Wuala

Seminar Future Internet SS2009

Florian Wohlfart
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München
Email: wohlfart@in.tum.de

***Zusammenfassung*— Wuala ist ein Cloud-Storage-Dienst, der auf einem Peer-to-Peer-Netzwerk als verteiltem Speicher basiert. Die Wuala-Entwickler haben es geschafft die aufwendige Technik ihres Peer-to-Peer-Netzwerks hinter einer einfach zu benutzenden Oberfläche zu verstecken, die wie ein Dateimanager aufgebaut ist. Die Benutzeroberfläche ist jedoch gerade für Vielnutzer zu wenig anpassbar und lässt sich nicht so schnell wie ein gewöhnlicher Dateimanager bedienen. Wuala wirbt damit dass die privaten Dateien in Wuala so sicher seien, dass sie angeblich nicht mal von Wuala selbst entschlüsselt werden könnten. In der Tat ist Wuala relativ sicher, solange man eigene Dateien hochlädt, die sonst niemand besitzt und ein sicheres Passwort wählt. Im Vergleich mit anderen Cloud-Storage-Diensten ist das Konzept von Wuala durchaus konkurrenzfähig und hebt sich durch einzigartige Features von der Masse ab.**

***Schlüsselworte*— Wuala, Peer-to-Peer, Cloud-Storage, Online-Backup, File-Sharing, Soziales Netzwerk**

I. Einleitung

A. Einführung in Wuala

Cloud-Storage-Dienste [1] sind eine relativ neue Entwicklung des Internets, welche es dem Benutzer ermöglichen seine Daten ständig zur Verfügung zu haben, sofern ein Internetzugang vorhanden ist. Wuala bietet hierbei den neuen, ungewöhnlichen Ansatz die Daten in einem Peer-to-Peer-Netzwerk zu speichern. Die Idee ist, dass Anwender auf ihrem Rechner Speicherplatz freigeben, auf dem Wuala Dateien von anderen Nutzern speichern darf. Im Gegenzug dazu bekommt der Nutzer Online-Speicherplatz im Wuala-Netzwerk. Man kann also lokalen Speicherplatz gegen Online-Speicherplatz eintauschen und so die Qualität seines Speichers verändern.
Dateien können in Wuala geheim gehalten werden, mit Freunden geteilt oder öffentlich zugänglich gemacht werden. Um das Geheimhalten von Daten im Peer-to-Peer-Netzwerk zu ermöglichen, werden die Daten verschlüsselt. Zur Verwaltung von privaten und öffentlichen Daten wurde eigens ein System zur Schlüsselverwaltung entwickelt. Auch wurde die Wuala-Software speziell auf den Umgang mit großen Multimedia-Dateien ausgerichtet.
Die Wuala-Software bekommt außerdem durch Features wie dem Bilden von Freundschaften unter Benutzern, erstellen von Gruppen, teilen von Dokumenten mit Freunden und dem Kommentieren von Dateien einen Community-Charakter. Darurch umfasst Wuala mehr als nur einen Online-Speicherplatz, es ausserdem ist ein soziales Netzwerk und kann als Ersatz für One-Click-Hoster dienen.
Das Konzept von Wuala baut darauf auf, dass viele Nutzer nur einen kleinen Teil ihrer zur Verfügung stehenden Ressourcen wie Speicherplatz und Bandbreite nutzen. Da die meisten Nutzer inzwischen eine Internet-Flatrate besitzen, verursacht Wuala bei ihnen keine zusätzlichen Kosten, bietet aber einen Mehrwert in Form von stets zugreifbarem Internet-Speicher.

B. Überblick

In dieser Arbeit soll nun zuerst die Funktionsweise von Wuala näher betrachtet werden, um die späteren Ausführungen zu verstehen. Hierbei werden einige effiziente und elegante Lösungen erklärt, wie etwa der Einsatz von Erasure Codes zur redundanten Speicherung der Dateien und das neu entwickelte System zum Schlüsselmanagement. Als nächstes wird die Benutzerfreundlichkeit der Benutzeroberfläche untersucht, wobei der Fokus auf effizientem Arbeiten und der multimediatauglichkeit von Wuala liegen. Darauf folgt der Kern dieser Arbeit, die Sicherheit von Wuala. Dazu wird untersucht in wieweit Wuala die IT-Schutzziele erfüllt. Im Anschluss folgt ein Vergleich mit ähnlichen Produken, sowie ein Fazit über die Software.

II. Funktionsweise

Da Wuala eine Reihe neuer, interessanter Ideen und Algorithmen beinhaltet wird hier auf die Technik und Funktionsweise von Wuala eingegangen, um die Software besser zu verstehen.

A. Redundante Speicherung

Da in einem Peer-to-Peer-Netzwerk nicht ständig alle Clients online sind, wird jede Datei in Wuala mehrfach redundant gespeichert, um eine hohe Verfügbarkeit garantieren zu können. Um diese Redundanz zu erzeugen gibt es zwei Möglichkeiten: die Vervielfältigung der Datei und die Vervielfältigung von Dateifragmenten durch Erasure Codes [2]. Da die Verfügbarkeit einer Datei beim Einsatz von Erasure Codes im Vergleich zur simplen Vervielfältigung der Datei um Größenordnungen höher ist [3], kommen in Wuala Erasure Codes zum Einsatz, die auf Basis von Dateifragmenten arbeiten.

