Measuring Privacy

Markus Schnappinger
Betreuer: Marcel von Maltitz
Seminar Future Internet „WS2014/15
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: ga67wap@mytum.de

KURZFASSUNG

Ein Energiekontrollsystem in einem Gebäude sammelt kontinuierlich Sensordaten. Bei der Abdeckung verschiedener Anwendungsfälle muss jedoch eine Privatsphäre-wahrende Darstellung dieser teils sensiblen Informationen gefunden werden. Nach einer Untersuchung von etablierten Methoden aus anderen Fachbereichen werden Möglichkeiten aufgezeigt in den einzelnen Szenarien einen geeigneten Datenschutz zu gewährleisten. Durch Anwendung der empfohlenen Verfahren ist es möglich, jeder Rolle Zugang zu von ihr benötigten Informationen zu geben ohne eine Überwachung der Nutzer oder das Erstellen eines Verhaltensprofils fürchten zu müssen.

Schlüsselworte

Privacy, Data Mining, Energiekontrollsysteme, IDEM

1. EINLEITUNG

Mit einer zunehmend energiebewussteren Lebensweise vieler Menschen gewinnen auch Energiekontrollsysteme in Gebäuden an Bedeutung. Derartige Systeme ermöglichen eine sekundengenaue Überwachung aller Stromflüsse durch Sensoren an den Verbrauchern und Leitungen. Neben Privathaushalten, die sich einen genauen Überblick über ihren Energieverbrauch verschaffen wollen, sollen derartige Systeme auch in öffentlichen Einrichtungen und Unternehmen Verwendung finden, um auch dort die Nutzer für Energieeinsparungen zu sensibilisieren und ein mögliches Einsparpotenzial aufzuzeigen. Um genaue zeitliche und lokale Informationen bereitstellen zu können, muss ein solches System mithilfe einer Vielzahl von Sensoren permanent hochauflösend Daten sammeln und zum späteren Abruf verwalten. Die so generierten Energiemessdaten können anschließend von verschiedenen Benutzergruppen in unterschiedlicher Granularität abgerufen werden; beispielsweise sollte jeder Nutzer den durch ihn verursachten Energieverbrauch mit hohem Detailgrad einsehen können, während ein Buchhalter hingegen zu Abrechnungszwecken lediglich den Gesamtverbrauch einer räumlichen Komponente über einen längeren Zeitraum benötigt. Gemäß des Datensparsamkeitprinzips „so wenig Daten wie möglich“ ist es notwendig dem Buchhalter in diesem Szenario weniger genaue Informationen bereitzustellen als dem Mitarbeiter selbst. So erhält jede Rolle Zugriff auf gerade so viele Informationen in gerade so genauer Auflösung wie sie zur Erfüllung der ihr zugedachten Aufgabe benötigt. Auf diese Weise wird ein Missbrauch der Daten beispielsweise zur Überwachung der Mitarbeiter anhand ihrer gesammelten energetischen Datensätze erschwert.

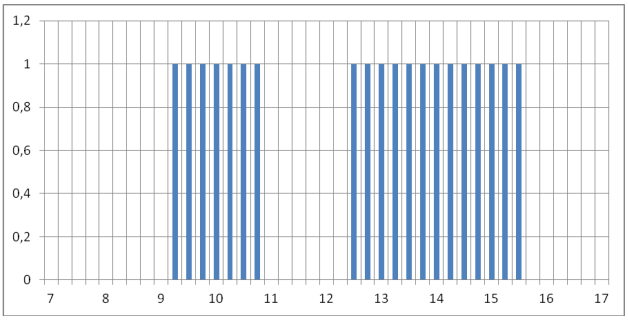

Figure 1. Beispielgraph eines Sensors

Zur Verdeutlichung dieser Gefahr nehmen wir an, der obige Verlauf (Figure 1) zeige die Messwerte eines Sensors, der den Stromverbrauch der Beleuchtung eines Ein-Mann-Büros aufzeichnet. So lässt sich aus diesen Werten folgern, der Mitarbeiter hat nicht um 9 Uhr sein Büro betreten, war nicht bis 17 Uhr im Raum und hat außerdem um die Mittagszeit seinen Arbeitsplatz für 75 Minuten verlassen. Bei Arbeitszeiten von 9 bis 17 Uhr und einer 45-minütigen Mittagspause würde dieser Datensatz vermutlich nicht zu seinen Gunsten interpretiert werden.

Entwickelt wird nun ein System, welches die gesammelten Daten sicher und sinnvoll verarbeitet und dabei die Einhaltung von Privatheits- und Datenschutzkriterien geeignet gewährleistet. Nach einem Versuch den Privatheitsbegriff intuitiv zu erfassen werden im Folgenden unterschiedliche Methoden zur Handhabung sensibler Daten, teils aus anderen Fachbereichen, vorgestellt und hinsichtlich ihrer Anwendbarkeit auf Energiekontrollsysteme in Gebäuden untersucht. Daran anschließend wird versucht diese hinsichtlich der hier gegebenen Anwendungsdomäne zu adaptieren und eigene Lösungsansätze sowie der aktuelle Forschungsstand werden präsentiert. Als besonderer Anwendungsfall wird das Wettkampfspiel EQ eingeführt, welches einen zum Energiesparen motivierenden Vergleich der Mitarbeiter bereitstellt und dabei keine Privatheitskriterien verletzt. Abschließend wird evaluiert, dass kein Ansatz alle Anwendungsfälle zufriedenstellend bedient und die Verwendung eines Methodensets die beste Option darstellt.

2. Intuitiv-naiver Privatheitsbegriff

In diesem Kapitel wird versucht den Begriff Privatheit zunächst informell zu erfassen und zu verdeutlichen welche Daten als schützenswert erachtet werden sollten. Nötig ist der Umgang mit sensiblen Informationen in unserem Alltag häufiger als man

doi: 10.2313/NET-2015-03-1_08

zunächst annehmen mag. In der Apotheke, im Reisebüro, bei der Bank, der Passkontrolle am Flughafen, beim Arzt, und an vielen weiteren Orten finden sich Abgrenzungen und Hinweisschilder, die zum Einhalten eines gewissen Abstands zur Sicherung der Privatsphäre ermahnen. Niemandem ist wohl dabei wenn ein anderer, womöglich nicht vertrauenswürdiger Mitmensch bestimmte Informationen über uns erlangt oder erlangen könnte. Meist lassen sich diese den Aggregationen Medizin und Finanzen zuordnen, sowie Informationen, welche zur Erstellung eines Verhaltensmusters oder Persönlichkeitsprofils verwendet werden könnten. Psychologisch lässt sich dies erklären durch die Angst, diese Daten könnten zu unserem Nachteil interpretiert werden. Eine bekannte Krankheit lässt einen Menschen schwach wirken, ein niedriges Gehalt weckt Schamgefühl, ein hohes Verlegenheit.

