte utenfor organisasjonens nettverk. Dette kan være data som ligger åpent på for eksempel sosiale medier. Intern data er data som nettverkslogger eller brukerhistorikk fra deltakere på nettverket i en organisasjon. Fordi det er forskjellige typer data blir det gjennomført en "uniformization" av datatyper. Dette betyr at data blir endret slik at det blir mulig for systemet å hente informasjon uavhengig av datatype. Det blir så gjennomført en clustering av data for å finne hendelser som er av samme karakter. Identiske data blir identifisert og kopier blir fjernet gjennom deduplisering. De gjenværende dataene blir så beriket med for eksempel geografisk lokasjon eller systemnavn. Informasjonen blir så lagret i forskjellige databaser etter type data. Disse databasene inneholder datahistorikk som blir brukt under sanntidsregistrering av angrep og analyse. Denne prosessen blir støttet av en big data motor som gjennomfører søk, korrelasjon og regresjon av data. Plattformen blir tilbudt som en SaaS, hvor man registrerer seg og oppgir informasjonen til nettverket man ønsker å overvåke. Bruken av cloud er nesten obligatorisk for å kunne holde kostnader på et nivå som gjør det økonomisk forsvarlig for selskapene å kjøpe tjenesten. Webtjenesten RESTful blir brukt for å tilby en integrasjon mellom et lag med visualisering og et lag med sanntids alarmer (Carvalho et al., 2016)

Artikkelen skrevet av Las-Casas, Dias, Meira & Guedes (2016) presenterer en arkitektur for cybersikkerhetsapplikasjoner basert på big data analytics. Denne arkitekturen har mange av de samme målsetningene som OwlSight. Hurtig og nøyaktig prosessering av store mengder med forskjellige datatyper er noe av det som går igjen. For å illustrere bruken av denne arkitekturen har det blitt implementert en applikasjon med mål om å prosessere store mengder med spam trafikk fra hele verden. Applikasjonen henter denne dataen fra honeypots, nettverk som med vilje har blitt gjort mottakelige for angrep. I dette tilfellet er det meldinger som inneholder spam og phishing. Innboksene

med meldingene blir lagret over ett HDFS slik at all sikkerhetsdata er tilgjengelig for applikasjoner som bruker Hadoop eller Spark. Hovedoppgaven til applikasjonen er å identifisere phishing e-mail i et sett med spam mails. Det blir brukt "*Natural Language Processing*" (NLP) og "*Locality-Sensitive Hashing*" (LSH) for å inspisere tekst i meldingene. Arkitekturen kan minne om OwlSight og står ovenfor mange av de samme utfordringene. Figur 13 visualiserer arkitekturen.



Figur 13 Arkitekturen til den foreslåtte løsningen. Las-Casas et al. (2016, s. 37)

Målet for arkitekturen er å visualisere data og gjøre dette leselig for mennesker. Det kan legges til forskjellige visualiseringsplattformer i arkitekturen gjennom å bruke HDFS som et repositorium eller ved å integrere dem direkte i applikasjonen.

4.3.4 Game-theoretic models

De siste årene har bruken av maskinlæringsteknikker og Big Data analyse fått et stort fokus i arbeidet mot cyberkriminalitet. Maskinlæringssystemer har rapportert gode resultater mot nye sofistikerte cyberangrep, inkludert ZDA's. Problemet er at disse systemene ikke alltid tar høyde for angripernes adaptive oppførsel for å komme seg rundt deteksjonsprosedyrer. Dette resulterer i at når systemer som dette blir introdusert for et virkelighetsscenario, er de ikke i stand til å håndtere intelligente angripere som jobber med fokus om å manipulere angrepsmetodene slik at de akkurat ikke blir fanget opp. Som et forslag for å kunne stille sterkere mot slike "adverserial"

angrep foreslår Anindya & Kantarcioglu (2018) å ta i bruk "game-theoretic models". "*Game theory*" er et begrep for vitenskapen rundt logiske avgjørelser tatt av mennesker, dyr eller datamaskiner". Anindya & Kantarcioglu (2018) utvikler teorien bak en "adversary's" mest optimale strategi for å kunne gjennomføre et "mimicry attack" mot en grupperingsbasert deteksjon av abnormaliteter. Altså et angrep som forkler seg som en vanlig hendelse i et system. Forsvarsstrategien blir formulert gjennom å finne de mest optimale parameterne fra et "game theoretic" synspunkt. Målet med å ta i bruk "game-theoretic models" er å kunne forstå valgene som angriperen gjør for å komme seg gjennom et forsvar ut i fra hvilke karakteristika forsvarssystemet har og dermed ligge et steg foran såkalte intelligente angrepsforsøk.

4.3.5 Rammeverk

Rammeverk blir brukt i mange ulike settinger og varianter for å løse problemer og utfordringer relatert til Big Data og cybersikkerhet. I litteraturen finner vi eksempler på rammeverk som fokuserer på konfigurering av maskinlæringsalgoritmer, innhenting av data eller oppdagelse av mistenkelig oppførsel av brukere.

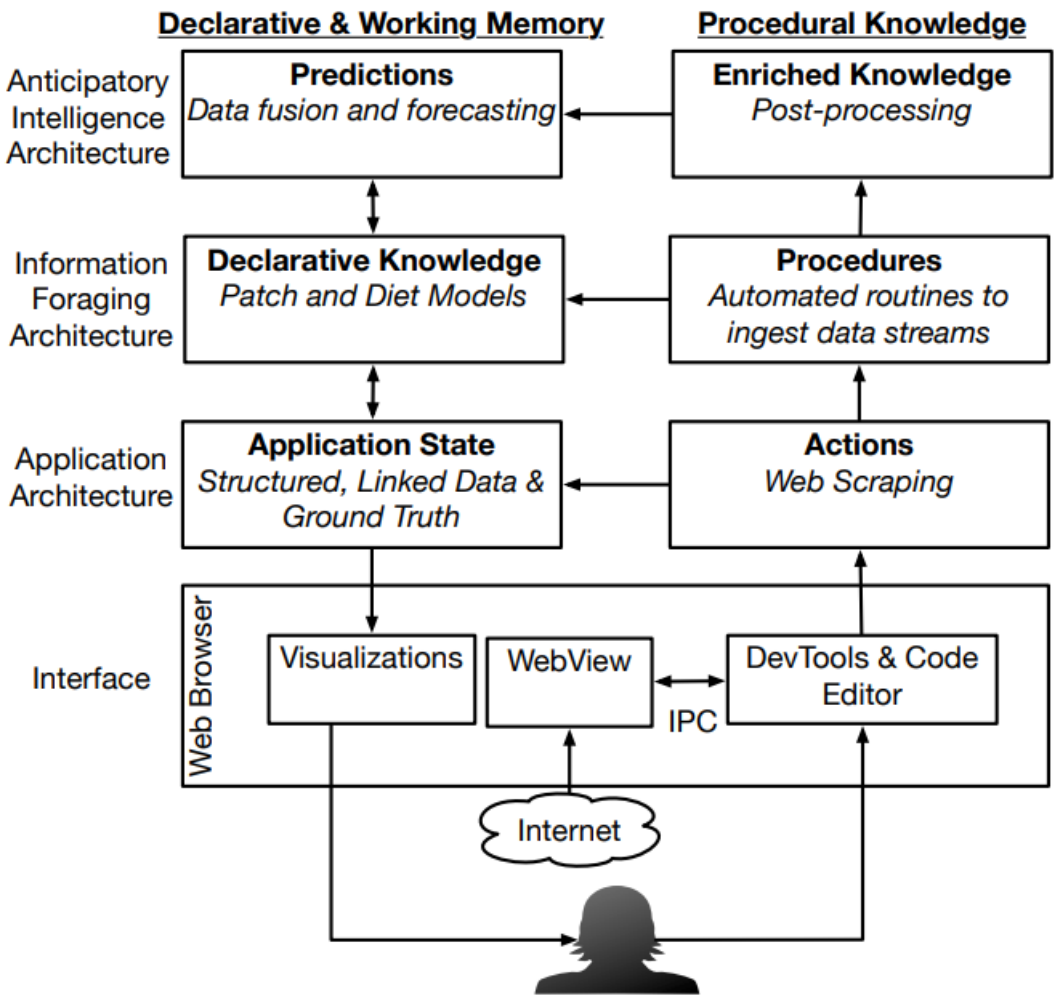
Maskinlæringsalgoritmer har i nyere tid blitt utforsket som en mulig kandidat for å identifisere trusler og potensielle angrep, noe som er blitt nevnt utfyllende i tidligere avsnitt, og SVM modeller har oppnådd imponerende ytelse når det kommer til å identifisere trusler og anomalier. En slik SVM modell baserer seg på "*supervised learning*" som betyr at den må forhåndsprogrammeres og "læres" for å fungere optimalt, noe som krever utfyllende kompetanse og mye prøve og feile for å oppnå tilfredsstillende resultater.

Artikkelen skrevet av Sabar et al., (2018) presenterer et bi-objektivt hyperheuristisk rammeverk for å opprette en konfigurasjon for en SVM modell. Rammeverket består av en "high-level" strategi og "low-level" heuristikk. Kombinasjonen av disse genererer en konfigurasjon for SVM modellen. Ved bruk av rammeverket kan en oppnå gode resultater selv om en ikke har så høy kompetanse på å konfigurere modellen.

Artikkelen konkluderer med at rammeverket er veldig effektivt, om ikke bedre, sammenlignet med tilsvarende modeller og andre algoritmer.

Et annet eksempel hvor rammeverk blir brukt for å håndtere utfordringene relatert til Big Data er Dalton, Dorr, Liang & Hollingshead (2018). I denne artikkelen kommer konseptet om informasjonshøsting eller innhenting fram. Artikkelen beskriver hvordan dette kan bli brukt for å oppdage offentlig tilgjengelig ressurser som kan predikere fremtidige cyberangrep. "*Information foraging for algorithm discovery*" (IFAD) er navnet på rammeverket og omfatter et system som legger til rette for brukere slik at de kan utforske informasjonskilder samtidig som veien til informasjon eller en ressurs blir kartlagt og lagret. Veien mellom en ressurs til den neste blir også kartlagt, som igjen

danner et nettverk av ressurser for informasjon. En bruker kan så utpeke en ressurs som en potensiell kilde for å finne flere prediktive variabler, hvor da utbytte fra ressursen blir sporet og omgjort til en poengscore. Ved å bruke disse poengscorene kan nettverkanalyse bli brukt for å identifisere flere potensielle høytytende ressurser. Figur 14 forklarer arkitekturen til IFAD.



Figur 14 Arkitekturen til IFAD. Dalton et al. (2018, s. 4643)

Å oppdage ressurser som forutser cyberangrep i offentlig tilgjengelige data er utfordrende grunnet vekstsatsen av søksdomenet og tilpasningsevnen til angripere. Implementasjonen av informasjonshøstingsstrategier balanserer menneskelig intuisjon med automasjon slik at et bredt utvalg av nye konsepter fra høyvolum datasamlinger kan være raskt testet for "veracity".