1) Erasure Codes: Angenommen eine Datei besteht aus n Fragmenten. Dann werden mit einem Erasure Code aus den n Fragmenten weitere m redundante Fragmente errechnet. Nun kann aus einer Untermenge der insgesamt $n + m$ Fragmente

wieder die vollständige Datei wiederherstellt werden, auch wenn ein paar der Fragmente fehlen. Wuala verwendet als Erasure Code den Reed-Solomon Code [4], welcher in der Lage ist aus beliebigen n der insgesamt $n+m$ Fragmente die vollständige Datei zu rekonstruieren. Eine Datei wird immer in $n = 100$ Fragmente aufgeteilt [5], die Größe eines Fragments hängt also von der Dateigröße ab. Die Anzahl der redundanten Fragmente wird durch den Redundanz-Faktor festgelegt, der unter anderem von der durchschnittlichen Online-Zeit der Rechner, auf denen die Fragmente gespeichert werden, und der Beliebtheit der Datei abhängt. Der Redundanz-Faktor beträgt in typischen Fällen 4, das heisst es werden ungefähr $m = 400$ redundante Fragmente gebildet. Somit werden insgesant ungefähr $n + m = 500$ Fragmente einer Datei im Netzwerk gespeichet. [3].

2) Hochladen von Dateien: Beim Hochladen einer Datei ins Wuala-Netzwerk geschieht also folgendes: Zuerst wird die Datei verschlüsselt. Dann wird sie in n Fragmente aufgeteilt und es werden m redundante Fragmente hinzugefügt. Schliesslich werden alle $n+m$ Fragmente ins Wuala-Netzwerk geladen, wobei ein Rechner nur höchstens ein Fragment einer Datei speichert, um die Datei gut zu verteilen. Zusätzlich werden die ersten n Fragmente der Datei auf den Wuala-Server geladen, welcher die ständige Verfügbarkeit der Datei sicherstellen soll und als Backup-Server dient.

3) Herunterladen von Dateien: Soll eine Datei aus dem Wuala-Netzwerk heruntergeladen werden, so versucht der Wuala-Client n beliebige Fragmente der Datei gleichzeitig aus dem Wuala-Netzwerk zu laden. Fehlen noch Fragmente, da sie momentan im Netzwerk nicht verfügbar sind, werden diese vom Wuala-Server geladen. Durch die vielen parallelen Downloads bringt diese Variante einen spürbaren Geschwindigkeitsvorteil gegenüber einem normalen Download vom Server. Nach dem Download wird die Datei aus den Fragmenten wiederhergestellt und entschlüsselt. Jetzt kann die Datei gelesen werden.

4) Wartung von Dateien: Verlässt ein Rechner das Wuala-Netzwerk dauerhaft, so gehen alle auf ihm gespeicherten Fragmente verloren. Deshalb überprüft der Wuala-Client regelmässig, ob noch genug Fragmente jeder Datei im Netzwerk vorhanden sind. Fehlt ein Fragment dauerhaft, so wird es automatisch neu berechnet und hochgeladen. Dies wird Wartung der Datei genannt.

B. Schlüsselmanagement

Da kein vorhandenes System zur Schlüsselverwaltung und Zugangskontrolle den Anforderungen der Wuala-Entwickler entsprach, entwickelten sie eine eigene Datenstruktur zum Schlüsselmanagement namens ”Cryptree” [6]. Laut den Wuala-Entwicklern ist Cryptree die erste kryptografische Datenstruktur, welche die neuesten Forschungsergebnisse im Bereich der kryptografischen Schlüsselhierarchien mit denen der Zugangskontrolle in Dateisystemen verbindet.

1) Kryptografische Links: Um den Aufbau des Cryptrees zu verstehen muss man wissen, was kryptografische Links sind. Kryptografische Links stellen einen Zusammenhang zwischen

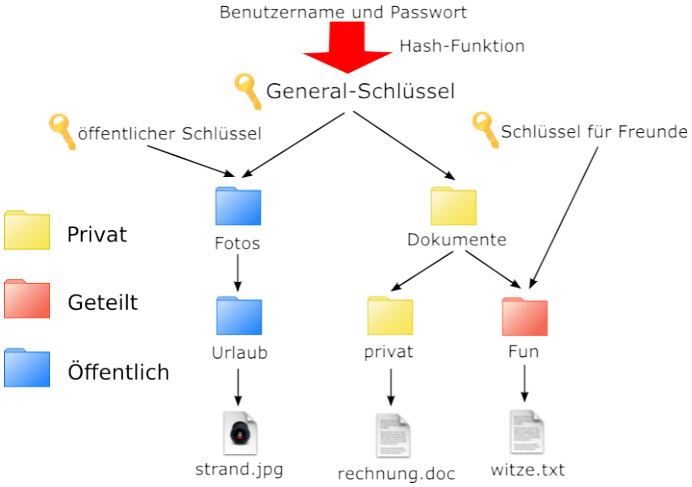

Abbildung 1. Beispielstruktur eines Cryptrees zum Lesezugriff. Jeder Ordner und jede Datei besitzt einen eigenen Schlüssel. Die Pfeile stehen für gerichtete kryptografische Links. In Richtung der Pfeile kann die Ordnersruktur entschlüsselt werden.