Barrieren beim Arzt oder bei Kreditinstituten erfüllen also offensichtlich direkt unser Bedürfnis, diese Daten zu schützen. Doch warum finden sie sich auch, zum Beispiel, in Apotheken? Dort wird lediglich über Medikationen gesprochen, nicht jedoch über Krankheiten und Gebrechen per se. Dennoch ist der Schutz der Daten auch hier sinnvoll. Die Argumentation bedarf dabei nur eines einzelnen, aber wesentlichen Schrittes, nämlich des Rückschlusses von einem ausgegebenen Medikament zum damit behandelten Gebrechen. Treffe ich meinen Nachbarn in der Apotheke beim Erstehen einer Hämorrhoidensalbe an, beeinflusst dies unser Verhältnis in gleichem Maße als wäre ich selbst bei der Diagnosestellung anwesend gewesen. Schützenswert sind also nicht nur Informationen, die wir geheim zu halten wünschen, sondern auch alle Daten, die direkt oder im gegenseitigen Zusammenwirken Rückschlüsse darauf erlauben. Im Umkehrschluss bedeutet dies auch, dass beim Umgang mit sensiblen Daten, zum Beispiel in einem Krankenhaus, sichergestellt werden muss, dass die betreffende Person nicht identifiziert werden kann. Um dies zu verhindern findet sich in der Medizin das Safe-Harbor-Prinzip, welches einen Katalog an sogenannten Identifiern bereitstellt, die einen Rückschluss auf eine Patientenidentität ermöglichen könnten und deshalb nicht veröffentlicht werden dürfen. Neben Namen, Telefon-, Fax- und Konto- sowie Sozialversicherungsnummern, gehören auch URLs und IP-Adressen ebenso dazu wie Photographien des Gesichts und vergleichbare Bildnisse, Fingerabdrücke oder Stimmaufzeichnungen, Autokennzeichen und Seriennummern, Seriennummern möglicher Implantate oder der Krankenhausdokumentation sowie alle temporalen Angaben über Geburt (ausgenommen das Jahr), Aufnahme, Entlassung, möglicherweise Tod. Sollte ein Patient über 89 Jahre alt sein und kein Zusammenfassen mit weiteren Personen dieser Altersgruppe möglich sein, müssen alle Hinweise auf das Alter gänzlich gestrichen werden. Zusätzlich dürfen geographische Angaben, die detaillierter als ein Staatsgebiet sind, nur in Form der ersten drei Ziffern des Postleitzahlgebietes aufgeführt werden. Sollten in einem Gebiet, welches durch diese drei Ziffern beschrieben wird, weniger als 20.000 Menschen wohnhaft sein, wird die Angabe durch 000 ersetzt. [1, 4] Während die erstgenannten Attribute intuitiv einleuchten, wirkt vor allem das letztgenannte ungemein kompliziert. Erwähnt sei an dieser Stelle, dass obiger Katalog in den USA entwickelt wurde. Studien dort zeigten, 87 Prozent aller Amerikaner können durch den Verbund aus fünftstelliger Postleitzahl, des Geschlechts und des Geburtsdatum identifiziert werden. [2] Obige Restriktion soll also einen solchen Schluss verhindern. Im Folgenden unterteilen wir Attribute analog zu [3] in drei Gruppen: Daten, die direkt auf eine Person schließen lassen, nennen wir explizite Identifier; einen Informationsverbund wie Geburtsdatum, Geschlecht und Postleitzahl, der im Zusammenspiel eine Identifikation ermöglichen könnte, bezeichnen wir als Quasiidentifier; schützenswerte Daten betiteln wir als sensibel.

Zunächst stellt sich nun die Frage, warum man nicht auch Quasiidentifier gemäß des Safe-Harbor-Prinzips verheimlicht. Die Antwort liegt in der verschwindend geringen Verwertbarkeit eines so modifizierten Datensatzes. Wir wählen als Beispiel eine klinische Studie über das Auftreten einer neuartigen Krankheit, bei der sowohl alle Identifier als auch Bestandteile des Quasiidentifiers unterdrückt werden. Zurück bleibt lediglich eine Liste von positiven und negativen Testergebnissen, aus denen sich keine räumliche Häufung, erhöhte Infektanfälligkeit einer bestimmten Altersgruppe, eines Geschlechts oder ähnliche wissenschaftlich interessante Eigenschaften manifestieren. Analog verhält es sich bei einer Psyeudonymisierung der Quasiidentifier, also dem Ersetzen der Daten durch beispielsweise Zufallszahlen oder Angaben ohne Bedeutung. Der Informationsgehalt ist identisch. Bei Fragen der nationalen Sicherheit mag dies unter Umständen eine praktikable Lösung sein, doch wenn wissenschaftlich verwertbare Informationen erhalten bleiben sollen, muss eine andere geeignete Sicherstellung der Privatheit gefunden werden. [2]

3. Gängige Praxis

Betrachten wir nun Maßnahmen, wie sie üblicherweise zum Schutz von vertraulichen Daten getroffen werden. Wir gehen dabei davon aus, dass die Originale eines Datensatzes unter Verschluss gehalten werden und lediglich Modifikationen desselben veröffentlicht werden. Um unbefugten Zugriff auf die Originale zu unterbinden, müssen nach Bundesdatenschutzgesetz [6] § 9(Anlage) folgende Maßnahmen ergriffen werden: Zunächst ist eine Zutrittskontrolle zu installieren, das heißt der Zutritt zu den Verarbeitungsanlagen muss verwehrt werden – beispielsweise durch eine verschlossene Tür. Eine Zugangskontrolle verhindert zusätzlich unbefugten Systemzugang, etwa durch eine Passwortabfrage. Eine anschließende Zugriffskontrolle gewährleistet Zugriff auf die Daten ausschließlich gemäß einer bestimmten Rolle – beispielsweise nur lesend. Des Weiteren müssen Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrollen installiert werden. Abschließend sei das unveräußerliche Recht eines Betroffenen auf Auskunft (§19,34) über erhobene Daten sowie auf Berichtigung, Sperrung und Löschung (§20,35) erwähnt. [4,6] Gesetzt den Fall der Schutz der vertraulichen Daten ist gegeben, widmen wir uns nun der Veröffentlichung potenziell sensibler Informationen.

3.1 k-Anonymität

Wie bereits erwähnt stellt das Unterdrücken oder Pseudonymisieren der Quasiidentifier aufgrund des zu hohen Informationsverlustes keine praktikable Lösung dar. Eine oftmals gebrauchte Methode eine Privatheit gemäß der in Kapitel 2 beschriebenen Kriterien zu gewährleisten besteht nun darin, lediglich Teile eines Attributs zu unterdrücken, sodass mehrere nicht unterscheidbare Tupel entstehen. Aus einer Postleitzahl 12345 wird etwa 123*; und Herr Schmidt aus 12345 ist nicht

länger von Herrn Schmidt aus 12346 und Herrn Schmidt aus 12347 unterscheidbar (Table 1).

Table 1. Beispieltabelle original (oben) und 3-anonymisiert

Name	Geschlecht	Postleitzahl
Schmidt	M	12345
Schmidt	M	12346
Schmidt	M	12347

Name	Geschlecht	Postleitzahl
Schmidt	M	1234*
Schmidt	M	1234*
Schmidt	M	1234*

Erhält man nun Kategorien mit jeweils mindestens k Tupeln, spricht man von k-Anonymität. Dies bedeutet jedes Tupel ist von mindestens k – 1 anderen nicht unterscheidbar. [2] Auf diese Weise wird die in Kapitel 2 formulierte Anforderung erfüllt, dass ein Individuum nicht eindeutig mit einem sensiblen Datum in Verbindung gebracht werden kann.

Im Weiteren verfeinern wir den durch diese Technik formalisierten Privatheitsbegriff anhand folgender Beispieltabelle, wie sie etwa in einem Krankenhausinformationssystem vorliegen könnte (Table 2).

Table 2. Krankenhaustabelle mit sensiblen Daten

	PLZ	Alter	Erkrankung
1	12344	21	Syphilis
2	12345	26	Filzläuse
3	12345	24	Chlamydien
4	12356	28	Gonorrhoe
5	12346	33	Beinfraktur
6	12348	44	Bandscheibenvorfall
7	12344	39	Krebs
8	12344	37	Krebs
9	12353	65	Herzinfarkt
10	12344	54	Herzinfarkt
11	12347	47	Herzinfarkt
12	12354	73	Herzinfarkt

Wir erreichen 4- Anonymität durch folgende Generalisierung (Table 3).