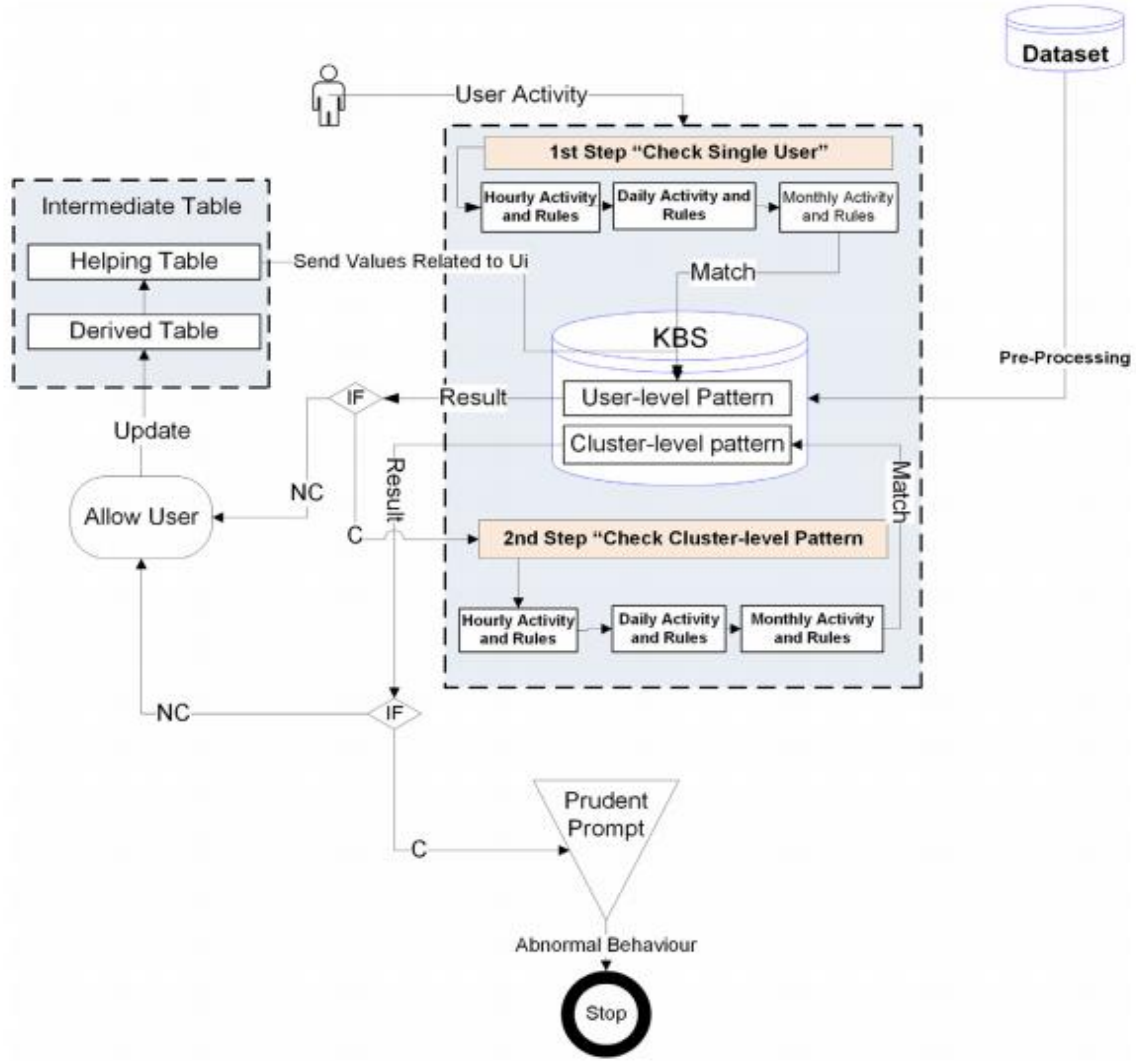
Shah et al. (2019) bruker rammeverk i en helt annen setting enn de tidligere presenterte artiklene. Utfordringen med kompromitterte brukere er blitt nevnt i 4.3.7, og Shah et al. (2019) presenterer et rammeverk for å oppdage slik misbruk av brukere ved å analysere atferdsmønstre.

Artikkelen presenterer en metode for å motvirke "compromised user credentials" (CUC), hvor en brukerkonto med utvidet tilgang (administrator, moderator etc) blir kompromittert og utnyttet for å skade miljøet brukerkontoen befinner seg i. Kort og godt hacket. Metoden tar utgangspunkt i ett adferdsmønster og etablerer et utgangspunkt for alle slike brukerkontoer. Skulle en brukerkonto avvike fra sitt atferdsmønster trigger det systemet og brukerkontoen blir flagget som en potensiell trussel. Et slikt system hindrer at brukerkontoer med utvidet tilgang blir misbrukt av personer som brukerkontoen i utgangspunktet ikke var tiltenkt, og stopper kontoen fra å utøve skadelige handlinger som brukerkontoen i utgangspunktet har full tilgang til.

Rammeverket består av tre komponenter:

- "*Knowledge base system*" (KBS)
- Intermediate tabeller
- *Forsiktig varsling* ("prudent prompt")

KBS består av to ulike kategorier: individuelle adferdsmønster og gruppeatferdsmønstre ("clustering"). KBS setter grunnlinjen eller utgangspunktet for alle brukere og lagrer informasjon som kan brukes for å sammenligne en gitt brukers nåværende atferd med tidligere atferd for å oppdage avvik. De Iintermediate tabellene består av to hovedtabeller: Hjelpetabell og avledet tabell. Disse tabellene utgjør aktiviteten til brukerne på nettverket og loggfører hendelser og handlinger brukerne foretar seg, samt tidsbruk og annen nyttig informasjon for å kunne oppdage avvik. Siste del av rammeverket består av varsling. Hvis mistenkelig oppførsel oppdages blir nåværende atferd først sjekket på individuelt nivå. Hvis dette ikke stemmer med KBS blir neste nivå sjekket, gruppeatferdsmønstre. Hvis ikke dette heller stemmer med KBS blir en varsling sendt ut om den kompromitterte brukeren, samt en liste med hvilke handlinger brukeren har utført som kan ansees som fiendtlige. Figur 15 viser hvordan rammeverket fungerer med de ulike komponentene.

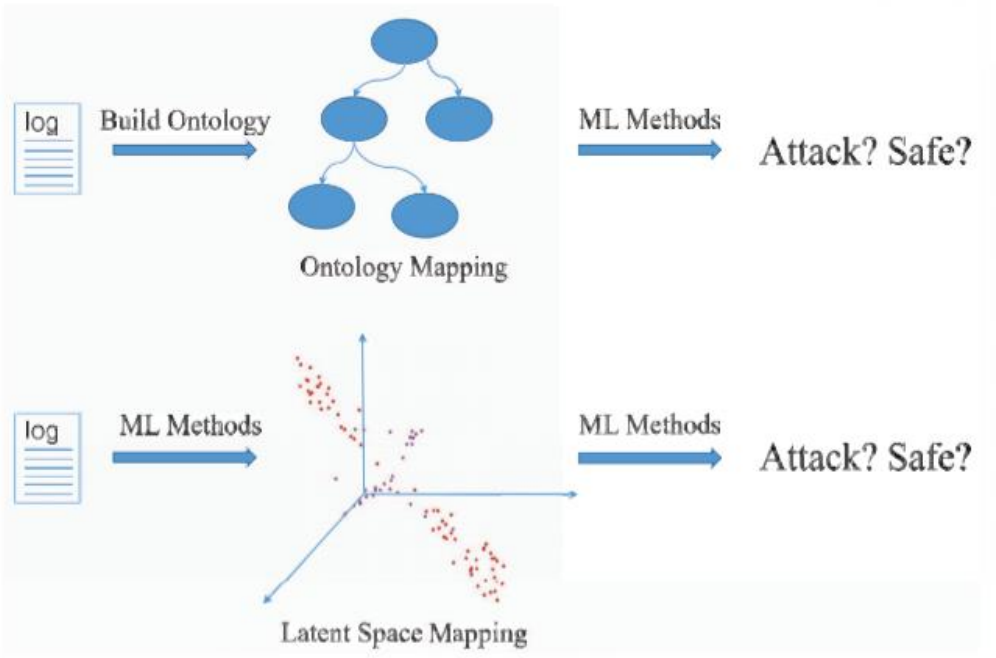


Figur 15 Visualisering av rammeverket med alle komponentene. Shah et al (2014, s. 412)

4.3.6 Ontologi

Den store mengden med ustrukturerte og strukturerte data fører med seg utfordringer når dette skal behandles. En av utfordringene er som nevnt tidligere at det finnes mange forskjellige datatyper og maskinspråk. Innen cybersikkerhet har det de siste årene blitt fokusert mye på å ta i bruk big data og analysere denne for å oppdage ting som anomalier, trusler eller angrep. Dette er en prosess som ofte har blitt forsøkt automatisert, med blandede resultater.

Innen deteksjon av angrep på systemer har forskere lagt frem ideen om å bruke ontologi for å skape et vokabular i et generalisert maskinprosesesserbart språk for innkommende datastrømmer som f.eks under oppdagelse av mulige angrep på IT-systemer i sanntid. Ontologi innen cybersikkerhet er en taksonomimodell basert på sikkerhetsrelasjoner for å muliggjøre normaliserte og semantiske dataformat som kan brukes i senere prosesser. Bruken av ontologi i et rammeverk, som er maskinlæringsbasert fra start til slutt for deteksjon av angrep, er noe som mangler. Motivert av disse faktorene foreslår Zheng et al. (2018) en maskinlæringsbasert metode for å lære, samt bruke, et "novel ontology framework for intelligent attack identification". Figur 15 visualiserer forskjellene på et rammeverk som bruker en latent fremvisning, eller clusteranalyse som kan brukes i deteksjon av angrep, og en ontologisk metode.



Figur 16 Ontologi i angrepsdeteksjon. Nedre: Latent representasjon. Zheng et al. (2018, s. 1310)

Ideen om å bruke ontologi i cybersikkerhet er god, men også veldig avansert. For å forklare tanken bak denne løsningen tar vi frem et eksempel fra Zheng et al (2018). En person studerer en tjeners loggfil uten noe kunnskap innen cybersikkerhet. Denne personen forstår nødvendigvis ikke hva hver logg betyr, men kan likevel forstå forskjellene på loggene fra et semantisk perspektiv. Dette vil si at personen ikke er

avhengig av formatet på loggene, hvis disse blir fremstilt med ord eller tegn som gir forståelse for personen. Dermed kan denne forståelsen bli overført til videre arbeid. Det er dette scenarioet som blir videreført til et MLs problem. Siden modellen ikke har kunnskap innen cybersikkerhet, blir alle logger sett på som tekstinformasjon. Denne informasjonen blir behandlet rått på et karakternivå for å forsikre semantisk forståelse av rådata. En programvare som for eksempel har ansvar for å blokkere IP-adresser med uønsket trafikk trenger informasjon for å oppdage disse adressene. Om denne informasjonen er i et format som er ukjent for programvaren kan ikke informasjonen behandles. Men om systemet eller programvaren som forsyner og mottar informasjon baserer formateringen på et språk som er felles, eller rådata som er forståelig for programvaren som skal utføre blokkeringen, vil effektiviteten øke og tidsbruk senkes.