zwei verschiedenen Schlüsseln K_1 und K_2 her, der es erlaubt von K_1 auf K_2 zu schliessen, jedoch nicht von K_2 auf K_1. Man schreibt $K_1 \rightarrow K_2$. Dieser Link lässt sich einfach erzeugen indem man K_2 mit K_1 verschlüsselt, wobei man ein symmetrisches oder asymmetrisches Verschlüsselungsverfahren verwenden kann. Nun kann jeder Besitzer von K_1 diesen Link entschlüsseln und so K_2 erhalten. Verwendet man ein asymmetrisches Schlüsselpaar um den Link zu erstellen, so benutzt man den öffentlichen Schlüssel und den geheimen Schlüssel um den Link zu entschlüsseln. Das hat den Vorteil, dass bei einer Änderung von K_2 nur der öffentliche Teil von K_1 bekannt sein muss, um den Link neu zu erstellen. Asymmetrisch verschlüsselte Kryptografische Links werden jedoch Aufgrund der Länge eines asymmetrischen Schlüssels nur an wenigen Stellen benutzt.

2) Cryptree: Der Cryptree besteht aus zwei baumähnlichen Verkettungen aus kryptografischen Links, die eine Ordnerstruktur nachbilden. Ein Baum regelt den Lese- und der andere den Schreibzugriff. Jeder Ordner und jede Datei besitzen ihren eigenen Schlüssel. Diese Schlüssel werden wie in Abbildung 1 gezeigt durch Kryptografische Links verbunden. Die Anordnung der gerichteten kryptografischen Links macht es möglich, jeweils die darunterliegenden Schlüssel zu entschlüsseln, jedoch nicht die darüberliegenden. Es existieren zwar sogenannte Backlinks zum jeweils darüberliegenden Ordner, mit diesen ist es jedoch nur möglich den Namen des Ordners zu entschlüsseln, um den aktuellen Pfad herauszufinden. Damit der Nutzer auf seine eigenen Daten zugreifen kann benötigt er den Generalschlüssel, der die Wurzel der Baumstruktur bildet. Da Wuala aus Sicherheitsgründen diesen Generalschlüssel nicht speichert, wird dieser durch eine Hashfunktion aus dem Benutzernamen und dem Passwort des Benutzers gebildet. Somit kann Wuala nur mit dem richtigen Passwort den Generalschlüssel berechnen. Will man einen Ordner mit Freunden teilen oder veröffentlichen, so generiert Wuala einen neuen

Schlüssel und einen Kryptografischen Link von diesem auf den Schlüssel des Ordners. Diesen neuen Schlüssel schickt man nun seinen Freunden bzw. veröffentlicht ihn. Als Konsequenz davon ist es nicht möglich eine Datei als öffentlich oder privat zu deklarieren, sondern nur ganze Ordner. Weiterhin ist des nicht möglich innerhalb eines öffentlichen Ordners private oder nur mit Freunden geteilte Unterordner zu erstellen. Diese intuitive Handhabung vereinfacht jedoch die Verwaltung der Zugriffsregeln und verhindert eine Zersplitterung von zugreifbaren Dateien.

C. Routing

Anfragen werden im Wuala-Netzwerk mit Hilfe einer verteilten Hash-Tabelle geroutet, das heisst das Routing ist dezentralisiert und gut skalierbar. Wuala benutzt ein eigenes Routingverfahren, welches auf Kademlia [7] aufbaut und somit den Zielhost innerhalb von $O(logn)$ Hops findet. Es gibt im Wuala-Netzwerk drei Klassen von Hosts [3]. Hat man keinen Speicher auf seinem Rechner freigegeben, so ist dieser ein ”client node”, das heisst seine Funktion im Wuala-Netzwerk ist ausschliesslich der Datenkonsum. Hat man auf seinem Rechner Speicher freigegeben, so gilt dieser als ”storage node”. Storage nodes speichern Dateifragmente, die von anderen Nutzern abgerufen werden können. Hinzu kommt eine geringere Anzahl an ”super nodes”, die für das Routing verantwortlich sind. Jedem storage- und client node ist ein solcher super node zugewiesen, der dessen Pakete über das Wuala-Netzwerk routet. Super nodes besitzen eine Routing-Tabelle mit den Adressen von anderen super- und storage nodes, um Anfragen weiterleiten zu können. In der Routing-Tabelle befinden sich die benachbarten super nodes ebenso wie zufällige andere super nodes und die dem super node zugewiesenen client und storage nodes. Die Kombination von benachbarten und zufälligen Einträgen in der Routing-Tabelle hat sich in Tests als besonders effizient erwiesen [3].