Table 3. 4-anonymisierte Krankenhaustabelle

	PLZ	Alter	Erkrankung
1	123**	<29	Syphilis
2	123**	<29	Filzläuse
3	123**	<29	Chlamydien
4	123**	<29	Gonorrhoe
5	1234*	30-45	Beinfraktur
6	1234*	40-45	Bandscheibenvorfall
7	1234*	30-45	Krebs
8	1234*	30-45	Krebs
9	123**	>=45	Herzinfarkt
10	123**	>=45	Herzinfarkt
11	123**	>=45	Herzinfarkt
12	123**	>=45	Herzinfarkt

Zweifelsfrei erfüllt diese Tabelle die Anforderung, dass kein Patient eindeutig identifiziert werden kann. Dennoch weisen solche k-anonymisierten Veröffentlichungen Schwächen auf; diese zeigen wir nun anhand eines Beispielszenarios auf. Angenommen, Anna arbeitet im Krankenhaus und hat Zugriff auf die obige anonymisierte Tabelle. Annas Mutter ist besorgt um ihren Nachbarn, der mit einem Krankenwagen in jenes Krankenhaus gebracht wurde, in dem Anna arbeitet. Ihre Mutter bittet also Anna nachzusehen, was ihrem Nachbarn fehlen könnte. Sein Alter schätzt sie auf 50 bis 60 Jahre. Obwohl Anna nicht eindeutig bestimmen kann, welches Tupel dem Nachbarn ihrer Mutter zugehörig ist, identifiziert sie dennoch einen Herzinfarkt als seine Erkrankung. Diese Schlussfolgerung beruht auf dem sogenannten Homogenitätsangriff nach [5]. Ein weiterer Angriff beruht auf vorhandenem Hintergrundwissen. Angenommen Anna sieht bei ihrer Tätigkeit im Krankenhaus einen Bekannten aus ihrem Sportverein zügig in ein Behandlungszimmer gehen. Da sie sein Alter von 37 Jahren kennt, schließt sie auf einen der Einträge 5-8. Allerdings kann sie die Einträge 5 und 6 mit dem zusätzlichen Wissen ausschließen, welches sie erlangt hat, als sie ihn selbstständig zu Fuß gehen sah. Da die Erkrankung der Einträge 7 und 8 identisch ist, schließt sie auf Krebs als Behandlungsgrund. Das Ausschließen von Einträgen aus einer Tupelkategorie kann also wieder zu einem Homogenitätsangriff führen [5]. Eine weitere Schwäche der k-Anonymität findet sich, wenn sich die Tupel sowohl in der Veröffentlichung als auch im originalen Datensatz in der gleichen Reihenfolge befinden und dem Angreifer das Sortierungsargument bekannt ist. Wurde zum Beispiel aufsteigend nach dem Alter sortiert (hier nicht der Fall), ist es wahrscheinlich, dass einem 45-jährigen Mann der erste Eintrag der Kategorie „>=45 Jahre alt“ zugehörig ist. Dieser Angriff kann durch Randomisieren unterbunden werden [2]. Eine weitere Angriffsmöglichkeit bieten mehrfache Veröffentlichungen, bei denen jeweils unterschiedliche Bestandteile des Quasiidentifiers aufgeführt werden. Man nehme zur Verdeutlichung eine Tabelle mit PLZ, Geschlecht und Krankheit sowie eine weitere mit den Einträgen Geburtsdatum und Krankheit. Ein Join der Tabellen über das gemeinsame Attribut Krankheit führt zum Quasiidentifier PLZ, Geschlecht und Geburtsdatum, der wie wir wissen ausreicht um einen Großteil aller Amerikaner zu identifizieren. Während die letzten beschriebenen Angriffe mit geringem Aufwand abgewehrt werden können, benötigt man für Hintergrundwissen-basierte und Homogenitätsangriffe eine Technik, die strenge Privatheitsanforderungen erfüllt als k-Anonymität.

3.2 l-Vielfalt

Eine Verschärfung der k-Anonymität bietet die l-Vielfalt. Wie oben dargelegt basiert ein Homogenitätsangriff auf der Tatsache, dass k-Anonymität zwar k nicht unterscheidbare Tupel bereitstellt, aber nicht gewährleistet, dass die mit ihnen verbundenen sensiblen Daten nicht identisch sind. Ziel ist es nun, dass ein Angreifer unabhängig von seinem Hintergrundwissen durch die anonymisierte Tabelle keinen Wissenszuwachs erlangen kann. Eine zu geringe Vielfalt in einem Block aus k Einträgen ermöglicht allerdings einen solchen Informationsgewinn und sollte daher vermieden werden. Deshalb wird die Schranke $l >= 2$, $l <= k$ eingeführt, welche aussagt, dass die l häufigsten Werte in jedem solchen Block ungefähr gleich häufig auftreten [5]. Auf diese Weise wird eine gewisse Heterogenität in den durch k-Anonymität generierten Blöcken erzeugt. Neben der Blockhomogenität kann wie erwähnt auch ein vorhandenes Hintergrundwissen eines Angreifers zu einem positiven Rückschluss führen. Um bei einer l-vielfältigen Tabelle einen Schluss ziehen zu können, benötigt man allerdings l-1 zusätzliche Informationen, da l-1 unzutreffende Tupel ausgeschlossen werden müssen. Auf diese Weise ist eine Parametrisierbarkeit der Metrik gegeben und die Strenge des Datenschutzes kann je nach Anwendungsfall angepasst werden. Somit stellt diese Technik eine nützliche Erweiterung der k-Anonymität dar, die den Homogenitätsangriff abwehren kann und Angriffe mit zusätzlichem Hintergrundwissen erschwert.

Problematisch ist dabei die Ungewissheit welcher Art ein potenzielles Hintergrundwissen ist [5]. Auch können bestimmte Einträge aufgrund von bekannten globalen Verteilungen, ethnischen Dispositionen etc. als wahrscheinlicher oder unwahrscheinlicher evaluiert werden [3]. Wir betrachten nochmals obiges Beispiel, als Anna ihren Sportkameraden im Krankenhaus identifizierte. Zwar waren hier bei vier zutreffenden Quasiidentifiern drei unterschiedliche Erkrankungen gelistet und damit eine ausreichende Vielfalt gegeben, dennoch konnte Anna zwei davon ausschließen und somit ein Krebsleiden folgern. Durch Anpassen der k- und l- Schranke durch den Veröffentlichenden hätte ein solcher Schluss erschwert werden können.

Neben menschlichen Faktoren offenbart folgendes Szenario eine weitere, schwerwiegendere Schwäche der l-Vielfalt. Ein weiteres Mal betrachten wir Anna, die wie gehabt Zugang zur Beispieltabelle *Table 3* hat. In einer Bar lernt Anna den Studenten Bernd kennen, den sie äußerst sympathisch findet. Im Laufe des Abends erwähnt Bernd er sei zum Zeitpunkt, der durch die Tabelle abgebildet wird, in Annas Krankenhaus Patient gewesen. Verunsichert durch diesen Umstand stellt Anna Nachforschungen an. Durch Bernds Äußeres und seinen Studentenstatus vermutet sie ein Alter unter 29 Jahren und fokussiert sich deshalb auf den ersten Block der Tabelle. Dieser ist 4-anonymisiert und aufgrund vier unterschiedlicher sensibler Einträge auch 4-vielfältig. Trotz dieser formal betrachtet exzellenten Privatheitskriterien fasst Anna bestürzt den Entschluss Bernd nicht wiedersehen zu wollen. Durchaus nachvollziehbar, offenbart doch die Tabelle trotz aller erfüllter Kriterien Bernds Infektion mit einer ansteckenden sexuell übertragbaren Erkrankung. Angesicht dieser Überkategorie ist es für Anna auch nur noch zweitrangig welche Infektionsart genau vorliegt.

Um auch auf Überkategorien basierende Schlüsse zu unterbinden, muss diese Formalisierung nochmals adaptiert und erweitert werden.