4.3.7 Redusere datamengde

Wang & Jones (2018) fokuserer på aspektene "Variety" og "Veracity" innenfor Big Data, to av de syv V'ene, satt opp mot nettverkstrafikk og angrep. En sentral utfordring ved Big Data mengden data som må prosesseres og duplikater av data, samtidig som datakvaliteten må opprettholdes. Wang prøver i sin artikkel å redusere datamengden som må analyseres ved å fjerne duplikater for å øke ytelsen og hastigheten til for eksempel et IDS system. Dette forbedrer også datakvaliteten ved å balansere data, da duplikater fører til ubalansert data.

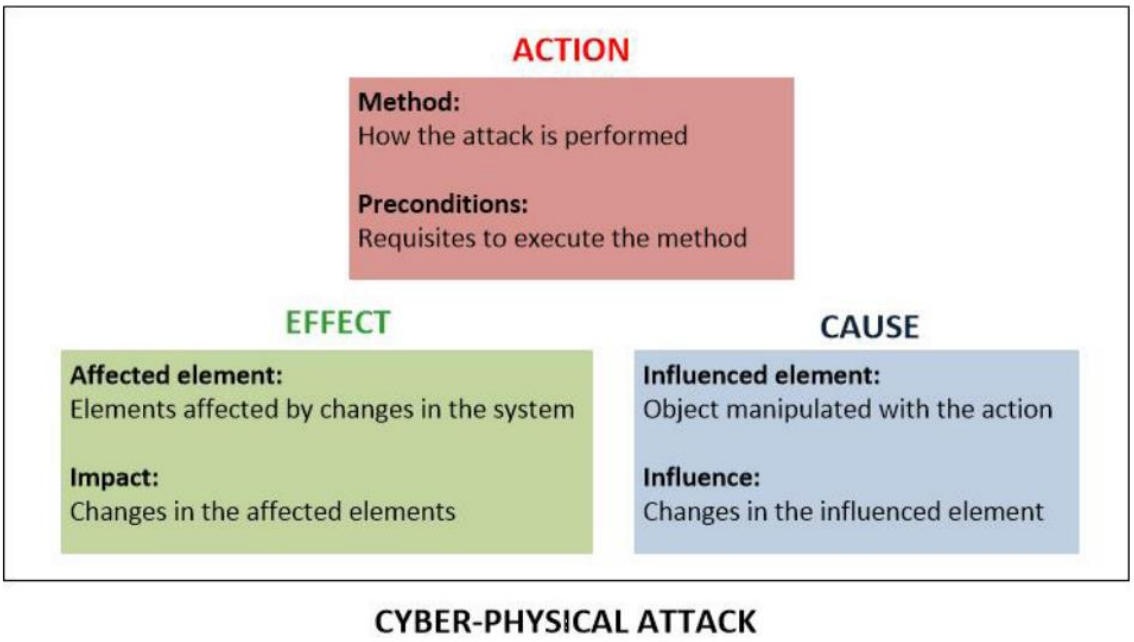
Kodespråket *R* og dens funksjoner blir brukt for å fjerne duplikater og utføre K-means clustering. Basert på to variabler ble fem klustere identifisert. MAWILab blir så brukt for å rense data, sørge for at dataene er komplett og for å opprettholde god datakvalitet. Eksempler på mangelfull data er tomme felter, skrivefeil, tegnsettingfeil osv. Slike feil kan for eksempel ødelegge "Veracity" for Big Data.

Artikkelen konkluderer med at R og dens funksjoner fungerer bra for å fjerne duplikater, analysere korrelasjonen mellom attributter og identifisere mistet data og datamønstre, samt håndtere ulike typer data osv. Dette løser til en viss grad utfordringene relatert til "Variety" og Veracity" innenfor Big Data. Datasettet ble redusert med 75,15% etter å ha fjernet duplikater som øker balansen i dataene. Dette fører igjen til høyere nøyaktighet for IDS systemet.

Wang nevner at et mulig fremtidig prosjekt kan være å utvikle et system som kan overvåke liknende datasett i sanntid for å potensielt nøytralisere ZDA..

Et annet eksempel på å redusere datamengder i Big Data er Bordel, Alcarria, Robles & Sanchez-Picot (2018). Artikkelen starter med å forklare "ambient intelligence environments", miljøer hvor fysiske komponenter og software er integrert i et sammenhengende system for å utføre og assistere beboerne i miljøet med dagligdagse oppgaver. Et eksempel på et slikt miljø er smarthus, men på en mye større skala. Slike

miljøer er utsatt for såkalte cyber-fysiske angrep, hvor en eller flere komponenter i systemet blir angrepet eller endret, og grunnet systemets avhengighet kan skaden spre seg til hele nettverket. Et cyber-fysisk angrep kan forklares ut i fra seks faktorer, forklart i Figur 17.



Figur 17 Strukturen til et cyber-fysisk angrep. Bordel et al. (2018, s. 34899)

Grunnet systemets natur, hvor komponenter ofte er plassert offentlig tilgjengelig, er det utfordrende å forhindre angrep. Derfor fokuseres det på å reagere effektivt og hurtig på angrep. Bordel et al. (2018) ser på maskinlæring og kunstig intelligens som mulige løsninger på dette problemet, hvor automatiserte systemer overvåker datastrømmene og leter etter anomalier og mistenkelig oppførsel. Mye av problemet for å få til dette er den enorme mengden med data som må gjennomgås. Bordel et al. (2018) foreslår at man kan ta i bruk matematiske formler og algoritmer for å minske store datasett, men fremdeles få samme resultat. Ta for eksempel et stort datasett med oppførsel fra brukere på nettet. Mange av brukerne kan ha lignende oppførsel og det vil derfor ikke være nødvendig å gå gjennom alle, *hvis* det er mulig å balansere dette. Matematiske formler er ikke noe vi ønsker å gå dypt inn på i vår oppgave, men hovedpoenget til Bordel et al. (2018) er å bruke et matematisk rammeverk som kan balansere og fjerne unødvendig informasjon fra datasett, og som likevel gir et likt resultat. Dette øker hastighet og fjerner unødvendige mengder med data, selv om alt i utgangspunktet må bli prosessert.

Den foreslåtte løsningen er basert på bruk av Stochastic Reduced Order Models (SROM), som blir komplementert med informasjonsteoretiske teknikker for å forbedre prosesseringstid og kompresjonsrate. Det viser seg at med bruk av slike teorier er det mulig å redusere datasett før bruk av SROM modeller, for å kalkulere det ferdig reduserte datasettet, samtidig som de statistiske egenskapene til det originale

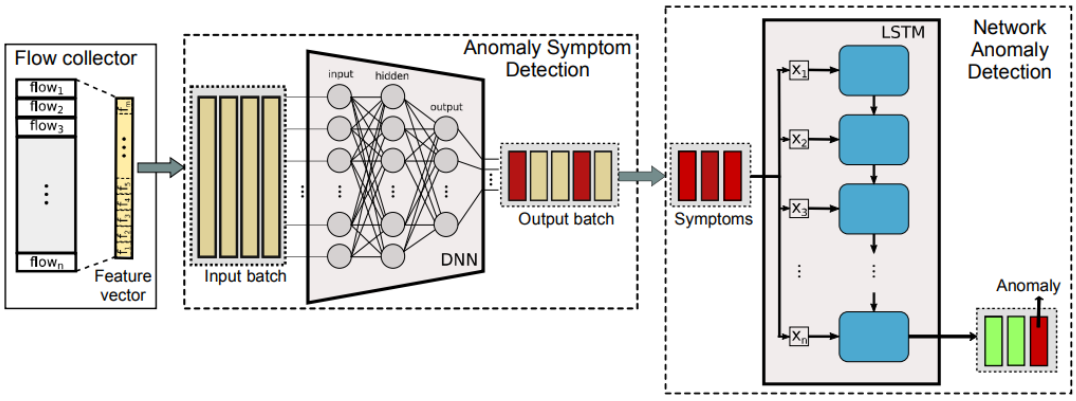
datasettet blir beholdt. Resultatene viser at reduserte datasett er gyldige løsninger for å trene intelligente sikkerhetssystemer, og samtidig opprettholde samme suksessfrekvens som hvis de originale datasettene ble brukt.

4.3.8 Arkitektur/Systemdesign

Inntreden av det nye 5G nettet fremkaller utfordringer relatert til IT-sikkerhet ved at volumet av data som kan overføres blir enormt. 5G-PPP konsortium har identifisert en håndfull KPI'er(Key performance indicators) som gir et innblikk i volumet og hastigheten til nettverket. Maimo et al. (2018) nevner fire av disse KPI'ene:

- 1000 ganger høyere mobildata volum per geografisk området
- 10 til 100 ganger flere tilkoblede enheter
- 10 til 100 ganger høyere typisk databruksats
- Ende til ende forsinkelse på <1ms

Datastrømmene vil med andre ord bli enorme og det vil kreve store ressurser å overvåke slike datastrømmer for anomalier og potensielle trusler i sanntid, slik et IDS skal. Artikkelen til Maimo et al. (2018) presenteres en 5G orientert arkitektur for å analysere 5G datastrømmer og identifisere trusler og anomalier i et 5G mobilt nettverk i sanntid ved hjelp av deep learning algoritmer. Artikkelen fokuserer ikke på nøyaktigheten av systemet, men heller ytelsen i form av hastighet og om systemet vil bli en flaskehals i et virkelighetsscenario. Figur 18 viser et overordnet design av arkitekturen.