D. Fairness

Ebenfalls eine Eigenentwicklung des Wuala-Teams ist ”Havelaar” [8], ein robustes System zur Bewertung des Nutzerverhaltens in Peer-to-Peer-Netzwerken. Verbraucht ein Benutzer sehr viele Ressourcen, trägt aber selbst nichts zum Netzwerk bei, so soll mit dem System seine seine verfügbare Bandbreite herabgesetzt werden. Man will jedoch die Bandbreite bei solchen Benutzern nicht künstlich begrenzen, sondern gibt stattdessen anderen Benutzern den Vortritt, wenn mehrere Benutzer gleichzeitig beim gleichen storage node nach einem Dateifragment fragen. Dieses Bewertungssystem soll also keine Nutzer bestrafen, sondern nur eine Belastung des Wuala-Netzwerkes durch Benutzer, die sehr viel Bandbreite beanspruchen, verhindern.

ver

III. Benutzerfreundlichkeit

Nach der Einführung in die Funktionsweise von Wuala soll nun die Benutzerfreundlichkeit und Praxistauglichkeit von Wuala untersucht werden. Da ich unter Linux arbeite beziehen sich alle Beobachtungen auf die Linux-Version von Wuala. Die Linux-Version könnte sich, vor allem weil es sich um eine Beta-Version handelt, von denen auf anderen Plattformen unterscheiden.

A. Der Java-Client

Die Wuala-Entwickler legen Wert auf eine intuitive Benutzeroberfläche und haben es geschafft die aufwendige Netzwerk-Technologie hinter einer einfachen Benutzeroberfläche zu verbergen, so dass der Nutzer fast nicht merkt, dass die Daten in einem Netzwerk gespeichert werden. Aufgrund der Ähnlichkeit mit einem Dateimanager findet man sich schnell zurecht und die meisten Funktionen sind selbsterklärend. Private, geteilte und öffentliche Ordner lassen sich durch verschiedene Farben gut unterscheiden. Zudem lassen sich Dateien per Drag&Drop herunter- beziehungsweise hochladen. Sehr gut gelungen ist auch die Integration von Multimedia-Inhalten. Große Ordner mit vielen Fotos werden schnell geladen und jedes Foto als Thumbnail präsentiert. Öffnet man eine Datei, so wird sie automatisch im passenden Programm geöffnet. Ausserdem gibt es eine Streaming-Funktion für große Dateien, wie zum Bespiel Videos. Ein nettes Feature ist eine Funktion zur automatischen Größenänderung von Fotos vor dem Upload.
Das Stöbern im öffentlichen Welt-Teil der Software, wo alle als öffentlich markierten Dateien gesammelt werden, ist nichts besonderes, da sich dort zur Zeit fast nur aus dem Internet kopierte Inhalte befinden. Sehr praktisch ist jedoch die Idee des Schweizer Fernsehens (SF) einen Teil ihrer Sendungen in Wuala anzubieten [9]. Für Vielnutzer ist die Benutzeroberfläche von Wuala jedoch zu wenig anpassbar. Die Bedienung ist nur über die Maus möglich, man kann nicht per Tastatur navigieren. Deshalb möchte man auf Dauer lieber mit seinem gewohnten Dateimanager arbeiten, was durch Wualas Integration ins Dateisystem möglich ist. Leider besitzt Wuala keine automatische Backup-Funktion, wodurch es nicht geeignet ist, um seine Daten zu sichern.

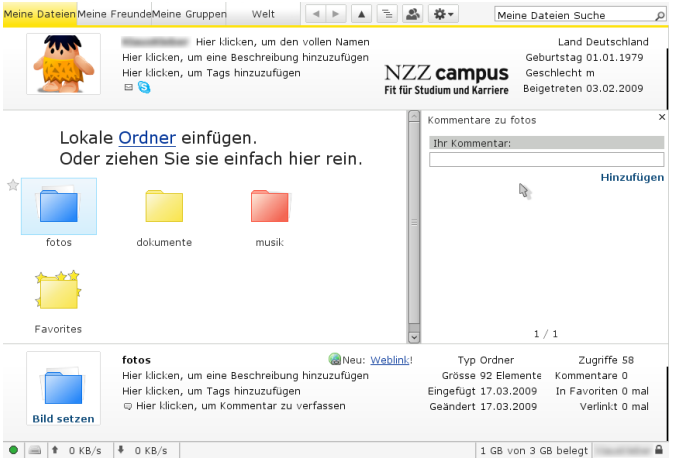

Abbildung 2. Bildschirmfoto des Wuala-Client

B. Dateisystemintegration

Die Dateisystemintegration erfolgt unter Linux durch einbinden eines NFS-Laufwerks. Somit hat man problemlosen Zugriff auf seine Wuala-Dateien und kann sie mit seinem eigenen Dateimanager verwalten. Die Integration ist jedoch nicht optimal gelöst. So kann man im Dateimanager nicht erkennen ob ein Ordner privat, geteilt oder öffentlich ist. Durch die Integration ins Dateisystem können auch andere Programme auf Dateien in Wuala zugreifen, wie zum Beispiel ein Skript zum Online-Backup wichtiger Dateien.