3.3 t-Nähe

Eine weitere Metrik namens t-Nähe beruht auf dem Ansatz die Verteilung eines sensiblen Datums in einem Äquivalenzblock möglichst der Verteilung dieses Datums im Gesamtvorkommen anzunähern. Bei erfüllter l-Vielfalt liegt die Wahrscheinlichkeit für eine richtige Zuordnung eines sensiblen Datums bei ca. $1/l$. Angenommen, eine Tabelle zeigt die Testergebnisse bezüglich einer negativ konnotierten Krankheit –beispielsweise AIDS. Ein Block in dieser k-anonymisierten Tabelle sollte entweder ausschließlich negative Testresultate beinhalten, da nicht krank zu sein keinen Nachteil mit sich bringt; oder gemäß oben 2-vielfältig sein, da mit positivem und negativem Testergebnis zwei Werte für das vertrauliche Attribut möglich sind. Folglich ergibt sich die Wahrscheinlichkeit $1/l$ beziehungsweise 0,5 dafür dass ein Mensch AIDS hat, dessen Eintrag in einem solchen Block vorkommt. Dies verletzt die Privatsphäre jenes Individuums, da diese Wahrscheinlichkeit sehr viel größer ist als die tatsächliche Wahrscheinlichkeit erkrankt zu sein, die in diesem Fall durch die Verteilung über alle Blöcke der Tabelle wiedergespiegelt wird. Dieses Problem versucht die t-Nähe zu bewältigen. Um dieses Ziel zu erreichen muss der Abstand zwischen zwei Attributen quantifiziert werden, was sich je nach Art der Attribute unterschiedlich gestaltet. Der kleinste zulässige Abstand einer Verteilung ist durch die Schranke t gegeben. Werden nominal skalierte Eintragungen untersucht, die keiner hierarchischen Ordnung folgen, beträgt dieser Abstand normiert 1. Alle möglichen Werte sind gleich unterschiedlich. Der Abstand ordinal skalierter Werte wie etwa numerischer Attribute, Skalen und ähnliches wird durch die Anzahl der zwischen ihnen liegenden Werte gekennzeichnet. Die Handhabung hierarchisch organisierter Nominalwerte hingegen erfordert Kenntnis dieser Hierarchie. Diese wird als Baumstruktur dargestellt; Blätter bilden die genauen Tabelleneinträge ab, Knoten mögliche Überkategorien. Alle Blätter besitzen zudem identische Tiefe n, welche den Nenner des Abstandes zweier Elemente bildet. Der Zähler stellt die Anzahl der Schritte dar, die man in der Hierarchie Richtung Wurzel unternehmen muss um einen gemeinsamen Vaterknoten beider Elemente zu finden [3]. Die oben verwendeten Krankheiten lassen sich wie folgt darstellen (Figure 2):

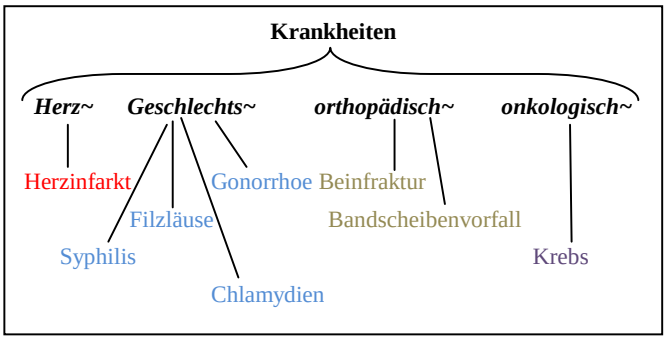

Figure 2. mögliche Hierarchie der dargestellten Krankheiten.

So beträgt der Abstand zwischen ‚Herzinfarkt' und ‚Krebs' 2, da erst in ‚Krankheiten' ein gemeinsamer Vorgänger gefunden wird. Zwischen ‚Beinfraktur' und ‚Bandscheibenvorfall' hingegen

doi: 10.2313/NET-2015-03-1_08

beträgt die Distanz 1, da beide den orthopädischen Gebrechen zuzuordnen sind.

3.4 Evaluierung der vorgestellten Methoden

Zwar lassen sich die vorgestellten Methoden zur Sicherung der Privatheit sensibler Daten leicht ineinander überführen und daher auch mit Hilfe von Adaptionen gängiger Algorithmen implementieren [5], so leidet dennoch mit zunehmender Sicherung der Daten auch deren Nutzbarkeit und wissenschaftliche Verwendbarkeit [3,5]. Begründet ist dies darin, dass bestimmte Einträge nur dann mit der gewünschten Technik aggregiert werden können wenn womöglich interessante Attribute oder Attributteile unterdrückt werden. Auch kann beobachtet werden, dass Äquivalenzblöcke einer anonymisierten Tabelle an Umfang zunehmen je mehr Kriterien zur Anwendung kommen [5]. Auch dies senkt nochmals die Verwendbarkeit einer Tabelle. Zusätzlich muss bei Verwendung der strengsten Richtlinie t-Nähe eine Hierarchie bekannt sein oder gegebenenfalls erstellt werden. Es muss nun evaluiert werden inwiefern die vorgestellten Metriken auf den eingangs erläuterten Kontext eines Energiekontrollsystems eines Gebäudes angewendet oder angepasst werden können.

4. Transfer zur Problemstellung

Während die in 3 dargestellten Techniken einen Schutz von sensiblen Absolutwerten in Tabellen bereitstellen können, sind bei einem Energiekontrollsystem zusätzlich zeitliche Verläufe schützenswert, da auch diese Dimension Aufschluss über Nutzerverhalten gibt, somit eine Möglichkeit zur Überwachung besteht und Profile abgeleitet werden können. Um dies zu unterbinden müssen die meist als Zeitreihen vorliegenden Informationen geeignet aggregiert werden. Die vorgestellten Techniken, wie sie zum Beispiel für medizinische Daten sinnvoll einsetzbar sind, können für diesen Anwendungsfall folglich nicht ohne Adaption übernommen werden, da die Daten in abweichendem Format vorliegen. Bevor in Kapitel 5 derartige Anpassungen erläutert werden, befasst sich dieser Abschnitt mit Problemen beim Transfer zur gegebenen Problemstellung und dortigen Anforderungen. Wie erwähnt existiert keine Isomorphie zwischen den tabellenbasierten Ansätzen aus Kapitel 3 und den hier relevanten zeitlichen Zusammenhängen, da von anderen Anwendungsfällen ausgegangen wird.

Als schützenswerte Eigenschaften eines Verlaufes können maximale und minimale Amplitude identifiziert werden sowie der Durchschnittswert während eines Zeitabschnittes. Gerade für Verhaltensprofile bedeutsam sind zudem markante Peaks zu bestimmten Zeitpunkten, ebenso wie erkennbare Trends und Entwicklungen. Privatsphäre-Anforderungen in diesem System beziehen sich demnach vor allem auf den Schutz dieser Daten in den gegebenen Anwendungsfällen. Ein solcher besteht beispielsweise darin, dass Nutzer die mit ihrer Person gekoppelten Daten unverfälscht und in höchster Detailstufe einsehen können. Während man auf die Energieinformationen anderer nur mit deren Einverständnis lesend zugreifen kann, ist eine zusätzliche Rolle des Energiemanagers zudem befugt diese von allen Mitarbeitern einzusehen. Buchhaltern hingegen stehen gemäß des Datensparsamkeitsprinzips nur stark aggregierte Werte und Summen zur Verfügung. Durch Public Displays, also Veröffentlichungen von Fakten in mittlerer Granularität, soll zudem eine Steigerung der Gebäudetransparenz möglich sein. Da folglich verschiedene Feinheitsgrade für verschiedene Szenarien erreicht werden müssen, muss der verwendete Privatheitsbegriff quantifizierbar und die entsprechende Technik parametrisierbar sein.