Figur 18 Design av arkitekturen. Maimo (2018, s. 4)

Resultatet er et todelt system. Steg en analyserer datastrømmer og leter etter anomalier over korte perioder. Nøyaktighet blir ofret for ytelse slik at systemet ikke skal fungere

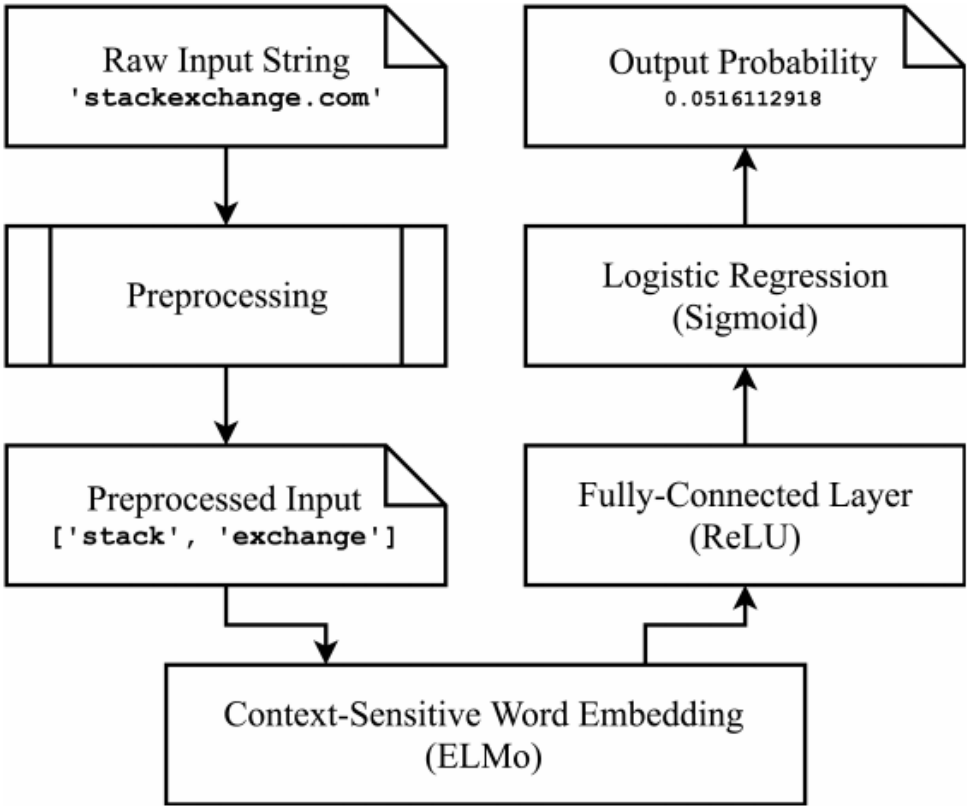
som en flaskehals. Hendelser som blir plukket ut blir sendt videre til steg to. Det består av en Long short-term memory (LSTM) rekursiv nettverksalgoritme som har blitt trent under oppsyn for å gjenkjenne midlertidige mønstre for typiske angrep.

Arkitekturen oppnådde en toppytelse på 2,47 millioner feature vektorer per sekund.

4.3.9 Maskinlæring/kunstig intelligens

Nesten alle artiklene vi har identifisert i vår litteraturstudie har inneholdt eller brukt en eller flere former for maskinlæring eller kunstig intelligens. Big data og maskinlæring/kunstig intelligens er to teknologier som går hånd i hånd da man stort sett er avhengig av maskinlæring/kunstig intelligens for å få utbytte eller verdi av data man sitter på i et Big Data system. Vanlig analyseteknikker holder rett og slett ikke mål. I dette underkapittelet tar vi for oss de artiklene som omhandler maskinlæring eller AI, men som ikke passet inn under de tidligere kategoriene.

Et slikt eksempel er Koh & Rhodes (2019) som tar for seg utfordringen relatert til domenegeneratorer, som tidligere nevnt i avsnitt 6.13. Løsningen Koh & Rhodes kommer opp med er en maskinlæringsalgoritme, nærmere bestemt LSTM, som inkorporerer konteksten av ordene brukt for å generere domener. Ved bruk av Embeddings from Language Models (ELMo) kan modellen differensiere ulike kontekster av ordene som er satt sammen, for så å gjenkjenne ord som ikke hører sammen i samme kontekst. På den måten kan modellen identifisere domener generert av en DGA med høy treffprosent. Metoden krever minimalt med treningsdata og modellen bruker kort tid på å trenes. Figur 19 viser hvordan modellen fungerer.



Figur 19 Hvordan LSTM fungerer. Koh & Rhodes (2019, s. 2968)

Resultatet viser at modellen oppnådde en nøyaktighet på 89,5% etter kun 30 treningseksempler på DAG domener, mens etter 100 eksempler traff den på 91,2%. Det betyr i praksis en false postive rate (FPR) på henholdsvis 1:1000 og 1:10000.

5 Diskusjon

I dette kapittelet vil vi diskutere studiens funn og komme med våre egne vurderinger rundt bekjempelse av cyberkriminalitet og trender ved bruk av big data som har kommet frem de siste seks årene.

5.1 Trender

Vår problemstilling la til grunn å identifisere eventuelle trender som kommer frem i litteraturen de siste seks årene. Etter å ha gjennomført en systematisk litteraturgjennomgang har vi identifisert et par markante trender i litteraturen innenfor området Big Data og cyberkriminalitet. Vi har utelatt å nevne maskinlæring/AI som en trend, selv om det kommer klart frem i matrisen. Dette på grunn av at vi anser maskinlæring/kunstig intelligens som en del av Big Data "pakken", og derfor ikke en selvstendig trend.

Derimot står IDS frem som en klar trend innenfor nyere forskning og totalt 24 av 37 artikler nevner eller bruker IDS på et eller annet vis. IDS er ikke et nytt begrep eller system og har eksistert lenge i form av signaturbaserte systemer (Britel, 2019). De siste årene har teknologien tatt et sprang i form av maskinlæring og kunstig intelligens som gir programvare og kode muligheten til å lære over tid, samt tilpasse seg ulike situasjoner og reagere "intelligent". Dette har ført til et nytt forskningsområde innenfor IDS hvor maskinlæring og kunstig intelligens blir brukt for å identifisere mistenkelig oppførsel fra brukere (Shah et al., 2019) eller anomalier og avvik i en datastrøm (Britel, 2019). Denne nye typen av IDS er mer dynamisk enn den tidligere signaturbaserte metoden og innehar muligheten til å ta til seg nye regler og kunnskap etterhvert som trusler blir oppdaget. På denne måten er systemet alltid oppdatert på nye trusler.

ZDA blir jevnlig nevnt i litteraturen som en av de mest sentrale og vanskeligste utfordringene med tanke på cybersikkerhet, og muligheten for å reagere effektivt på slike angrep har tidligere vært svært begrenset. Nyere forskning har i stor grad fokusert på bruken av maskinlæring og kunstig intelligens for å oppdage slike angrep, samt reagere med effektive tiltak for å nøytralisere eller begrense ZDA. Muligheten for å oppdage og nøytralisere slike angrep i sanntid er banebrytende og kan potensielt endre sikkerhetsmiljøet slik vi kjenner det idag. Slike hull eller "exploits", som ZDA er, blir ofte solgt for store summer på darknet, og en slik forvandling kan ødelegge slike svarte markeder for uoppdagede sikkerhetshull.

Den nest største trenden blant foreslåtte løsninger etter IDS, er ifølge vår matrise rammeverk. Rammeverk blir nevnt i hele 8 artikler og brukes som et verktøy for å simplifisere kompliserte oppgaver som for eksempel å konfigurere ML algoritmer for å oppnå god ytelse eller sette opp et IDS basert på Big Data. Slike rammeverk er gode

utgangspunkt for aktører som ønsker å benytte seg av teknologien, men ikke innehar nok kompetanse for å utvikle og implementere systemer fra bunnen av.

Dette bringer oss videre til den tredje største trenden, nemlig systemdesign. Systemdesign har mange likhetstrekk med rammeverk, men skiller seg ut ved å forklare systemer på et mer teknisk nivå og hvordan komponenter skal fungere sammen for å danne for eksempel et fungerende IDS. Eksempler på systemdesign finner vi i blant annet hos Maimo et al., (2018) og Ahn, Kim & Chung (2014).

Visualisering av Big Data systemer markerer seg også som en slags trend, hvor totalt 4 artikler tar for seg emnet. Fokuset ligger på å best mulig visualisere Big Data systemer i sanntid for å kunne reagere raskt hvis systemet identifiserer avvik eller anomalier i nettverket. Slike visualiseringer blir ofte gjort gjennom dashboards.

Videre har vi identifisert gjennom vår studie at en håndfull maskinlæringsmodeller og DL algoritmer går igjen i litteraturen. Blant annet SVM og LSTM er populære valg blant forskerne da de oppnår god nøyaktighet innenfor bruksområdet cybersikkerhet og å oppdage anomalier i en datastrøm. Også CNN (Convential neural network) blir brukt hyppig i litteraturen.

5.2 Forskningshull

Nyere forskning innen Big Data og cybersikker har stort fokus på å identifisere potensielle trusler og anomalier eller avvik i datastrømmer og nettverk. Gjennom vår studie har vi avdekket et par temaer som vi mener kan kategoriseres som forskningshull og lede videre til fremtidig forskning. Ved å avdekke slike forskningshull kan vi bidra med å fremme forskningen innen Big Data og cybersikkerhet og på sikt tette hull ved å opplyse om deres eksistens.

Som tidligere nevnt fokuserer litteraturen mye på å identifisere trusler, men steget derfra til reaktive handlinger er ikke tatt. For eksempel har IDS kun som oppgave å oppdage trusler for så å varsle om oppdagelsen, men håndteringen av trusselen eller iverksetting av tiltak blir ikke nevnt i litteraturen.

En av utfordringene som går igjen handler om behandlingen av både strukturert og ustrukturert data som kommer i forskjellige formater. Dette fører til økt behandlingstid og effektiviteten til big data analyse går drastisk ned. Som et tiltak for dette foreslår Zheng et al., (2018) å ta i bruk ontologi for å utvikle et generalisert maskinprosesserbart språk. Det kommer allikevel ikke frem et forslag for hva slags type språk dette kan være. Dette gjelder for alle artiklene. Det kan fortsatt hende at det eksisterer forskning på dette i andre artikler. Men sett ut i fra vårt forskningsperspektiv med fokus på å sette sammen big data og cybersikkerhet, har ikke litteraturen fra vårt søk gitt noe tydelig svar.

5.3 Diskusjon og integrasjon

I denne studien har vi gjennomført en systematisk litteraturgjennomgang hvor omfanget besto av 37 artikler som ble lest i fulltekst. Ut i fra disse 37 artiklene har vi fått et godt overblikk over hvilke fokusområder og trender som går igjen i nyere forskning innen Big Data og cybersikkerhet. Fra vårt synspunkt tolker vi situasjonen som at sikkerhetsmiljøet står overfor en radikal endring innen angrep og trusler, med tilsvarende radikale endringer på forsvarssiden. Potensiale og mulighetene ved bruk av Big Data, maskinlæring og kunstig intelligens for å bekjempe cyberkriminalitet er et enormt fagfelt med mange ulike fokusområder, der vi har fokusert på noen hovedkategorier. Prosessen med å oppdage trusler og anomalier i en datastrøm er vektlagt grundig i litteraturen og fremstår som en klar trend innen nyere forskning. Samtidig fremstår det som at teknologien er uferdig og uprøvd i virkelige scenarioer da de fleste eksperimenter publisert i litteraturen bruker datasett som grunnlag og ikke datastrømmer i sanntid. Dette fremkommer også i kapittelet om fremtidig forskning hvor dette blir utpekt som et fremtidig forskningsområde i en rekke artikler. Dette viser at teknologien fortsatt er på et ungt og utprøvende stadium og implementering i virkelighetsscenarioer er fortsatt et stykke frem i tid. Derimot er nåværende resultater veldig lovende og potensiale for Big Data, maskinlæring og kunstig intelligens mye større enn det som er utforsket i dag. Fokuset på IDS er interessant å trekke fram, da det er såpass dominerende i nyere forskning og nevnes i et klart flertall av artiklene. Samtidig kan vi lese fra litteraturstudien gjort i 2013, oppsummert i kapittel 3 tidligere forskning, at samme fokus eksisterte på den tiden:

"The largest application of security analytics is in threat monitoring and incident investigations, which is of major concern to both financial and defense institutions. The focus is on discovering and learning both known and unknown cyber attack patterns, which is expected to remarkably influence the efficiency of identifying hidden threats faster, track down attackers and predict future attacks with increasing accuracy (minimum false positive rate)."(Mahmood & Afzal 2013).