C. Zugriff über die Wuala-Webseite

Die Online-Schnittstelle zur Verwaltung der Dateien ist gut gelungen. Die Webseite ist schlicht gehalten und einfach zu benutzen. Sehr praktisch ist, dass hochgeladene Fotos automatisch als Bildergalerie angezeigt werden. Auch die Möglichkeit private Links zu verschicken, um jemand der keinen Wuala-Account hat den Online-Zugriff auf ausgewählte Dateien zu gewähren ist nützlich und ersetzt lästige One-Klick-Hoster. Ich musste jedoch feststellen, dass die Seite vor allem bei der Anzeige von Fotos relativ langsam lädt. Auch ist es per Design nicht möglich Dateien über ein Web-Formular hochzuladen, da die Dateien vor dem Upload verschlüsselt werden müssen.

D. Tauschen von Speicher

Benötigt man mehr Online-Speicher, so kann man entweder zusätzlicher Speicher bei Wuala kaufen, oder lokalen Speicher gegen Online-Speicher tauschen. Hierbei gilt die Formel:

$$\begin{aligned} Onlinespeicher \quad = \quad & Zur\ Verfügung\ gestellter \\ & Speicherplatz\ * \\ & prozentuale\ Onlinezeit \end{aligned}$$

Somit bekommt ein Nutzer, der 20GB auf seiner Festplatte freigibt und im Durchschnitt jeden Tag 6 Stunden online ist, 5GB Online-Speicherplatz. Gibt man mehr als 20GB auf seiner Festplatte frei, so müssen mindestens 10% des freigegebenen Speichers auch bereits von Wuala benutzt werden, damit der zusätzliche Online-Speicher angerechnet wird [10]. Somit muss man bevor man den zusätzlichen Online-Speicher nutzen kann zuerst warten bis Wuala genug fremde Fragmente auf dem Rechner gesammelt hat.

IV. Sicherheit

Der Schutz der Dateien in Wuala ist gerade wegen des Konzeptes private Dateien in einem Peer-to-Peer-Netzwerk zu speichern von großer Bedeutung. In der IT-Sicherheit wird der Schutz von Dateien in mehrere konkrete Schutzziele untergliedert [11]. Im Folgenden wird untersucht wie gut Wuala für seinen Einsatzzweck relevante Schutzziele erfüllt. Am Ende dieses Kapitels wird noch kurz auf den Aspekt des nicht öffentlichen Quellcodes eingegangen.

A. Authentizität

Der Benutzer authentifiziert sich gegenüber Wuala durch ein Passwort, wie bei fast allen Diensten im Internet. Diese Methode ist nicht gerade sicher, jedoch gibt es keine Alternative die sich ähnlich einfach implementieren und benutzen lässt.

B. Datenintegrität

Da die Daten im Wuala-Netzwerk auf viele fremde Rechner verteilt liegen und deshalb nicht vor Manipulationen geschützt werden können, müssen unberechtigte Änderungen der Daten erkannt werden. Die Integrität einer Datei wird deshalb durch eine separate Hash-Datei auf dem zentralen Wuala-Server überprüft. Wird eine neue Datei ins Wuala-Netzwerk geladen oder eine alte überschrieben, so wird automatisch ein Hash-Wert der Datei gebildet und auf den Wuala-Server geladen. Beim Abrufen der Datei wird nun der gespeicherte Hash-Wert vom Wuala-Server geladen und mit dem Hash-Wert der heruntergeladenen Datei verglichen. Zum Bilden des Hash-Wertes kommt SHA-256 zum Einsatz [12]. Die Kollisionsfreiheit des Algorithmus macht es praktisch unmöglich zwei verschiedene Dateien mit dem gleichen Hash-Wert zu finden. Somit kann eine unbemerke Änderung der Datei (nahezu) ausgeschlossen werden, solange der Hash-Wert vor Veränderungen geschützt ist. Dieser Hash-Wert wird im Klartext auf dem Wuala-Server gespeichert, kann jedoch nur überschrieben werden, wenn die Schreib-Operation mit dem passenden Signatur-Schlüssel signiert ist. Im Besitz dieses Schlüssels sind nur Benutzer mit Schreibrecht für diese Datei. Dadurch kann trotz der Speicherung der Daten in einem nicht verlässlichen Netzwerk deren Integrität garantiert werden.