4.1 Motivationsmetrik EQ

Zur Verdeutlichung dass die Definition einer anwendungsspezifischen Metrik möglich ist, welche privatsphäreschützend ist und trotzdem einen Nutzen bietet, wird in diesem Abschnitt eine solche entwickelt.

Um bei den Nutzern des Gebäudes ein erhöhtes Bewusstsein für den individuellen Energieverbrauch zu schaffen ist ein spielerischer Wettkampf ein guter Antrieb. Dieser sollte durch einen Vergleich mit anderen einen Anreiz bereitstellen sich zu verbessern, ohne dabei sensible Daten und konkrete Werte zu offenbaren. Eine solche Privatsphäre-erhaltende Metrik namens EQ wird im Folgenden präsentiert. Inspiriert vom Konzept des Intelligenzquotienten, welcher die eigene Leistung mit dem durchschnittlich erzielten Erfolg in Relation setzt, wird auch hier ein solcher Ansatz verfolgt. Anstatt den Quotient aus dem Energieverbrauch des Nutzers und dem durchschnittlichen Energieverbrauch zu berechnen, betrachten wir hier allerdings den Kehrbruch desselben, da ein höherer Verbrauch zu einem niedrigerem Ergebnis führen sollte. Der EQ eines Nutzers berechnet sich demnach als $\frac{Mittelwert\ aller}{eigener\ Wert} \cdot 100$. Obwohl dies simpel erscheinen mag, erfüllt diese Metrik dennoch alle Anforderungen. Basierend auf seinem persönlichen Wert kann ein Teilnehmer lediglich auf den Durchschnittswert zurückschließen – in dessen Kenntnis kann er allerdings auch durch Public Displays gelangen. Außerdem beinhaltet diese Methode zwei psychologische Tricks: Zum Einen stimuliert es den menschlichen Trieb besser als der Durchschnitt sein zu wollen, zum Anderen wird durch die Multiplikation mit 100 auch ein optischer Anreiz gegeben einen dreistelligen Wert zu erreichen. Um den Zweck der Mitarbeitermotivation zu erfüllen reicht der Vergleich jenes mit dem Mittelwert aus, sich analog zum Intelligenzquotienten um eine Normalverteilung der Werte zu bemühen ist weder sinnvoll noch gerechtfertigt.

5. Adaption und neue Lösungsansätze

Dieses Kapitel beschäftigt sich mit Möglichkeiten die identifizierten Anwendungsfälle abzudecken und zeitgleich sensible Daten zu schützen. Nach einem Versuch die durch Graphen dargestellten Verläufe sinnvoll und Privatsphäre-erhaltend zu modifizieren wird der Ansatz verfolgt, diese Verläufe auf Tabellen abzubilden, sodass die Techniken k-Anonymität, l-Vielfalt und t-Nähe zur Anwendung kommen können. Anschließend werden Möglichkeiten zur tatsächlichen Aggregation von Zeitserien präsentiert sowie deren Anwendbarkeit im Kontext der Energiekontrollsysteme untersucht.

doi: 10.2313/NET-2015-03-1_08

5.1 Modifikationen des Verlaufsgraphen

Im folgenden Abschnitt wird der Graph, welcher den schützenswerten Verlauf darstellt, auf unterschiedliche Arten modifiziert. Um die nach Kapitel 4 sensiblen Informationen wie Minimum, Maximum, Peaks und deren Zeitpunkte zu schützen, existiert die Möglichkeit die Skalierung des Graphen bewusst zu manipulieren oder zu unterdrücken. Auf diese Weise sind keine Zeitpunkte von der x-Achse ablesbar, und die fehlende beziehungsweise verfälschte y-Achse verschleiert konkrete Werte.

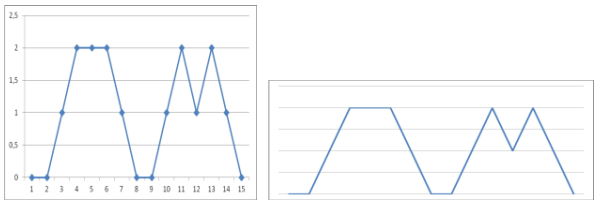

Figure 3. Graph mit Skalierung und ohne (rechts)

Obwohl sensible Daten geschützt wurden, enthält ein so modifizierter Verlauf (Figure 3) auch keine bei Auswertungen relevanten Informationen. Das Ändern der Skalierung ist reduzierbar auf den Pseudonymisierungsansatz bei Tabellen. Konkrete Werte werden durch mutmaßlich unsinnige oder falsche ersetzt und das Resultat schützt zwar die Privatsphäre der Nutzer, aber weist im Gegenzug keine wissenschaftliche Verwertbarkeit und Nutzbarkeit auf. Gerade bei Anwendungsfällen, die exakte Werte benötigen, etwa zu Abrechnungszwecken, ist von dieser Technik abzuraten. Auch bleiben Entwicklungen erkennbar.

Eine weitere Möglichkeit Interpretationen eines Verlaufsgraphen zu erschweren besteht im Flippen dieses Graphen mit einer Wahrscheinlichkeit p. Als Flippen definieren wir, dass beginnend von einem Ausgangswert zum Zeitpunkt t_0 jeder Anstieg zu einem Abstieg geändert wird. Der Betrag der Änderung bleibt dabei erhalten. Eine Zahlenfolge (1, 1, 3, 4) wird demnach in die Folge (1, 1, -1, -2) transformiert. Um eine triviale Rekonstruktion des tatsächlichen Verlaufs zu erschweren wird jeder Graph nur mit der Wahrscheinlichkeit p geflippt, mit der Wahrscheinlichkeit 1-p bleibt der ursprüngliche erhalten. Dennoch ist durch einen Hintergrundwissens-Angriff leicht herauszufinden ob es sich um eine modifizierte Ansicht handelt oder nicht. Dazu ausreichend ist bereits die Kenntnis der Art des Sensors beziehungsweise des durch ihn überwachten Verbrauchers. Der Stromverbrauch der meisten Arbeitsgeräte wird zu Beginn der Arbeitszeit vermutlich nicht nach unten gehen; diese Erkenntnis allein reicht in den meisten Fällen bereits aus um einen Graphen als geflippt oder original zu identifizieren. Auch ist diese Technik nicht für unterschiedliche Anwendungsfälle parametrisierbar.

Eine weitere Möglichkeit genaue Informationen zu verheimlichen besteht im Hinzufügen von Rauschen. Die variable Stärke des Rauschens kann dabei als Parameter der Granularität fungieren und entsprechend angepasst werden. Trotz des Rauschens können allerdings weiterhin Trends und Entwicklungen nachvollzogen werden; ist dies durch einen zu hohen Rauschanteil nicht mehr gegeben so kann auch davon ausgegangen werden, dass die Granularität zu gering ist und keinerlei Informationswert mehr enthalten ist. Auch ist Rauschen deshalb keine gute Option, da Aggregationen für Abrechnungen wie im Anwendungsfall des Buchhalters exakt sein müssen. Bedingt einsetzbar ist diese Technik allerdings in Fällen, in welchen das Zerlegen von zusammengesetzten Kurven verhindert werden soll. Kennt man charakteristische Muster einzelner Verbraucher, so ist man in der Lage aggregierte Zeitreihen durch Differenzbildung zu deaggregieren. Rauschen verhindert allerdings das saubere Entdecken von Mustern.

5.2 Abbilden auf Tabellen

Während der vorherige Abschnitt versuchte, Energieverläufe gemäß der Anwendungsfälle und Privatheitskriterien zu modifizieren, verfolgt dieses Unterkapitel Ansätze, welche die Verläufe auf Tabellen abbilden. Zielsetzung hierbei ist, im Anschluss daran die Techniken k-Anonymität, l-Vielfalt und t-Nähe verwenden zu können.