Dette er det interessant å merke seg da det i praksis betyr at forskningen har beholdt fokus på det aktuelle området siden før 2013. Derimot har vi ingen eksempler i vår studie hvor hovedmålet er å identifisere angriperne, som blir nevnt som en av de to største bruksområdene av Mahmood & Afzal. Ahmed & Kit (2018) er i nærheten med sin artikkel hvor et IDS blir brukt for å identifisere trusler, men også samtidig samle inn bevis for angrepet som er blitt utført ved å lagre loggfiler som inneholder kriminelle handlinger som på sikt kan føre til identifisering av angriperne. Dette er derimot ikke fokusområdet til artikkelen da det ligger på identifisering og varsling av trusler, samt oppdage nye typer trusler som ikke tidligere er kjent. Nyere forskning har med andre ord forlatt et av de største bruksområdene ifølge Mahmood & Afzal. Hvorfor dette har skjedd er vanskelig å forklare. Vår teori er at dagens angripere er såpass sofistikerte og innehar et mye høyere kompetansenivå enn hva som tidligere var "normalt" og de vet hvordan man skjuler seg. Litteraturen nevner stadig en økning i kompetansen til

cyberangripere, blant annet Koh & Rhodes(2019). Det er med andre ord unødvendig å bruke tid og ressurser på å lete etter angriperne da man som oftest treffer en vegg i form av et nettverk med VPN'er og andre teknikker og metoder for å skjule sin identitet, som til slutt leder ingensteder. Derfor har fokuset blitt enda mer rettet mot identifisering, predikering og varsling av trusler og angrep for å jobbe preventivt mot angrep istedenfor reaktivt.

Bruksområdene til Big Data innen cybersikkerhet begrenses nærmest kun av fantasien. Muligheten fra å utføre omfattende analyser av datastrømmer og oppdage trusler eller anomalier, til å kunne personifisere opplæring innen phishing basert på personlighetstrekk, illustrerer bredden Big Data treffer og hvor mange ulike bruksområder som eksisterer. Med tanke på at vi kun har sett begynnelsen av utviklingen til Big Data illustrerer dette hvor omfattende og spennende Big Data i et sikkerhetsperspektiv er. Fremtidige systemer med Big Data vil mest sannsynlig drive seg selv og fungere fullstendig automatisert, hvor maskinlæring og kunstig intelligens konstant forbedrer systemets ytelse og evne til å utføre oppgaven den er satt til ved å analysere egen prestasjon.

Vi finner spesielt artikkelen relatert til brukeratferd, Shah et al (2019), veldig interessant hvor en brukers atferdsmønster blir kartlagt og målt opp mot nåværende oppførsel. Muligheten til å oppdage skadelig eller mistenkelig oppførsel fra en ellers legitim bruker kan forhindre stor skade på et nettverk og gjør konsekvensene av at brukere blir kompromittert av hackere mindre betydelig i et helhetlig perspektiv. Prinsippet med analyse av brukeratferd kan også brukes i andre settinger, for eksempel Ngejane, Mabuza-Hocquet, Eloff & Lefophane (2018) og Pantic & Husain(2019). Det er likevel en utfordring relatert til personvern her som burde nevnes, da ikke alle brukere er komfortable med at all aktivitet blir loggført og analysert for å bekrefte at kontoen opereres av korrekt bruker. Med innføringen av *GDPR*(General Data Protection Regulation) nå nylig, som stiller enda strengere krav til personvern og lagring av persondata, vil det i mange tilfeller være en utfordring å få samtykke fra samtlige brukere om å overvåke deres aktivitet for å opprettholde sikkerhet. Dette vil kanskje for mange være et overtramp av deres personvern og begrense bruken og utbytte av et slikt system ved at noen brukere unnlater å samtykke til overvåkning. Dette er utfordringer som må løses både praktisk og juridisk før et slik system kan implementeres i et virkelighetsscenario.

Utfordringer relatert til "adversial" oppførsel, hvor angripere utnytter det faktum at maskinlæring og kunstig intelligens blir brukt for å overvåke og beskytte et nettverk, er høyst interessant. Dette var et perspektiv vi ikke hadde sett for oss når vi begynte på vår studie, men det har vist seg å være en viktig del av litteraturen og av utfordringene som må løses før slike systemer kan brukes i virkelighetsscenarioer. Slike angripere truer hele konseptet med maskinlæring hvor systemet lærer over tid og konstant forbedrer sin egen ytelse ved å mate systemet med manipulerte data som reduserer ytelsen til modellen. På denne måten har angriperne nærmest direkte tilgang til treningsdataen

modellen bruker, og på den måten kan de påvirke hvordan modellen fungerer. Både Duddu (2018) og Anindya & Kantarcioglu (2018) nevner disse utfordringene i sine artikler og viser til ulike måter å håndtere problemet på. Vi finner det veldig interessant at en del av utfordringen med maskinlæring er å filtrere ut data som modellen *ikke* skal lære av, men heller ignorere for å opprettholde ytelsen. Dette gir en ny dimensjon til maskinlæring og hvor komplisert det er å utvikle slike modeller, samt kompetansen det kreves for å oppnå og opprettholde høy ytelse.

Big data analyse sammen med maskinlæring gjør det mulig å trekke konklusjoner og finne ny informasjon på bakgrunn av hvilke data som blir analysert. De typene analyseapplikasjoner som inngår i litteraturen er såpass kraftige og intelligente at man gjerne vil påstå at anonymitet er umulig å oppnå. Dette har skapt en stor debatt omkring personvern ved bruk av big data analyse. Dev Mishra & Beer Singh (2017) forklarer hvordan big data analyse kan være en stor fordel for organisasjoner, men også hva slags utfordringer som kan oppstå. Organisasjoner som velger å ta i bruk big data analyse må ta hensyn til mange nye utfordringer, spesielt når det kommer til personvern. En av disse er faren for at data som blir samlet inn kan eksistere for alltid. Dette fordi det er vanskelig å holde kontroll over hvor dataen blir tatt i bruk, og i hvilke systemer dette blir lagret. Dette blir en ekstra utfordring med tanke på de nye GDPR reglene og da spesielt paragrafene som omhandler hvor lenge persondata kan bli lagret. For å kunne bruke big data analyse må derfor organisasjoner ta hensyn til dette under utarbeiding av analyseapplikasjonene.

I kapittel 6 var vi innom viktigheten av å ha den nyeste og mest oppdaterte informasjonen rundt cyberkriminalitet. Dette gjaldt da spesielt for å kunne stå imot ZDA. Nunes et al., (2018) foreslår å bruke data fra darknet og deepnet. Det er på disse kanalene at mange cyberkriminelle samarbeider og legger ut ny malware gratis, eller for salg, som kan brukes for å utnytte kjente eller ukjente sikkerhetshull. Vi tenker at det bør kunne være mulig for forskere og sikkerhetsaktører å bruke åpne hackerforum eller infiltrere lukkede forum. Og på denne måten få tak i malware for så og ta i bruk omvendt konstruksjon ("reverse engineering") for å finne ut av hvordan sikkerhetshull blir utnyttet, så fort som mulig. Om denne metoden er for treg kunne man ha testet malware i et isolert nettverk for å se hva slags karakteristikker malwaren har og utvikle nye læringsmodeller og algoritmer basert på oppførselen. Her kan det igjen oppstå problemer om det skulle bli kjent at sikkerhetsfirmaer bruker informasjon fra slike forumer. Falsk malware med en oppførsel som villeder analysen av sikkerhetsdata til fordel for de cyberkriminelle til eksempel.

En av de mest sentrale utfordringene relatert til Big Data ligger veldig i ordet, mengden data som må håndteres og prosesseres. Slik prosessering legger krav på enorme mengder datakraft og krever kraftig og ikke minst dyr infrastruktur. I nyere tid har noe av denne problematikken blitt løst med introduseringen av skyløsninger og Big Data as a service, hvor infrastruktur og plattform kan leies over nett. På den måten slipper man å investere i dyr infrastruktur selv, samt kompetansen det krever for å sette opp, drive

og forbedre et slikt system. Det løser derimot ikke hele problemet, da det ideelle IDS system analyserer data hurtig, i sanntid og med høy nøyaktighet. Det vil i noen tilfeller ikke være mulig å oppnå hvis ytelsen skal opprettholdes uten å skape flaskehalser. En flaskehals i et sikkerhetsperspektiv kan være veldig farlig for et nettverk da flaskehalsen som regel må fjernes for å opprettholde stabilitet og tilgang til tjenester. Hvis et IDS system blir slått av for å hindre at nettverket stopper opp, eksponeres nettverket for angrep. Forskerne har derfor sett på muligheter for å redusere mengden data som må analyseres ved å bruke maskinlæring og kunstig intelligens, samt andre metoder som f.eks kodespråket R eller SROM modeller Bordel et al., (2019). Ved å redusere mengden data som trengs å analyseres ved å fjerne duplikater kan man oppnå høyere ytelse med samme infrastruktur og potensielt unngå flaskehalser.

Et stort fokus i litteraturen går på prosessen med å identifisere og gjenkjenne trusler eller angrep, slik som vi tidligere har nevnt i form av IDS. Det vi derimot ikke ser noe til er prosessen videre etter at en trussel er identifisert og hvordan reaktive tiltak blir iverksatt for å begrense eller nøytralisere gitt trussel. Dette går muligens utenfor scopet til forskerne og ligger kanskje lenger frem i tid enn hvor vi er nå. Det er uansett interessant å nevne da nåværende forskning på dette feltet ikke forklarer hvordan et slikt system skal se ut eller fungere. Vi ser for oss et scenario hvor maskinlæring/kunstig intelligens identifiserer og gjenkjenner en trussel, altså et IDS system, men samtidig kartlegger egenskapene til trusselen og på bakgrunn av den informasjonen kan iverksette passende tiltak for å begrense eller nøytralisere trusselen. Disse tiltakene blir muligens utført av et separat system, men trigges av IDS systemet og får instruksene sine derfra. Dette vil i så fall være neste steg etter at teknologien er blitt stabil og klar for virkelighetsscenarioer med analyse av datastrømmer i sanntid. Dette kan være interessant for forskere å se nærmere på i årene som kommer.

