تعیین و دسته‌بندی معیارهای قابلیت اطمینان در حفاظت رقمی

دکتر حمید قاضی‌زاده [۱]، مریم سادات سیدین [۲]، حیدر مختاری [۳]

تاریخ ارسال: ۱۳۹۷/۱/۱۶ ـ تاریخ پذیرش: ۱۳۹۷/۳/۸

چکیده

هدف: از آنجاکه فرایند مدیریت محتوای دیجیتال برای تضمین دسترس‌پذیری طولانی‌مدت به این محتواست، شناخت معیارهای تضمین قابلیت اطمینان و دوام این آرشیوها اهمیت فراوان دارد. هدف این پژوهش، تعیین و دسته‌بندی معیارهای قابلیت اطمینان در حفاظت رقمی در این آرشیوهاست.

روش: روش پژوهش کتابخانه‌ای ومروری ـ تحلیلی است تا بتوان برای تضمین قابلیت اطمینان در نظام‌های حفاظت دیجیتال، بهترین شیوه‌ها و استانداردها را استخراج و از آنها استفاده کرد.

یافته ها: سطوح قابلیت اطمینان آرشیوهای دیجیتال و الزام های آن در سه سطح نیروی انسانی، وجوه فناوری و زمینهٔ اقتصادی، قابل دسته‌بندی است که هر کدام از سطوح به بخش های فرعی تری نظیر شیوه اداره و دوام سازمانی، ساختار سازمانی و به کارگماری نیروی انسانی، دوام‌پذیری مالی، ایجاد بسته‌های آرشیوسازی و مدیریت دسترسی دسته‌بندی شده و عملکرد متفاوتی خواهدداشت.

نتایج: نتایج نشان داد می‌توان این معیارها را در سه گروهِ کلی برای عمل و پژوهش در باب آزمون اطمینان‌پذیری و دوام آرشیوهای دیجیتال مختلف، به‌کار برد.

کلیدواژه‌ها: حفاظت رقمی، قابلیت اطمینان، آرشیو دیجیتال، معیارهای دسته‌بندی.

---

۱. عضو هیئت‌علمی گروه علم اطلاعات و دانش‌شناسی دانشگاه پیام نور. ghazi.hamid@gmail.com

۲. دانشجوی دکترای علم اطلاعات و دانش‌شناسی دانشگاه آزاد همدان. maryamseyedein@yahoo.com

۳. عضو هیئت‌علمی گروه علم اطلاعات و دانش‌شناسی دانشگاه پیام نور. mokhtariazad@gmail.com

مقدمه و بیان مسئله

آرشیو دیجیتال رسانه‌های دیجیتال با مجموعه‌ای از پیشینه‌های رقمیِ تولیدشده توسط سازمان‌ها و افراد است که برای استفاده‌های آتی، ذخیره و از آن حفاظت می‌شود و در دسترس قرار می‌گیرد. ویژگی منحصربه‌فرد رسانه‌های دیجیتال نسبت به رسانه‌های سنتی، ایجاد و حفظ محتوایی به‌روز است؛ ولی این رسانه‌ها سریع‌تر از رسانه‌های سنتی دچار آسیب‌دیدگی می‌شوند و این آسیب‌دیدگی آنها ممکن است سبب از بین رفتن بخشی یا تمامی داده‌های ذخیره‌شده شود. پیشرفت‌های چشمگیر در قدرت پردازش کامپیوتر، افزایش پهنای باند شبکه اینترنت و ارتباطات فناورانه منجر به تولید فراوان اطلاعات در قالب‌های دیجیتال شده است. البته، انقلاب‌های فناورانه منجر به کهنگی‌های زودرس سخت‌افزاری و نرم‌افزاری نیز می‌شود. این تحولات، در ساختار و قالب‌های داده نیز تأثیرهای شگرفی دارد؛ به‌طوری‌که قالب‌های جدید با قابلیت‌های بیشتر به سرعت روی کار می‌آیند تا اطلاعات، مؤثرتر نمایش داده شوند. از طرفی، با پیشرفت‌های فناوری و تحولات رسانه‌ها و قالب‌های اطلاعاتی، نیازها و ذائقه‌های اطلاعاتی جامعه نیز تغییر می‌کند. از این‌رو، برنامهٔ حفاظت در آرشیوهای دیجیتال باید چنان باشد که دوام آنها را در مدت‌زمان طولانی تضمین کند (CCSDS[1] , 2002) و قابلیت آنها را افزایش دهد و روزآمدی‌شان را تسریع کند.