5.2.1 Pointer

In 5.1 wurde der Versuch unternommen die sensiblen Daten eines Verlaufs wie Ausschläge und genaue Zeitpunkte zu verheimlichen. Zu klären bleibt zudem die Frage, wie die Zugehörigkeit eines Verlaufs zu einem Sensor oder zu einer Person geschützt werden kann. Trivialerweise bietet sich dafür eine Tabelle bestehend aus der Identität des Nutzers und weiteren Attributen an. Diese weiteren Attribute definieren Pointer auf mit dieser Person gekoppelte Energieströme, zum Beispiel in seinem Büro, gebuchte Meetingräume, benutzte Gerätschaften etc. Diese Pointer weisen auf Dateien, in denen der Verlauf gespeichert ist.

Table 4. ID-1 identifiziert eine Person, ABC-12 einen mit dieser Person gekoppelten Verlaufsgraphen

Person	Büro	Meetingräume	Geräte
ID-1	ABC-12	DEF-34	GHI-45

Um diese Tabelle mittels z.B. l-Vielfalt zu anonymisieren, sollten statt eines expliziten Identifiers wie hier in *Table 4* Quasiidentifier aus mehrere Attributen verwendet werden, da die auf Unterdrückung von Teilen des Quasiidentifiers basierenden Techniken bei einem einzigen, eindeutigen Identifier nicht anwendbar sind. Je nach innerbetrieblicher Struktur bieten sich hierfür Büronummern, Geburtsjahre und ähnliches an.

Auf diese Weise kann eine Privatheit betreffend der Verwaltung der Kopplung von Personen und zeitlichen Entwicklungen gemäß der in Kapitel 3 erwähnten Techniken gewährleistet werden. Beachtet werden muss dabei allerdings auch, dass Angriffe mit zusätzlichem Hintergrundwissen unter Kollegen mit täglichem Umgang eine besondere Gefahr darstellen. Zu klären bleibt nun weiterhin die Frage wie die sensiblen Informationen innerhalb dieses Verlaufs geschützt werden können.

5.2.2 Charakteristika als Tabellenattribute

Nachdem wir in 5.2.1 eine Methode entwickelt haben den Zugang zu personenbezogenen Zeitserien gemäß geeigneter Kriterien zu verwalten wird nun eine Methode vorgestellt, die einen Schutz der Privatheit innerhalb dieser Daten mithilfe von Tabellen gewährleisten soll. Hierzu bedienen wir uns Eigenschaften eines Verlaufs, die diese Zeitserie zum Einen charakterisieren und zum Anderen in Tabellen abbildbar sind. Als solche erachten wir den Durchschnittswert, Gesamtsumme, sowie die Anzahl der

Zeitschritte, in denen der Wert innerhalb eines bestimmten Intervalls liegt. Auf diese Weise soll realisiert werden, bestimmten Rollen die laut Anwendungsszenario erforderlichen Daten zukommen zu lassen ohne die Möglichkeit einer zeitlichen Überwachung oder Verhaltensmustererkennung zu bieten. Durch diesen Ansatz können außerdem Trends und Entwicklungen verheimlicht werden wie später gezeigt werden wird.

Zur Veranschaulichung der Vorgehensweise betrachten wir folgenden Verlauf (Figure 4) und zwei ihn charakterisierende Tabellen (Table 5) in unterschiedlicher Granularität.

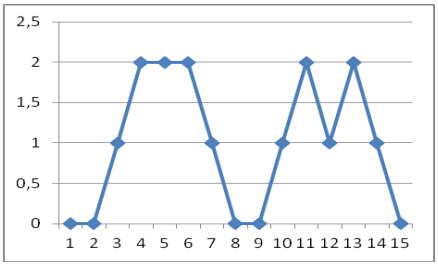

Figure 4. Beispieldaten eines Sensors

Table 5. Tabelle zu Graph aus *Figure 4*. Oben in höherer Auflösung, unten in niedrigerer

Durchschnitt	Summe	[0 ; 0,5[	[0,5 ; 1,5]	]1,5 ; 2,5]
1	15	5	5	5

Durchschnitt	Summe	<1	>= 1
1	15	5	10

Wie dieses Beispiel belegt, können durch Wahl unterschiedlicher Intervalle verschiedene Feinheitsgerade erreicht werden. Je nach Anwendungsfall ist die Darstellung also adaptierbar. Die sensiblen Daten Minimum und Maximum werden nicht offenbart; bei Wahl von geschlossenen Intervallen können diese lediglich einem Bereich zugeordnet werden, nicht aber exakt identifiziert werden. Bei Darstellung mit offenen Intervallen sind diese Eigenschaften sogar noch stärker verheimlicht. Auch werden schützenswerte Informationen über markante Ausschläge nicht preisgegeben. Gerade bei Profiling- und Überwachungsangriffen sind deren Zeitpunkte besonders interessant, doch diese Daten lassen sich aus obiger Darstellung weder ablesen noch berechnen. Außerdem wurden in Kapitel 4 erkennbare Trends als Gefahrenpotenzial identifiziert. Das folgende Beispiel belegt jedoch, dass auch Entwicklungen des Verlaufs mit dieser Technik nicht erkannt werden können. Sowohl *Figure 4* als auch die drei nachstehenden Graphen (Figure 5) werden auf die in *Table 5* zu findenden Tabellen abgebildet, wobei sie jedoch unterschiedlichste Trends darstellen.

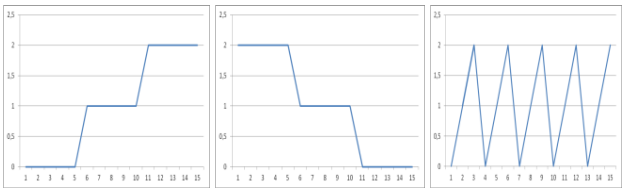

Figure 5. links ein monoton steigender Graph, mittig ein monoton fallender sowie rechts ein periodizierender Graph

Neben den nun erfüllten Anforderungen bezüglich der Verheimlichung von Entwicklungen sowie der Parametrisierbarkeit zur Bereitstellung unterschiedlicher Granularitäten ist es durch die Angabe von Durchschnittswerten auch für Public Displays geeignet. Ebenso können Buchhalter zu Abrechnungszwecken die angezeigte Gesamtsumme verwenden ohne Einblick in den tatsächlichen Verlauf der Zeitserie zu erhalten. Spezielle Methoden zur Berechnung dieser Summe werden in Abschnitt 5.3 vorgestellt. Doch nun kommen wir nochmals auf die in Kapitel 3 erläuterten Techniken zum Schutz sensibler Daten in Tabellen zurück und verbinden dieses Wissen mit der entwickelten Methode, Zeitserien auf Tabellen abzubilden. Hierzu wählen wir als Quasiidentifier den Verbund aus Raumnummer und Geburtsdatum, sensible Daten sind alle Charakteristika unserer Sensordaten analog zu obigem Beispiel. Eine so entstandene Beispieltabelle kann wie folgt aussehen (Table 6):

Table 6. Kombinierte Tabelle

Quasiidentifier		Sensible Daten				
Raum	*Geburt*	*Schnitt*	*Summe*	*<1*	*[1 ; 2]*	*>2*
05.5.23	1990	2,1	25	2	8	5
05.5.23	1964	1,9	23	6	4	5
05.5.12	1988	1,4	18	5	9	1

Auf diese Tabelle können nun die Techniken k-Anonymität, l-Vielfalt und t-Nähe fast ohne Adaption angewendet werden. Einem Buchhalter können 2-anonyme räumliche Aggregationen mit den Spalten Raum und Summe präsentiert werden, für Public Displays bieten sich l-vielfältige Durchschnittswerte an um einen Homogenitätsangriff abzuwehren. Die sehr gute Parametrisierbarkeit ergibt sich aus der Wahl der Intervalle und Intervallgrenzen, sowie der Entscheidung welche Spalten der sensiblen Daten veröffentlicht werden und der abschließenden Anwendung von k-Anonymisierung und artverwandten Techniken. Mit dieser Methode ist demnach eine Möglichkeit zur Privatsphäreerhaltung gefunden worden, die alle Privatheitskriterien wie oben erarbeitet erfüllt. Ein Nachteil allerdings liegt in der nötigen Diskretisierung kontinuierlicher Sensordaten um die Anzahl der Zeiteinheiten zu bestimmen, während jener der Messwert in einem bestimmten Intervall der Bildmenge lag.