C. Informationsvertraulichkeit

Um unberechtigte Lesezugriffe auf Dateien zu verhindern werden alle Dateien vor dem Upload ins Wuala-Netzwerk verschlüsselt. Dazu wird AES mit 128 bit Schlüssellänge benutzt. Der AES-Algorithmus mit einer Schlüssellänge von 128 bit gilt als sicher und ist im Moment auch mit speziellen Supercomputern nicht zu knacken [13]. Als Modus der AES-Blockchiffre wird inzwischen Cipher Block Chaining (CBC) [11] verwendet [14], welches eine höhere Sicherheit bietet als zuvor verwendete Electronic Code Book (ECB) [11]. Zusätzlich wird sichergestellt, dass die für den CBC-Modus benötigten Initialisierungsvektoren für alle Dateien, die mit dem gleichen Schlüssel verschlüsselt sind, verschieden sind. Die AES-Schlüssel werden mit dem schon vorgestellten Cryptree verwaltet. Durch den Aufbau von Cryptree ist der Besitzer des Schlüssels eines Ordners in der Lage dessen Dateien und alle Unterordner zu entschlüsseln, jedoch keine Nachbar- oder höher gelegene Ordner. Es können nur die Namen der höher gelegenen Ordner entschlüsselt werden um den globalen Pfad des Ordners zu ermitteln. Dies ermöglicht es die Schlüssel für einzelne Ordner und Dateien freizugeben, ohne die anderen Schlüssel zu gefährden. Gelangt ein Angreifer an den Schlüssel des Wurzel-Ordners eines Benutzers, so kann er alle Ordner und Dateien des Benutzers entschlüsseln. Damit der Benutzer selbst an den Schlüssel des Wurzel-Ordners kommt, wird dieser wie bereits erwähnt aus einem Hash-Wert über den Benutzernamen und das Passwort gebildet. Somit ist jeder Benutzer selbst für die Sicherheit seiner Daten verantwortlich, indem er ein sicheres Passwort wählt. Der AES-Schlüssel zur Verschlüsselung einer Datei wird aus einem dem SHA-256 Hash-Wert über der Datei selbst generiert [15].

Dadurch unterscheiden sich gleiche Dateien auch nach der Verschlüsselung nicht und eine weit verbreitete Datei, die viele Nutzer hochgeladen haben muss nur einmal gespeichert werden, was Speicherplatz spart. Der Nachteil daran ist, dass man über die Hashes zur Verifikation der Datei herausfinden kann wer alles diese Datei besitzt, auch wenn der Benutzer diese Datei in einem privaten Ordner gespeichert hat [16]. Zwar hat nur Wuala allein die Möglichkeit den Hashwerten Benutzer zuzuordnen, jedoch ist es Wuala dadurch möglich das Netzwerk zu zensieren: Dazu hat Wuala eine Sammlung an Dateien, die sie verbieten möchten. Nun werden diese Dateien verschlüsselt und ihre Hash-Werte gebildet und mit den Hash-Werten aus Wuala verglichen. Wuala kann diese Dateien laut den AGBs [17] ohne Angabe eines Grundes löschen. Weiterhin kann Wuala alle Benutzer ausfindig machen, die eine dieser Dateien besitzen. Speichert man in Wuala private, selbst erstellte Dateien die niemand sonst besitzt, so ist dies nicht möglich.

D. Verfügbarkeit

Um eine möglichst hohe Verfügbarkeit der Dateien im Wuala-Netzwerk zu gewährleisten wird jede Datei wie in Kapitel 2 beschrieben mit Hilfe von Erasure Codes redundant gespeichert, was eine hohe Verfügbarkeit gewährleistet. Zusätzlich wird jede Datei auf dem zentalen Wuala-Server gespeichert. Somit kann eine Datei auch abgerufen werden, wenn sie nicht oder nicht vollständig im Netzwerk verfügbar ist. Sollte der Wuala-Server einmal ausfallen, so könnte eine Datei im Großteil aller Fälle theoretisch immer noch aus dem Netzwerk geladen werden. Das macht jedoch keinen Sinn, da die Integriät der Datei ohne den Wuala-Server nicht geprüft werden kann. Deshalb ist die Verfügbarkeit von Dateien im Wuala-Netzwerk von der Verfügbarkeit des Wuala-Servers abhängig.

E. Verbindlichkeit anstatt Anonymität

Wuala ordnet jeder Datei und jedem Kommentar einen Besitzer in Form eines Wuala-Benutzers zu. Außerdem wird bei jedem Log-in eines Wuala-Nutzers seine IP-Adresse und die Zeit mitprotokolliert [18]. Dadurch kann es Strafverfolgern im Falle eines Gesetzesbruchs ermöglicht werden Rückschlüsse auf die reale Person, welche die Datei ins Wuala-Netzwerk geladen hat, zu ziehen. Anonymität ist im Wuala-Netzwerk von den Entwicklern nicht gewollt [19]. Da es keine Möglichkeit gibt Dateien anonym hochzuladen ist es möglich, das Verbreiten von illegalen Dateien und Urheberrechtsverletzungen zu verfolgen, was Wuala in den AGBs [17] ausdrücklich ankündigt wenn ein solcher Verstoß gemeldet wird. Dort kann ebenfalls nachgelesen werden, dass Wuala selbst jedoch nicht aktiv werden das Netzwerk nach illegalen Inhalten durchsuchen will. Im Oktober 2008 wurde in Wuala auf Druck der Filmindustrie eine Gruppe geschlossen, die hauptsächlich dem Tausch unheberrechtlich geschützter Dateien diente [20]. Da sich scheinbar Mitarbeiter der Filmindustrie in der Gruppe befanden und Wuala über die Missachtung der Uhrheberrechte informierten, wurde die Gruppe geschlossen um die Nutzer vor Abmahnungen zu schützen. Dieser Fall zeigt, dass Wuala sich so gut wie möglich aus rechtlichen Streitigkeiten heraus halten will und nicht darauf aus ist seine eigenen Nutzer zu verklagen.