حفاظت دیجیتال، حفاظت از منابعی است که در اصل دیجیتالی پدیدآمده یا حاصل قالب‌بندی مجدد[2] هستند. فرایند مدیریت محتوای دیجیتال دربردارندهٔ مجموعه‌ای از فعالیت‌ها در طول زمان معیّن برای تضمین دسترس‌پذیری طولانی‌مدت به این محتواست (Kahle, 1996). بر این اساس، حفاظت بلندمدت[3] فرایندی مداوم است که در آن به پیشینه‌های دیجیتال، اطلاعات توصیفی اختصاص می‌یابد و سپس

1. Consultative Committee of Space and Data Systems
2. Reformatting
3. Long term preservation

آنها برای مدت‌زمان طولانی در چندین محل ـ البته با بالاترین درجه وضوح[1] ـ ذخیره می‌شوند. در حفاظت دیجیتال، به‌منظور جلوگیری از اتلاف داده[2] و یا ناتوانی در خواندن داده، پیشینه‌ها به‌طور دوره‌ای به یک رسانهٔ جدید انتقال می‌یابند و قالب‌ها قبل از کهنه‌شدن تغییر می‌کنند. بدین‌ترتیب، دسترسی به مجموعه‌های دیجیتال در حال و آینده امکان‌پذیر می‌شود. در گذشته، به‌دلیل نبود «اجتماع حفاظت دیجیتال»[3] سازمان‌یافته، نبودِ توافق در روش‌های حفاظت دیجیتال و فقدان استانداردها، هر آرشیو به شیوهٔ خاصّ خود حفاظت دیجیتاِل بلندمدت را انجام می‌داد (CCSDS, 2010). از آنجاکه هدف آرشیوهای دیجیتال، به‌ویژه در نظام اطلاعاتی آرشیوی باز، حفاظت بلندمدت و دسترس‌پذیری طولانی است، بالا بردن میزان اطمینان‌پذیری و دوام آنها اهمیت فراوان دارد (Ross & McHugh, 2005). بر این اساس، تدوین معیارهایی که ویژگی‌های آرشیوی مطمئن را توصیف کند، اهمیت فوق‌العاده دارد.

وجود معیارهای مشترک در اطمینان‌پذیری در حفاظت دیجیتال، گامی ارزنده در جلوگیری از دوباره‌کاری و اتلاف زمان و نیروست. بنابراین، شناخت و تعیین معیارهای قابلیت اطمینان در حفاظت رقمی ضروری است. در این پژوهش، معیارهای قابلیت اطمینان در متون منتشرشدهٔ دهه‌های اخیر مورد توجه و واکاوی قرار گرفته است تا بتوان برای تضمین قابلیت اطمینان در نظام‌های حفاظت دیجیتال، بهترین شیوه‌ها و استانداردها را استخراج و از آنها استفاده کرد. همچنین در بررسی اطمینان‌پذیری به این نوع حفاظت در آرشیوهای خاص، می‌توان از این معیارها برای تحقیق و عمل بهره‌مند شد.

در این راستا، پژوهش مروری حاضر برای پاسخگویی به این سؤال انجام شده است که نظام‌های حفاظت‌شدهٔ دیجیتال به چه معیارهایی از قابلیت اطمینان در حفاظت بلندمدت از داده‌ها تأکید کرده‌اند و نیز اینکه معیارهای قابلیت اطمینان در نظام‌های حفاظت دیجیتال در هر دورهٔ مشخص طی دهه‌های اخیر متفاوت از دیگر دوره‌ها بوده

---

1. Resolution
2. Data corruption
3. Preservation Digital Society

است یا معیارهایی مشترک می‌توان برای آنها در نظر داشت.

روش پژوهش

روش پژوهش حاضر مروری ـ تحلیلی است. به‌منظور بررسی متون مرتبط موجود، در گوگل اسکالر با کلیدواژه‌های لاتین trustworthiness, reliability, digital preservation, digital archive و کلیدواژه‌های فارسی «قابلیت اطمینان»، «حفاظت دیجیتال» و «آرشیوهای دیجیتال» جستجوهایی انجام شد. با مرور نتایج به‌دست‌آمده، از میان متون بازیابی‌شده مواردی به‌عنوان مرتبط در نظر گرفته شد که در بخش بعد (مرور پیشینه) شرح داده می‌شوند.