5.3 Tatsächliche Aggregation

Dieser Abschnitt widmet sich dem aktuellen Forschungsthema, wie Summen von Privatsphäre-Restriktionen unterliegenden

doi: 10.2313/NET-2015-03-1_08

Summanden errechnet werden können. Interessant ist dies im Kontext der Energiekontrollsysteme besonders für den Anwendungsfall des Buchhalters. Neben diesem Aspekt wird zudem die Anpassbarkeit der Techniken relevant für ihre Anwendbarkeit sein. Hierzu untersuchen wir zunächst den in [9] verfolgten Ansatz. Dieser ist an das Verschlüsselungsverfahren nach Diffie-Hellman angelehnt.

In einem ersten Schritt wird ein zufälliger Generator g aus der zyklischen Gruppe G ausgewählt sowie n+1 geheime Zahlen s_i, sodass die Summe aller s_i null ist. Beginnend bei i=1 wird jedes s_i dem Teilnehmer i zugewiesen, welcher es als Secret Key verwendet. Der zu schützende Wert wird als x definiert, beziehungsweise x‘, falls ein Rauschen hinzugefügt wurde. Im Anschluss daran berechnet jeder Teilnehmer zum Zeitschritt t den Ciphertext c nach der Formel

$$c \leftarrow g^{x'} \cdot H(t)^{s_i}$$

wobei H(t) eine Hashfunktion auf G darstellt. Die verschlüsselten Werte werden nun dem Server übertragen, dieser berechnet

$$V \leftarrow H(t)^{s_0} \cdot \prod_{i=1}^{n} c_i$$

Mit $\prod_{i=1}^{n} (H(t)^{s_i}) = 1$ ergibt sich die Äquivalenz

$$V = g^{\sum_{i=1}^{n} x_i}$$

Nun kann der Server, dem g bekannt ist, die Summe aller ursprünglichen Werte mithilfe des diskreten Logarithmus berechnen. Die Erhaltung der Privatsphäre in diesem Verfahren wird analog zum Diffie-Hellman Algorithmus durch die Wahl einer geeigneten Gruppe G basierend auf einer genügend großen Primzahl p begründet. Mithilfe weniger Modifikationen kann diese Methode so adaptiert werden, dass statt Summen auch Produkte sensibler Informationen aggregiert werden können.[9] Durch die Verschlüsselung können weder der Server noch ein potenzieller Man in the Middle die sensiblen Summanden auslesen. Nach Durchlauf des Protokolls steht dem Server lediglich die aggregierte Summe zur Verfügung. Obwohl das Verfahren also Angriffe gegen den Datenschutz zu unterbinden vermag, wird dennoch zum Austausch der Schlüssel eine vertrauenswürdige Verbindung benötigt.

Ein weiterer Ansatz mit ähnlichem Ziel wird in [8] verfolgt. Auch hier wird mit einer Initiationsphase und der Wahl eines Generators g begonnen. Zunächst wird ein privater Schlüssel λ festgelegt, und jedem User u wird ein λ_u zugewiesen, sodass λ die Summe aller λ_u darstellt. Anschließend addiert jeder Nutzer zu seinem geschützten Wert x_u eine nur ihm bekannte Zufallszahl r_u und verschlüsselt das Resultat, da Rauschen alleine keinen genügenden Schutz darstellt. Verwendet wird dazu das Paillier-Kryptosystem. Der zentrale Server berechnet nun das Produkt aller übertragenen Werte, welches in der verschlüsselten Darstellung der Summe aller (x_u + r_u) besteht. Nach dem Distributivgesetz gilt $c = \sum_{u=1}^{|User|}(x_u + r_u) = \sum_{u=1}^{|User|} x_u + \sum_{u=1}^{|User|} r_u$.

Nachdem der Server aber die r_u nicht kennt, sendet er c an alle Teilnehmer zurück. Diese berechnen nun Antworten basierend auf ihrem persönlichen Schlüssel und ihrer Zufallszahl r und schicken diese Antwort c’$_u$ an den Server zurück. Dabei gilt $c'_u = c^{\lambda_u} \cdot g^{-r_u \cdot \lambda}$. Das Produkt dieser c’$_u$ berechnet der Server um anschließend die endgültige Entschlüsselung der gesuchten Summe wie folgt als $\frac{L(c' \bmod m^2)}{L(g^{\lambda} \bmod m^2)}$ zu berechnen. Dabei bezeichnet m eine Primzahl, so dass alle verschlüsselten Nachrichten aus {0,1,…,m-1} stammen. Auch wird definiert $L(z) = \frac{z-1}{m}$.

Wir fassen diese Schritte wie folgt zusammen: Um die Summe aller x_u zu berechnen fügt jeder Nutzer seinem Wert ein Rauschen r_u hinzu. Da das Rauschen alleine keinen genügenden Schutz gewährleistet, verschlüsselt jeder Nutzer die Summe aus seinem Wert und Rauschen. Aufgrund der Verschlüsselung kann der Server lediglich die Verschlüsselung der Summe aller übertragenen (x_u + r_u) berechnen. Dieser verschlüsselte Wert wird anschließend zu den Klienten zurückgesandt, welche diesen dazu benutzen basierend auf ihrem Secret Key Informationen zur Entschlüsselung der Gesamtsumme bereitstellen.

Für einen formalen Beweis dieser Methode sei auf [8] und [10] verwiesen. Der Vorteil dieser Variante liegt in der verteilten Entschlüsselung der Daten, so kann ein Angreifer selbst dann keine Informationen gewinnen, wenn es ihm gelingen sollte einen der Teilnehmer zu infiltrieren. Andererseits liegt in der dezentralen Abwicklung auch eine große Schwäche der Variante, da so ein falscher, fehlender oder zu langsam übertragener Wert zu einem Misserfolg führen kann. In der Konsequenz wird also ein permanenter Online-Status aller Nutzer erwartet.

6. Bewertung hinsichtlich Anwendungsfälle

Um eine Empfehlung hinsichtlich einer Entscheidung für eine der erläuterten Datenschutztechniken abgeben zu können, befasst sich dieser Abschnitt nochmals mit den Vor- und Nachteilen jener und evaluiert sie bezüglich der gegebenen Anwendungsfälle. Diese bestanden zum Einen in der Anforderung, dass Nutzer die von ihnen verursachten Energiedaten in höchster Auflösung einsehen können, die anderer Teilnehmer allerdings nur mit deren Einverständnis. Die Daten in feinster Auflösung müssen folglich unverfälscht zur Verfügung stehen. Zum Anderen sollen Public Displays in mittlerer Granularität zudem die Energietransparenz eines Gebäudes erhöhen, auch sind räumliche Aggregationen zu Abrechnungszwecken sinnvoll. Da folglich verschiedene Feinheitsgrade der Daten zur Verfügung gestellt werden müssen, ist außerdem die Parametrisierbarkeit einer Technik ein wichtiger Punkt. Eine solche Anpassbarkeit stellen zwar k-Anonymität, l-Vielfalt und t-Nähe bereit, haben allerdings den Nachteil des sinkenden Informationswerts der Daten bei steigendem Datenschutz. Außerdem basieren diese Methoden auf der Tatsache, dass Daten in Tabellenform vorliegen, was hier nicht der Fall ist. Nachdem die Daten des Energiekontrollsystems allerdings durch die in 5.2.2 beschriebene Methode in diese Darstellungsweise überführt wurden, sind jene Verfahren

durchaus anwendbar. Der Einsatz dieser Kombination wird für die meisten Anwendungsfälle empfohlen. Für das Szenario eines Buchhalters, der lediglich summierte Verbräuche in bestimmten Gebäudeteilen benötigt, legen wir dem Anwender nahe, eines der Verfahren aus 5.3 zu verwenden. Diese garantieren eine Summierung der Werte ohne Einblick in die Einzelverbräuche zu gewähren. Der Einblick eines Nutzers in seine eigenen Energiedaten und der Zugang des Energiemanagers zu diesen können in einer Tabellenform angelehnt an 5.2.1 verwaltet werden, bei der Links auf feingranulare Daten zur Verfügung gestellt werden.