F. Nicht-öffentlicher Quellcode

Obwohl Wuala auf einer ganzen Reihe von Open-Source-Projekten basiert [21], ist der Quellcode von Wuala nicht öffentlich zugänglich. Auf meine Anfrage hin wurde mir mitgeteilt, dass es auch nicht geplant sei den Quellcode zu veröffentlichen. Da man also nicht selbst überprüfen kann was das Programm macht bleibt nur den Wuala-Entwicklern zu vertrauen, dass Wuala keine Spyware, Trojaner oder sonstige Schadprogramme enthält. So könnte der Wuala-Client beispielsweise das Benutzerpasswort speichern und an einen Wuala-Server senden. Privatpersonen werden trotzdem wohl nicht allzu skeptisch sein und dem schweizer Startup ihre privaten Daten anvertrauen. Für Firmen - welche ausdrücklich zur Wuala-Zielgruppe gehören [22] - die ihre Geschäftsdaten in Wuala speichern möchten stellt dies jedoch eine grössere Hürde dar.

V. Vergleich mit serverbasierten Cloud-Storage-Diensten

Wuala sticht durch zwei Besonderheiten aus der Masse der Cloud-Storage-Services hervor: Erstens speichert es die Dateien als einziger Service in einem Peer-to-Peer-Netzwerk ab und nicht nur auf einem zentralen Server. Zweitens ist es der einzige Service, der Community-Features eines Sozialen Netzwerks wie das Bilden von Freundschaften und Gruppen, sowie eine Kommentarfunktion bietet [23].
Auch bei der Sicherheit geht Wuala andere Wege. Wuala verschlüsselt die Dateien nämlich schon vor dem Upload ins Netz. Dadurch kann angeblich nicht einmal Wuala selbst meine privaten Dateien entschlüsseln. Da der Quellcode von Wuala nicht öffentlich ist, kann das nicht überprüft werden. Andere Services, wie zum Beispiel Dropbox [24], verwenden eine SSL-Verschlüsselung zur Übertragung auf den Server wo sie dann vom Anbieter verschlüsselt werden. Dadurch ist der Anbieter in der Lage alle Dateien zu entschlüsseln.
Bei der Geschwindigkeit hat Wuala einen Vorteil gegenüber rein serverbasierten Diensten, da eine Datei parallel von mehreren Rechnern geladen wird, anstatt sequentiell von einem Server. Dieser Vorteil wird umso spürbarer, je mehr das Wuala-Netzerk wächst, da dann tendenziell weniger Dateien vom Server geladen werden müssen. Beim Upload gibt es im Normalfall keine spürbaren Unterschiede. Falls jedoch eine Datei ins Wuala-Netzwerk geladen werden soll, die bereits vorhanden ist, muss diese nicht nochmals hochgeladen werden, wodurch sich wieder ein Geschwindigkeitsvorteil für Wuala ergibt.
Für die meisten Cloud-Storage-Dienste muss ein Client-Programm installiert werden, welche meist für Windows und MacOS verfügbar sind. Linux wird nur ungefähr von der Hälfte der Cloud-Storage-Dienste unterstützt. Hervorzuheben ist hier Box.net [25] welches keine Client-Software benötigt

und komplett über den Browser bedient wird.
Die Dateisystem-Interation ist bei Wuala Wuala bietet zwar eine Integration ins Dateisystem, diese ist jedoch noch verbesserungswürdig. Andere Anbieter wie Dropbox [24] und ZumoDrive [26] haben ihre Dienste besser ins Dateisystem integriert. Hier zeigt ein kleines Symbol an jeder Datei an, ob die Datei aktuell mit der Online-Version synchronisiert ist. Zudem bieten beide Dienste eine History-Funktion, mit der alte Versionen einer Datei wiederhergestellt werden können.
Die Preise für zusätzlichen Speicher für Wuala liegen am unteren Ende der Preisspanne für Cloud-Storing-Dienste. Zusätzlich bietet Wuala als einzigster Anbieter die Option lokalen Speicherplatz gegen Online-Speicher zu tauschen, und so völlig kostenlos zusätzlichen Speicher zu erhalten.

Tabelle I
VERGLEICH AUSGEWÄHLTER CLOUD-STORAGE-DIENSTE

	Wuala	Dropbox	ZumoDrive	Box.net
Kostenloser Speicher	1GB	2GB	1GB	1GB
50 GB extra (pro Jahr)	60 Euro	75 Euro	109 Euro	-
Dateisystem-Integration	ja	ja	ja	nein
Betriebsysteme	W,M,L	W,M,L	W,M	alle
History-Funktion	nein	ja	ja	ja

Legende: W = Windows, M = MacOS, L = Linux, Stand: 29.04.2009

VI. ZUSAMMENFASSUNG UND AUSBLICK

Wuala ist für den Heimanwender eine gute Lösung seine Dateien online verfügbar zu machen. Es besitzt keine gravierenden Sicherheitslücken und bieten kostenlos jede Menge Speicher. Durch die Einzigartigkeit und Leistungsfähigkeit der Software hat Wuala gute Karten auf dem umkämpften Online-Speicher-Markt zu bestehen. Gespannt sein darf man außerdem welche neuen Entwicklungen die Fusion von Wuala mit dem Festplattenhersteller LaCie [27] bringt. Da LaCie bereits eine Festplatte mit Internetzugriff [28] im Programm hat, liegt es nahe dass LaCie eine Wuala-fähige Festplatte auf den Markt bringen könnte.