Behandling av data i ulike format som er både ustrukturert og strukturert er noe av det som krever mest når man skal analysere datastrømmer. Vi ser at dette påpekes flere ganger i litteraturen og viser seg som et av de største problemene innen prosessering av data. Vi tenkte i utgangspunktet at det vil være bortimot umulig å oversette alle maskinspråk og datatyper til et generalisert maskinprosesserbart språk på grunn av det store mangfoldet. Zheng et al., (2018) påpeker at tidligere arbeid har demonstrert at ontologien fungerer som et maskinprosesesserbart språk. Likevel krever de mye brukte metodene for ontologi generering at sikkerhetseksperter manuelt analyserer innsamlet data og trekker ut representativ informasjon, noe som fører til at kompleksiteten øker, effektiviteten reduseres og kostnader knyttet til tidsbruk øker.

6 Konklusjon

Denne systematiske litteraturstudien har tatt for seg 37 artikler innen Big Data og cybersikkerhet hvor målet har vært å få en oversikt over nåværende standpunkt på forskningsområdet samt avdekke eventuelle trender i litteraturen. Studiens funn har blitt delt opp i tre hovedkategorier: Utfordringer, foreslåtte løsninger og trender. Totalt 13 utfordringer og 9 foreslåtte løsninger ble identifisert i studien, samt trender som preger forskningen de siste 6 årene.

Ut ifra funnene gjort i studien har vi diskutert nåværende situasjon på forskningsområdet Big Data og cybersikkerhet ut ifra teori samt våre egne erfaringer og kompetanse om temaet. Studien har avdekket at Big Data er et revolusjonerende verktøy for å bekjempe cyberkriminalitet, men det er i mange tilfeller ikke er modent nok til å implementeres i virkelighetsscenarioer grunnet manglende stabilitet, kompetanse, ressurskostnad og uløste utfordringer relatert til blant annet ytelse. Videre forskning og utvikling av eksisterende teknologi og maskinvare vil på sikt kunne gjøre Big Data til et av de viktigste verktøyene innen IT sikkerhet for å holde tritt med økningen av trusler og angrep som forekommer i cyberspace.

Studien har avdekket at det eksisterer trender innen nyere forskning. Da spesielt IDS som dominerer forskningsfeltet, men også litt mindre markante trender som visualisering av Big Data systemer, redusering av data og bruken av rammeverk og systemdesign. Dette er alle trender innen foreslåtte løsninger.

Videre viser funnene i studien en rekke utfordringer som blir nevnt hyppig i litteraturen. Av utfordringer er det verdt å nevne blant annet ZDA, Big Data prosessering, identifisering av avvik/anomalier og konfigurering av ML algoritmer.

6.1 Bidraget til denne studien

Denne studien har hjulpet med å belyse utfordringene og potensielle løsninger som fremkommer i litteraturen på området Big Data og cybersikkerhet. Trender innen litteraturen har blitt identifisert, samt eventuelle forskningshull og forslag til fremtidig forskning.
Videre har studien avdekket nåværende status innen forsking på Big Data og cybersikkerhet og har hjulpet med å skape en oversikt over hva som er blitt gjort hittil, og hva som det bør forskes videre på for å skape et bedre sikkerhetssystem for morgendagens trusler og angrep.

6.2 Begrensninger ved studien

Vår studie inneholder en del begrensninger som er verdt å belyse. Vi har kun hentet litteratur fra databasen Scopus da dette ble fremstilt som den "beste" databasen å hente data fra av vår foreleser i faget "IS 420 - Aktuelle tema og forskningsområder innen informasjonssystemer". Nesten samtlige artikler publisert på Scopus er fagfellevurdert. Dette hever kvaliteten på publikasjonene, noe andre databaser, som Google Scholar, ikke tar hensyn til.

Utredningen har blitt utført innenfor et begrenset tidsrom på seks måneder i sammenheng med IS-501 Masteroppgave i informasjonssystemer på Universitetet i Agder. Tilgangen til ressurser har vært begrenset til hva UiA kan tilby, da i form av for eksempel tilgang til artikler som krever abonnement. I enkelte tilfeller har artikler blitt utelatt fra studien på grunn av manglende tilgang til fulltekst.

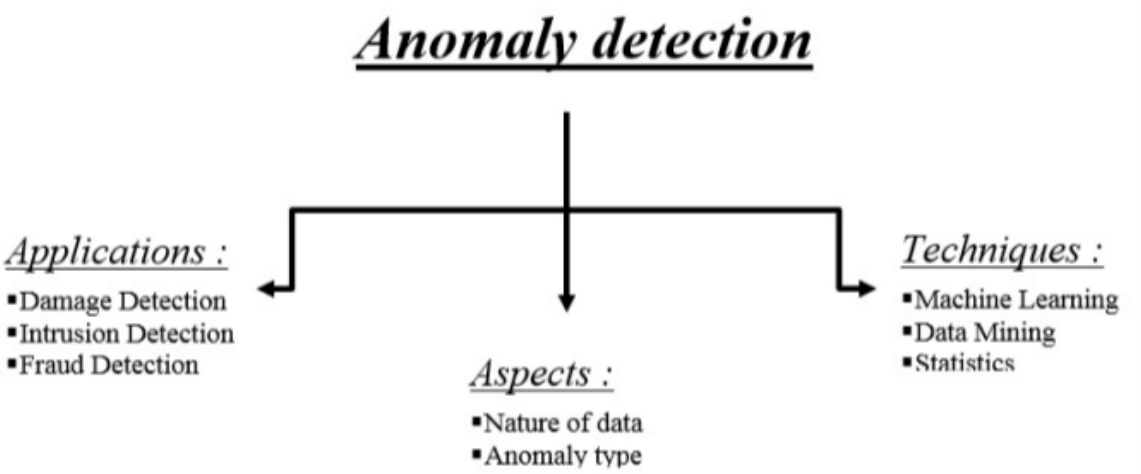
Artikler utenfor vårt omfang har blitt utelatt fra studien. Dette inkluderer artikler og publiseringer som ikke angår Big Data og cybersikkerhet hvor Big Data blir brukt for å bekjempe cyberkriminalitet. Eksempler er artikler som omhandler cyberangrep på Big Data kilder, som sosiale medier e.l, hvor Big Data ikke blir brukt for å bekjempe angrepet, men kun som et mål.

Artikler publisert tidligere enn 2014 er ikke tatt med i studien.

6.3 Aktuelle områder for fremtidig forskning

Å hente inn data rundt nyere typer angrep og skadevare virker å være forslag til fremtidig forskning som gjentar seg mest i litteraturen. Dette blir nevnt av; Ciancioso, Budhwa & Hayajneh (2018), Teoh et al., (2018), Sezari et al., (2018), Najada et al., (2019), Terzi, Terzi & Sagiroglu (2017) og Carvalho (2016). Cianciose et al (2018) foreslår å bygge et "*anti malware tool*" (AMT) som automatisk lager varianter av allerede eksisterende skadevare, samt varianter av disse igjen, som så blir lagret i en database. Dette gjør det mulig for et sikkerhetsfirma å revidere sitt eget AMT. Som en fortsettelse på dette forslår Cianciose et al., (2018) å utvikle et AMT som kan emulere et virkelighetsbasert nettverksmiljø ved bruk av dynamisk heuristiske- og sandkassemetoder for å oppdage skadevare som prøver å komme seg rundt eksisterende forsvar. Sezari et al., (2018) ønsker også å bruke en lignende metode ved å simulere et nettverk som brukes på en flyplass. Her er det mange ukjente enheter som hele tiden kobler seg opp. Dette kan føre til at nye angrep og skadevare kan bli introdusert i nettverk. Modellen som Sezari et al., (2018) har foreslått vil dermed bli testet på de nyeste, mest populære og farligste angrepene. Dette for å validere og optimalisere modellen. Videre trengs det kryss-validering av resultater og introduksjoner av andre modeller.

Forslaget om å utforske samt videreutvikle flere modeller og algoritmer er et ganske åpenbart tema for videre forskning og blir nevnt av blant annet; Teoh et al., (2018), Britel (2019), Las Casas et al., (2016), Terzi et al., (2017) og Dev Mishra & Beer Singh (2017). Britel (2019) presenterer i sin artikkel noen av variablene som må tas hensyn til under arbeid med oppdagelse av anomalier i et nettverk og viser til dette i figuren under.



Figur 20 Variabler som må tas hensyn til under arbeid med oppdagelse av anomalier. Britel (2019, s.2)

Britel (2019) har fokusert mest på en algoritme som kalles KOAD. Britel (2019) presiserer at for å kunne håndtere alle aspektene ved leting etter abnormiteter må det jobbes videre med å utforske flere læringsbaserte alternativer som adresserer denne utfordringen.

Infrastrukturene som brukes innen IDS må også undersøkes mer. Foreløpige konklusjoner i forskningslitteraturen sier at bruken av Big Data analyse som en tjeneste i skyen er et utgangspunkt for en infrastruktur som kan være med på å løse problemet med manglende kompetanse, kostnader og datakraft. En slik infrastruktur som baserer seg på Big Data analyse som en tjeneste som fokuserer på sanntidsanalyse av sikkerhetsdata, virker fremdeles å være en løsning som krever mer forskning. En fullstendig tjeneste av denne typen er foreløpig ikke tilgjengelig. En slik infrastruktur krever også som nevnt i 5.1, store mengder datakraft og kan føre til at ytelsen blir påvirket i et større nettverk da alle datastrømmene må analyseres i sanntid. Det er kritisk at IDS holder seg oppe selv under stor pågang. Går IDS ned vil nettverket være svært sårbart. Det er derfor nødvendig med mer forskning på hvordan Big Data analyse kan brukes som en tjeneste i en infrastruktur som opererer på et realistisk nettverk.

7 Referanser

Ahmed, A. A., & Kit, Y. W. (2018). Collecting and analyzing digital proof material to detect cybercrimes. *Proceedings - IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, IEEE 16th International Conference on Pervasive Intelligence and Computing, and IEEE 4th International Conference on Big Data Intelligence*, ss. 736-741.

Ahn, S.-H., Kim, N.-U., & Chung, T.-M. (2014). Big Data Analysis System Concept for Detecting Unknown Attacks. *International Conference on Advanced Communication Technology*, ss. 269-272.

Aksu, D., & Aydin, M. A. (2019). Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms. *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism*, ss. 77-80.

Anindya, I. C., & Kantarcioglu, M. (2018). Adversarial anomaly detection using centroid-based clustering. *IEEE 19th International Conference on Information Reuse and Integration for Data Science*, ss. 1-8.

Apurva, A., Ranakoti, P., Yadav, S., Tomer, S., & Roy, N. R. (2017). Redefining Cyber Security with Big Data Analytics. *International Conference on Computing and Communication Technologies for Smart Nation*, ss. 199-203.