7. ZUSAMMENFASSUNG

Mit dem derzeit steigendem Energiebewusstsein vieler Menschen erhielten auch Energiekontrollsysteme Einzug in Privathäuser ebenso wie in gewerbliche oder behördliche Gebäude. Diese Systeme sammeln kontinuierlich Energieverbrauchsdaten durch eine Vielzahl an Sensoren. Dabei soll es jedem Nutzer möglich sein, von ihm verursachte Energiedaten in höchster Auflösung einsehen zu können, die anderer Teilnehmer allerdings nur mit deren Einverständnis. Bestimmte Rollen wie zum Beispiel ein Buchhalter sollen zudem aggregierte Informationen zu Abrechnungszwecken erhalten können, ebenso sollen Public Displays bereitgestellt werden können. Es soll außerdem nicht möglich sein, mithilfe der freigegebenen Daten Teilnehmer des Energiekontrollsystems zu überwachen oder ein Verhaltensmuster jener zu erkennen, weshalb markante Stellen im Verlaufsgraphen und deren zeitlicher Zusammenhang nicht offenliegen dürfen. Etablierte Methoden zum Schutz sensibler Daten, beispielsweise aus dem Bereich der medizinischen Statistik, stützen sich auf eine Abbildung der Informationen in Tabellen. Hierbei bezeichnet man einen Verbund nicht sensibler Daten, die ein Individuum identifizieren können, als Quasiidentifier. Ein verbreiteter Ansatz ist nun eine Unentscheidbarkeit bei der Zuordnung eines solchen Quasiidentifiers zu einem geschützten Datum zu erreichen. Eine solche Methode namens k-Anonymität stellt eine Tabelle bereit, bei der jeder Quasiidentifier von mindestens k-1 anderen Zeilen nicht zu unterscheiden ist. Dennoch ist in manchen Fällen eine Zuordnung einer Person zu einem sensiblen Eintrag möglich, falls entweder zusätzliches Hintergrundwissen vorliegt oder die sensiblen Daten innerhalb der k nicht unterscheidbaren Einträgen identisch sind. Um dies zu verhindern wird die Technik l-Vielfalt dargestellt, die zusätzlich eine Heterogenität innerhalb der durch k-Anonymisierung entstandenen Äquivalenzblöcke gewährleistet. Allerdings sagt l-Vielfalt lediglich etwas über die Unterschiedlichkeit der sensiblen Daten aus, nicht jedoch über deren Ähnlichkeit. So ist ein Angriff auf die Privatsphäre dennoch möglich, falls zwar eine große Vielfalt an Werten herrscht, aber diese alle einer gewissen Überkategorie zuzurechnen sind. Somit kann leicht auf diese Überkategorie geschlossen werden, welche allerdings ebenfalls als schützenswert erachtet wird. Um dies zu verhindern fordert die Technik t–Nähe die Unterschreitung einer gewissen Distanz zwischen der Verteilung der sensiblen Werte innerhalb nicht unterscheidbarer Quasiidentifier und ihrer Verteilung über die Gesamtheit aller Einträge.

Obwohl durch diese Schritte der Schutz der Privatsphäre zwar stark zunimmt, schwindet jedoch durch verstärkte Restriktionen und vermehrte Unterdrückung von Teilen des Quasiidentifiers der Nutzen und wissenschaftlicher Informationswert des Outputs. Auch sind diese Techniken lediglich auf Tabellen anwendbar. In einem Energiekontrollsystem sind hingegen vor allem Energieverläufe interessant, weshalb im Anschluss zuerst eine Technik vorgestellt wird solche Verläufe in Tabellen zu verlinken, bevor eine Methode entwickelt wird diese Verläufe auf Tabellen anhand ihrer Charakteristika abzubilden. Sinnvoll ist dies deshalb, da hierdurch wiederum die etablierten Methoden k-Anonymität und artverwandte Techniken angewandt werden können. Um Privatsphäre-erhaltend Summen zu generieren werden zwei Methoden vorgestellt, welche dies ohne Kenntnis der tatsächlichen Summanden ermöglichen. Ein Einsatz dieser Verfahren wird im Anwendungsfall eines Buchhalter als sinnvoll erachtet, da ihm somit lediglich Aggregationen zu Abrechnungszwecken zur Verfügung stehen und keine Einzeldaten bekannt werden. Für den Anwendungsfall des Energiemanagers ebenso wie für die Einsicht der Nutzer in die eigenen Daten wird ein Zugang zu einer Tabelle gemäß der in 5.2.1 dargestellten Technik empfohlen, bei der Links auf feingranulare Daten zur Verfügung gestellt werden. Für weitere Anwendungsszenarien wird die Verwendung einer Charakteristika-basierten Tabellendarstellung der Verläufe analog zu 5.2.2 nahegelegt, welche anschließend mithilfe der Verfahren zum Schutz von Tabellendaten aggregiert werden kann. Mit dem Spiel EQ wird zudem ein spielerischer Wettkampf präsentiert, welcher den Nutzern eine Einordung des eigenen Energieverbrauchs bereitstellt ohne sensible Daten anderer offenzulegen.

8. REFERENZEN

[1] U.S. Department of Health and Human Services, “De-identifying protected health information under the privacy rule”, 2007. *URL: http://privacyruleandresearch.nih.gov/pr_08.asp#8a, zul. aufgerufen am 28.08.2014*

[2] Sweeney, Latanya. "k-anonymity: A model for protecting privacy." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10.05 (2002): 557-570.

[3] Li, Ninghui, Tiancheng Li, and Suresh Venkatasubramanian. "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity." *ICDE*. Vol. 7. 2007.

[4] Klaus Kuhn, „Datenschutz in der Medizin“, *Vorlesungsunterlagen zur Veranstaltung Medizin II (Krankheitslehre, klinische Propädeutik, Einführung in die Medizinische Informatik)*, IMSE-TUM, 2014 URL:https://www.moodle.tum.de/pluginfile.php/389365/mod_resource/content/1/med2_ss14_v10a.pdf

[5] Machanavajjhala, Ashwin, et al. "l-diversity: Privacy beyond k-anonymity." *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1.1 (2007): 3.

[6] Bundesdatenschutzgesetz, Bundesministerium der Justiz und für den Verbraucherschutz. *URL: http://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html*

[7] Zhu, Ye, Yongjian Fu, and Huirong Fu. "On privacy in time series data mining."*Advances in Knowledge Discovery and Data Mining*. Springer Berlin Heidelberg, 2008. 479-493.

[8] Rastogi, Vibhor, and Suman Nath. "Differentially private aggregation of distributed time-series with transformation and encryption." *Proceedings of the 2010 ACM SIGMOD*

International Conference on Management of data. ACM, 2010.

[9] Shi, Elaine, et al. "Privacy-Preserving Aggregation of Time-Series Data." *NDSS*. Vol. 2. No. 3. 2011.

[10] Rastogi, Vibor., and Nath, Suman. “Differentially private aggregation of distributed time-series with transformation and encryption”. *Tech.Rep. MSR-TR-2009-186*, Microsoft Research, 2009. Extended version of [8]