LITERATUR

[1] Wikipedia.com, "Cloud Storage," *http://en.wikipedia.org/w/index.php?title=Cloud_computing&oldid=286817477#Storage*, 29.04.2009
[2] Wikipedia.com, "Erasure code," *http://en.wikipedia.org/w/index.php? title=Erasure_code&oldid=258867740*, 29.04.2009
[3] D. Grolimund, "Wuala - a distributed file system," *http://www.youtube.com/watch?v=3xKZ4KGkQY8*, 29.04.2009
[4] Wikipedia.com, "Reed–Solomon error correction," *http://en.wikipedia.org/wiki/Reed_Solomon*, 29.04.2009
[5] GetSatisfaction.com, "Cleversafe - Wuala's Twin?," *http://getsatisfaction.com/wuala/topics/cleversafe_wualas_twin*, 29.04.2009
[6] D. Grolimund, L. Meissner, S. Schmid, R. Wattenhofer, "Cryptree: A Folder Tree Structure for Cryptographic File Systems," SRDS, 2006
[7] Petar Maymounkov, David Mazières, "Kademlia: A Peer-to-peer Information System Based on the XOR Metric," New York University, *http://pdos.csail.mit.edu/ petar/papers/maymounkov-kademlia-lncs.pdf*
[8] D. Grolimund, L. Meissner, S. Schmid, R. Wattenhofer, "Havelaar: A Robust and Efficient Reputation System for Active Peer-to-Peer Systems," NETECON, 2006
[9] Wuala, "Schweizer Fernsehen - Wuala, social online storage," *http://www.wuala.com/Schweizer%20Fernsehen*
[10] GetSatisfaction.com, "Send me data!," *http://getsatisfaction.com/wuala/topics/send_me_data*, 29.04.2009
[11] C. Eckert, "IT-Sicherheit," 5. Auflage, München: Oldenbourg-Verlag, 2008
[12] C. Percival, "Wuala update," *http://www.daemonology.net/blog/2007-10-26-wuala-update.html*, 29.04.2009
[13] National Institute of Standards and Technology, "AES Questions & Answers," *http://www.nist.gov/public_affairs/releases/aesq&a.htm*, 29.04.2009
[14] C. Percival, "Wuala's improved security," *http://www.daemonology.net/blog/2008-11-07-wuala-security.html*, 29.04.2009
[15] GetSatisfaction.com, "Instant upload?! Hows that work with encryption?," *http://getsatisfaction.com/wuala/topics/instant_upload_hows_that_work_with_encryption*, 29.04.2009
[16] GetSatisfaction.com, "Dateien löschen innerhalb des Wuala," *http://getsatisfaction.com/wuala/topics/dateien_l_schen_innerhalb_des_wuala*, 29.04.2009
[17] Wuala, "Allgemeine Geschäftsbedingungen," *http://www.wuala.com/de/about/terms*, 29.04.2009
[18] GetSatisfaction.com, "IP-Log," *http://getsatisfaction.com/wuala/topics/ip_log*, 29.04.2009
[19] GetSatisfaction.com, "Complete Privacy; feature request," *http://getsatisfaction.com/wuala/topics/complete_privacy_feature_request*, 29.04.2009
[20] gulli.com, "Filmindustrie lässt gulli-Usergroup löschen (update)," *http://www.gulli.com/news/wuala-filmindustrie-l-sst-2008-10-09*, 29.04.2009
[21] Wuala, "Quellcode von Drittanbietern," *http://www.wuala.com/de/about/thirdpartycode*, 29.04.2009
[22] Wuala, "Wer benutzt Wuala?," *http://www.wuala.com/de/learn/usecases*, 29.04.2009
[23] Neue Zürcher Zeitung, "Festplatte mit sozialer Ader," *http://www.nzz.ch/magazin/mobil/festplatte_mit_sozialer_ader_1.804251.html*, 29.04.2009
[24] Dropbox, *https://www.getdropbox.com*, 29.04.2009
[25] Box.net, *http://www.box.net*, 29.04.200
[26] ZumoDrive, *http://zumodrive.com*, 29.04.200
[27] Wuala, "Exciting news: Wuala merges with LaCie," *http://www.wuala.com/blog/2009/03/exciting-news-wuala-merges-with-lacie.html*, 29.04.2009
[28] LaCie, "LaCie Internet Space," *http://www.lacie.com/de/products/ product.htm?pid=11136*, 29.04.2009