Arthur, L. (2013, August 15). *What is Big Data?* Hentet fra Forbes: https://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data/#c9833f25c85b

BBVA. (2017, Mai 8). *The five V's og Big DAta*. Hentet fra BBVA: https://www.bbva.com/en/five-vs-big-data/

Bergem, H., & Traskjær, Ø. (2018). Litteraturgjennomgang rapport - "What are the findings in empirical IS and related research about the challenges and the potential ways for addressing them in grocery e-commerce?".

Bordel, B., Alcarria, R., Robles, T., & Sánchez-Picot, Á. (2018). Stochastic and information theory techniques to reduce large datasets and detect cyberattacks in ambient intelligence environments. *IEEE Access*, ss. 34896-34910.

Britel, M. (2019). Big data analytic for intrusion detection system. *International Conference on Electronics, Control, Optimization and Computer Science*.

Bronson, R. (2018, Desember 25). *4 Reasons Cybersecurity Is More Important Than Ever*. Hentet fra TechWell: https://www.techwell.com/techwell-insights/2018/12/4-reasons-cybersecurity-more-important-ever

Carvalho, V., Polidoro, M., & Magalhaes, J. (2016). OwlSight: Platform for Real-time Detection and Visualization of Cyber Threats. *2nd IEEE International Conference on Big Data Security on Cloud, 2nd IEEE International Conference on High Performance and Smart Computing, and IEEE International Conference on Intelligent Data and Security*, ss. 61-68.

Ciancioso, R., Budhwa, D., & Hayajneh, T. (2018). A framework for zero day exploit detection and containment. *IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, IEEE 15th International Conference on Pervasive Intelligence and Computing,*

and IEEE 3rd International Conference on Big Data Intelligence and Computing, ss. 663-668.

Dalton, A., Dorr, B., Liang, L., & Hollingshead, K. (2018). Improving cyber-attack predictions through information foraging. *IEEE International Conference on Big Data*, ss. 4642-4647.

Datatilsynet. (2013). Big Data - personvernprinsipper under press.

Dev Mishra, A., & Beer Singh, Y. (2017). Big Data Analytics for Security and Privacy Challenges. *IEEE International Conference on Computing, Communication and Automation*, ss. 50-53.

Duddu, V. (2018). A survey of adversarial machine learning in cyber warfare. *Defence Science Journa*, ss. 356-366.

Dvergsdal, H. (2019, April 30). *nevralt nettverk*. Hentet fra SNL: https://snl.no/nevralt_nettverk

Elster, A. C., & Tidemann, A. (2019, Januar 17). *Maskinlæring*. Hentet fra SNL: https://snl.no/maskinlæring

Everett, C. (2015). Big data – the future of cyber-security or its latest threat? . *Computer Fraud and Security*, ss. 14-17.

Feng, Y., Akiyama, H., Lu, L., & Sakurai, K. (2018). Feature selection for machine learning-based early detection of distributed cyber attacks. *Proceedings - IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, and IEEE 16th International Conference on Pervasive Intelligence and Computing*, ss. 181-186.

Grodzinski, M. (2013, Januar 25). *Big Data – Så mye mer enn bare kundesegmentering!* Hentet fra Capgemini: https://www.capgemini.com/no-no/2013/01/big-data-sa-mye-mer-enn-bare-kundesegmentering/

Gupta, D., & Rani, R. (2018). Big Data Framework for Zero-Day Malware Detection. *Cybernetics and Systems*, ss. 103-121.

Harms, C. (2007). Grooming: An operational definition and coding scheme. *Sex Offender Law Report*, ss. 1-6.

Johannessen, N., Åsebø, S., Bach, D., Stangvik, E. O., Skjetne, O. L., & Johnsen, A. B. (2017, Februar 13). *VG avslører: Politikere og toppbyråkrater rammet av hackerangrep*. Hentet fra VG: https://www.vg.no/nyheter/innenriks/i/ldwlo/vg-avsloerer-politikere-og-toppbyraakrater-rammet-av-hackerangrep

Kazemi, Z., & Zarrabi, H. (2018). Using deep networks for fraud detection in the credit card transactions. *IEEE 4th International Conference on Knowledge-Based Engineering and Innovation*, ss. 630-633.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele University*, ss. 1-26.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering.

Kleinman, A. (2014, Oktober 11). *200,000 Snapchat Photos Leaked On 4Chan*. Hentet fra Huffpost: https://www.huffpost.com/entry/snapchat-leak_n_5965590

Koh, J., & Rhodes, B. (2019). Inline Detection of Domain Generation Algorithms with Context-Sensitive Word Embeddings. *IEEE International Conference on Big Data*, ss. 2966-2971.

Las-Casas, P., Dias, V. M., & Guedes, D. (2016). A Big Data architecture for security data and its application to characterization. *2nd IEEE International Conference on Big Data Security on Cloud, 2nd IEEE International Conference on High Performance and Smart Computing, and IEEE International Conference on Intelligent Data and Security*, ss. 36-41.

Mahmood, T., & Afzal, U. (2013). Security Analytics: Big Data Analytics for Cybersecurity - A Review of Trends, Techniques and Tools . *2nd National Conference on Information Assurance* .

Maimo, L., Clemente, F., Perez, M., & Perez, G. (2018). On the performance of a deep learning-based anomaly detection system for 5G networks. *IEEE SmartWorld Ubiquitous Intelligence and Computing, Advanced and Trusted Computed, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovation*, ss. 1-8.

More, R., Unakal, A., Kulkarni, V., & Goudar, R. (2018, Januar). Real Time Threat Detection System in Cloud using Big Data Analytics. *2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology*, ss. 1262-1264.

Najada, H., Mahgoub, I., & Mohammed, I. (2019). Cyber Intrusion Prediction and Taxonomy System Using Deep Learning and Distributed Big Data Processing. *Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence*, ss. 631-638.

Ngejane, C., Mabuza-Hocquet, G., Eloff, J., & Lefophane, S. (2018). Mitigating Online Sexual Grooming Cybercrime on Social Media Using Machine Learning: A Desktop Survey. *International Conference on Advances in Big Data, Computing and Data Communication Systems*.

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., . . . Shakarian, P. (2016). Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence. *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data*, ss. 7-12.

Pantic, N., & Husain, M. (2019). A Decision Support System for Personality Based Phishing Susceptibility Analysis. *2018 IEEE International Conference on Big Data*, ss. 3066-3071.

Sabar, N., Yi, X., & Song, A. (2018). A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security. *IEEE Access*, ss. 10421-10431.

Sarmadawy, H. (2017, Mai 13). *Dette er løsepengeviruset wannacry*. Hentet fra VG: https://www.vg.no/nyheter/innenriks/i/zp3z5/dette-er-loesepengeviruset-wannacry

Sezari, B., Moller, D., & Deutschmann, A. (2018). Anomaly-Based Network Intrusion Detection Model Using Deep Learning in Airports. *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering*, ss. 1725-1729.

Shah, S., Shah, B., Amin, A., Al-Obeidat, F., Chow, F. M., & Anwar, S. (2019). Compromised user credentials detection in a digital enterprise using behavioral analytics. *Future Generation Computer Systems*, ss. 407-417.

Symantac. (n.d). *Zero-day vulnerability: What it is, and how it works*. Hentet fra US Norton: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

Teoh, T., Chiew, G., Franco, E., Ng, P., Benjamin, M., & Goh, Y. (2018). Anomaly detection in cyber security attacks on networks using MLP deep learning. *International Conference on Smart Computing and Electronic Enterprise*.

Teoh, T., Chiew, G., Jaddoo, Y., Michael, H., Karunakaran, A., & Goh, Y. (2018). Applying RNN and J48 Deep Learning in Android Cyber Security Space for Threat Analysis. *International Conference on Smart Computing and Electronic Enterprise*.

Terzi, D., Terzi, R., & Sagiroglu, S. (2017). Big Data Analytics for Network Anomaly Detection from Netflow Data. *2nd International Conference on Computer Science and Engineering*, ss. 592-597.

Tomter, L., & Gundersen, M. (2019, April 14). *IT-sjefen i Hydro om dataangrepet: – Man tror krisen blir stor, så blir den enda verre*. Hentet fra NRK: https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043

Wang, L., & Jones, R. (2018). Big Data Analytics of Network Traffic and Attacks. *Proceedings of the IEEE National Aerospace Electronics Conference*, ss. 117-123.

Weisman, S. (n.d). *What is a distributed denial of service attack (DDoS) and what can you do about them?* Hentet fra US Norton: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

Wikipedia. (2019). *Game theory*. Hentet fra Wikipedia: https://en.wikipedia.org/wiki/Game_theory

Zheng, H., Wang, Y., Han, C., Le, F. H., & Lu, J. (2018). Learning and Applying Ontology for Machine Learning in Cyber Attack Detection. *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering*, ss. 1309-1315.

8 Vedlegg

Vedlegg 1: Konseptmatrise cyberkrim

1	Kategori	Cyberkrim						
2	Konsepter / Referanser	Intrusion angrep	Seksuell grooming	Phishing	Ddos	Kredittkort svindel	Malware	Brute force angrep
3	Gupta & Rani (2018)						x	
4	Apurva, Ranakoti, Yadav, Tomer, Roy (2018)	x						
5	More, Unakal, Kulkarni, Goudar (2018)	x						
6	Dalton, Dorr, Liang, Hollingshead (2018)	x						
7	Cesur, Ceyhan, Kermen, Sağiroğlu (2017)	x						
8	Dev Mishra, Beer Singh (2017)							
9	Terzi, Terzi, Sagiroglu (2017)	x			x			
10	Nunes et al. (2016)	x					x	
11	Carvalho, Polidoro, Magalhaes (2016)	x					x	
12	Las-Casas, Dias, Meira, Guedes (2016)	x		x			x	
13	Everett (2015)	x		x	x		x	
14	Kim, Kim, Chung (2014)	x						
15	Ahn, Kim, Chung (2014)	x						
16	Shah et al. (2019)	x						
17	Najada, Mahgoub, Mohammed (2019)	x			x			x
18	Aksu, Aydin (2019)	x						
19	Pantic, Husain (2019)			x				
20	Koh, Rhodes (2019)						x	
21	Britel (2019)	x			x		x	
22	Wang, Jones (2018)	x						
23	Teoh et al. (2018)	x					x	
24	Teoh et al. (2018)						x	
25	Ahmed, Kit (2018)	x						
26	Feng, Akiyama, Lu, Sakurai (2018)				x			
27	Ngejane, Mabuza-Hocquet, Eloff, Lefophane (2018)		x					
28	Zheng et al. (2018)	x						
29	Sezari, Moller, Deutschmann (2018)	x					x	
30	Anindya, Kantarcioglu (2018)	x						
31	Duddu (2018)	x			x		x	
32	Maimo, Clemente, Perez, Perez (2018)	x						
33	Teoh, Zhang, Nguwi, Elovici (2018)	x						
34	Teoh, Nguwi, Elovici, Cheung (2018)	x					x	
35	Vani, Krishnamurthy (2018)	x						
36	Bordel, Alcarria, Robles, Sanchez-Picot (2018)	x						
37	Chen, Zhang, Liu, Tang (2018)	x						
38	Kazemi, Zarrabi (2018)					x		
39	Sabar, Yi, Song (2018)	x						

Vedlegg 2: Konseptmatrise utfordringer

1	Kategori	Utfordinger											
2	Konsepter / Referanser	Big Data prosessering	Oppdage avvik/anomalier i nettverk	Kompromitterte brukere	Konfigurering av ML algoritmer	Zero day attacks	Kostnader	Kompetanse	Personvern	Adversial/Intelligente motstandere	Oppdage unormal kontakt med barn	Personlighetstrekk	Domenegeneratorer
3	Gupta & Rani (2018)	x			x	x							
4	Apurva, Ranakoti, Yadav, Tomer, Roy (2018)	x	x				x	x					
5	More, Unakal, Kulkarni, Goudar (2018)	x											
6	Dalton, Dorr, Liang, Hollingshead (2018)				x								
7	Cesur, Ceyhan, Kermen, Sağiroğlu (2017)	x			x								
8	Dev Mishra, Beer Singh (2017)								x				
9	Terzi, Terzi, Sagiroglu (2017)	x	x										
10	Nunes et al. (2016)	x			x	x							
11	Carvalho, Polidoro, Magalhaes (2016)	x			x	x							
12	Las-Casas, Dias, Meira, Guedes (2016)	x				x							
13	Everett (2015)	x		x		x	x	x					
14	Kim, Kim, Chung (2014)	x	x										
15	Ahn, Kim, Chung (2014)	x	x	x				x					
16	Shah et al. (2019)		x	x									
17	Najada, Mahgoub, Mohammed (2019)		x	x	x								
18	Aksu, Aydin (2019)		x		x								
19	Pantic, Husain (2019)											x	
20	Koh, Rhodes (2019)												x
21	Britel (2019)	x	x										
22	Wang, Jones (2018)	x											
23	Teoh et al. (2018)		x										
24	Teoh et al. (2018)	x	x										
25	Ahmed, Kit (2018)	x	x										
26	Feng, Akiyama, Lu, Sakurai (2018)		x		x								
27	Ngejane, Mabuza-Hocquet, Eloff, Lefophane (2018)										x		
28	Zheng et al. (2018)		x										
29	Sezari, Moller, Deutschmann (2018)		x			x							
30	Anindya, Kantarcioglu (2018)		x			x				x			
31	Duddu (2018)	x	x	x	x	x				x			
32	Maimo, Clemente, Perez, Perez (2018)	x	x										
33	Teoh, Zhang, Nguwi, Elovici (2018)		x										
34	Teoh, Nguwi, Elovici, Cheung (2018)	x	x		x								
35	Vani, Krishnamurthy (2018)		x			x							
36	Bordel, Alcarria, Robles, Sanchez-Picot (2018)	x											
37	Chen, Zhang, Liu, Tang (2018)		x										
38	Kazemi, Zarrabi (2018)		x										
39	Sabar, Yi, Song (2018)				x			x					

Vedlegg 3: Konseptmatrise foreslåtte løsninger

1	Kategori	Foreslått løsning									
2	Konsepter / Referanser	Big data visualisering	IDS	Maskinlæring/AI	Rammeverk	Systemdesign	Game-theoretic models	Ontologi	Redusere datamengder	Korrelasjonsanalyser	Personifisert opplæring
3	Gupta & Rani (2018)		x	x							
4	Apurva, Ranakoti, Yadav, Tomer, Roy (2018)										
5	More, Unakal, Kulkarni, Goudar (2018)		x	x		x					
6	Dalton, Dorr, Liang, Hollingshead (2018)				x						
7	Cesur, Ceyhan, Kermen, Sağiroğlu (2017)			x		x					
8	Dev Mishra, Beer Singh (2017)										
9	Terzi, Terzi, Sagiroglu (2017)		x								
10	Nunes et al. (2016)		x	x							
11	Carvalho, Polidoro, Magalhaes (2016)	x	x	x	x						
12	Las-Casas, Dias, Meira, Guedes (2016)	x			x						
13	Everett (2015)			x							
14	Kim, Kim, Chung (2014)	x	x	x		x				x	
15	Ahn, Kim, Chung (2014)	x	x			x					
16	Shah et al. (2019)		x		x						
17	Najada, Mahgoub, Mohammed (2019)		x	x	x						
18	Aksu, Aydin (2019)		x	x							
19	Pantic, Husain (2019)				x						x
20	Koh, Rhodes (2019)			x							
21	Britel (2019)		x	x							
22	Wang, Jones (2018)			x					x		
23	Teoh et al. (2018)		x	x							
24	Teoh et al. (2018)		x	x							
25	Ahmed, Kit (2018)		x			x					
26	Feng, Akiyama, Lu, Sakurai (2018)			x							
27	Ngejane, Mabuza-Hocquet, Eloff, Lefophane (2018)			x							
28	Zheng et al. (2018)		x	x				x			
29	Sezari, Moller, Deutschmann (2018)		x	x							
30	Anindya, Kantarcioglu (2018)		x	x			x				
31	Duddu (2018)		x	x							
32	Maimo, Clemente, Perez, Perez (2018)		x	x		x					
33	Teoh, Zhang, Nguwi, Elovici (2018)		x	x							
34	Teoh, Nguwi, Elovici, Cheung (2018)		x	x							
35	Vani, Krishnamurthy (2018)		x	x							
36	Bordel, Alcarria, Robles, Sanchez-Picot (2018)			x	x				x		
37	Chen, Zhang, Liu, Tang (2018)		x	x							
38	Kazemi, Zarrabi (2018)			x							
39	Sabar, Yi, Song (2018)		x	x							

Vedlegg 4: Liste over artikler identifisert i studien

Forfatter(e)	Tittel	Årstall
Ahmed, A.A., Kit, Y.W.	Collecting and analyzing digital proof material to detect cybercrimes	2018
Ahn, S.-H., Kim, N.-U., Chung, T.-M.	Big Data Analysis System Concept for Detecting Unknown Attacks	2014
Aksu, D., Aydin, M.A.	Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and	2019

	Support Vector Machine Algorithms	
Anindya, I.C., Kantarcioglu, M.	Adversarial anomaly detection using centroid-based clustering	2018
Apurva, A., Ranakoti, P., Yadav, S., Tomer, S., Roy, N.R.	Redefining Cyber Security with Big Data Analytics	2018
Bordel, B., Alcarria, R., Robles, T., Sanchez-Picot, A.	Stochastic and information theory techniques to reduce large datasets and detect cyberattacks in ambient intelligence environments	2018
Britel, M.	Big data analytic for intrusion detection system	2019
Carvalho, V.S., Polidoro, M.J., Magalhaes, J.P.	OwlSight: Platform for Real-time Detection and Visualization of Cyber Threats	2016
Cesur, R., Ceyhan, E.B., Kermen, A., Sağiroğlu, Ş.	Determination of Potential Criminals in Social Network	2017
Chen, X., Zhang, L., Liu, Y., Tang, C.	Ensemble learning methods for power system cyber-Attack detection	2018
Ciancioso, R., Budhwa, D., Hayajneh, T.	A framework for zero day exploit detection and containment	2018
Dalton, A., Dorr, B., Liang, L., Hollingshead, K.	Improving cyber-attack predictions through information foraging.	2018
Dev Mishra, A., Beer Singh, Y.	Big Data Analytics for Security and Privacy Challenges	2017

Duddu, V.	A survey of adversarial machine learning in cyber warfare	2018
Everett, C.	Big data – the future of cyber-security or its latest threat?	2015
Feng, Y., Akiyama, H., Lu, L., Sakurai, K.	Feature selection for machine learning-based early detection of distributed cyber attacks	2018
Gupta, D., Rani, R.	Big Data Framework for Zero-Day Malware Detection	2018
Kazemi, Z., Zarrabi, H.	Using deep networks for fraud detection in the credit card transactions	2018
Kim, H., Kim, I., Chung, T.-M.	Abnormal Behavior Detection Technique Based on Big Data	2014
Koh, J.J., Rhodes, B.	Inline Detection of Domain Generation Algorithms with Context-Sensitive Word Embeddings	2019
Las-Casas, P.H.B., Dias, V.S., Meira, W., Guedes, D.	A Big Data architecture for security data and its application to characterization	2016
Maimo, L.F., Clemente, F.J.G., Perez, M.G., Perez, G.M.	On the performance of a deep learning-based anomaly detection system for 5G networks	2018
More, R., Unakal, A., Kulkarni, V., Goudar, R.H.	Real Time Threat Detection System in Cloud using Big Data Analytics	2018

Najada, H.A., Mahgoub, I., Mohammed, I.	Cyber Intrusion Prediction and Taxonomy System Using Deep Learning and Distributed Big Data Processing	2019
Ngejane, C.H., Mabuza-Hocquet, G., Eloff, J.H.P., Lefophane, S.	Mitigating Online Sexual Grooming Cybercrime on Social Media Using Machine Learning: A Desktop Survey	2018
Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., Robertson, J., Shakarian, J., Thart, A., Shakarian, P.	Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence	2016
Pantic, N., Husain, M.	A Decision Support System for Personality Based Phishing Susceptibility Analysis	2019
Sabar, N.R., Yi, X., Song, A.	A Bi-objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security	2018
Sezari, B., Moller, D.P.F., Deutschmann, A.	Anomaly-Based Network Intrusion Detection Model Using Deep Learning in Airports	2018
Shah, S., Shah, B., Amin, A., Al-Obeidat, F., Chow, F., Moreira, F.J.L., Anwar, S.	Compromised user credentials detection in a digital enterprise using behavioral analytics	2019
Teoh, T.T., Chiew, G., Franco, E.J., Ng, P.C., Benjamin, M.P., Goh, Y.J.	Anomaly detection in cyber security attacks on networks using MLP deep learning	2018

Teoh, T.T., Chiew, G., Jaddoo, Y., Michael, H., Karunakaran, A., Goh, Y.J.	Applying RNN and J48 Deep Learning in Android Cyber Security Space for Threat Analysis	2018
Teoh, T.T., Nguwi, Y.Y., Elovici, Y., Cheung, N.M., Ng, W.L.	Analyst intuition based Hidden Markov Model on high speed, temporal cyber security big data	2018
Teoh, T.T., Zhang, Y., Nguwi, Y.Y., Elovici, Y., Ng, W.L.	Analyst intuition inspired high velocity big data analysis using PCA ranked fuzzy k-means clustering with multi-layer perceptron (MLP) to obviate cyber security risk	2018
Terzi, D.S., Terzi, R., Sagiroglu, S.	Big Data Analytics for Network Anomaly Detection from Netflow Data	2017
Vani, Y.S.K., Krishnamurthy	Survey: Anomaly detection in network using big data analytics	2018
Wang, L., Jones, R.	Big Data Analytics of Network Traffic and Attacks	2018
Zheng, H., Wang, Y., Han, C., Le, F., He, R., Lu, J.	Learning and Applying Ontology for Machine Learning in Cyber Attack Detection	2018