پیشینه پژوهش

در منابع فارسی «قابلیت اطمینان» را کم‌وبیش این طور تعریف می‌کنند: «احتمال ادامه کار یک سیستم یا وسیلهٔ کامپیوتری تحت شرایط مشخص در طی یک دورهٔ معیّن.»(فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، ۱۳۸۲، ذیل واژه) و نیز احتمال آنکه قطعه، دستگاه یا سیستمی کارکرد مورد نظر را تحت شرایط مفروض، از قبیل شرایط زیست‌محیطی، محدودیت‌های زمان عمل، فراوانی و دقت نگهداری در دورهٔ زمانی مشخص، به‌صورت رضایت‌بخش انجام دهد (پارکر، ۱۳۷۹: ۶۷۲).

از نظر سابقهٔ تاریخی، قابلیت اطمینان در پیشینه‌های چاپی وجود دارد که می‌توان آن را به کارکرد علم اطلاع‌رسانی منتسب کرد. به‌عنوان مثال، در قرن ۱۶، گروهی از پیروان فلسفهٔ بدبینی به نام Pyrrhonist به قابلیت اطمینان منابع تاریخی حمله کردند و معتقد بودند که دانش از طریق مجموعه‌ای از منابع غیرقابل‌اطمینان در طول تاریخ فیلتر شده است.

«توماس نوبل»[1] (۱۹۹۰) معتقد بود یکی از ویژگی‌های دوران باستان نسبت به قرون وسطی، تفاوت در نسخه‌های حفاظت‌شده در آرشیوهای عمومی نسبت به نسخه‌هایی است که در دست مردم قرار می‌گرفت. در نتیجه، بحث قابلیت اطمینان به اسناد پدید

1. Thomas Noble

آمد که به روش گردآوری اسناد و اعتبار نویسنده بستگی داشت).

در بررسی متون مربوط به قابلیت اطمینان در گوگل اسکالر، در دهۀ ۱۹۹۰، به پژوهش‌هایی در تضمین قابلیت اطمینان در نظام‌های تجارت الکترونیک برمی‌خوریم که برخی مربوط به طراحی رابط کاربراست (از جمله Kim& Moon, 1998؛ Van Mulken, André & Müller, 1999؛ Cassell & Bickmore, 2000). البته، در این دهه قابلیت اطمینان در نرم‌افزارها (از جمله Amoroso et al, 1994) و وب (Portz, 2000) است.

محققان دیگر طی این دهه (از جمله Duranti, 1995و MacNeil, 2000) در بحث از قابلیت اطمینان اسناد، ویژگی‌های متعددی را در نظر گرفته‌اند. از جمله:

- قابلیت اعتماد[1]
- اصالت[2]
- سندیّت.

در متون علم اطلاع‌رسانی، به مدل کلتون (Kelton, Fleischmann & Wallace, 2008) برمی‌خوریم که چهار ویژگی را برای منبع اطلاعاتیِ مطمئن برمی‌شمارد:

- صحت[3]
- هدفمندی[4]
- اعتبار[5]
- ثبات.[6]

طی دهه‌های بعد، پژوهشگران دیگر، برای بررسی قابلیت اطمینان داده‌های پزشکی،

---

1. Reliability
2. Genuineness
3. Authenticity
4. Objectivity
5. Validity
6. Stability

مدل Time-variant Medical Data Trustworthiness (TMDT) را پیشنهاد دادند. در این مدل که مبتنی برروبکرد آماری ـ ریاضی بود، به داده‌های پزشکی ابرداده‌هایی نظیر سازمان‌های مرتبط با سلامت، زمان و شاغلان پزشکی اختصاص یافته است (Alhaqbani, & Fidge, 2009)

در وب ۲ و ابزارهای آن، مانند ویکی‌ها، نگرانی‌هایی دربارهٔ کیفیت دانش و قابلیت اطمینان گروه‌هایی که دانش را به اشتراک می‌گذارند، وجود دارد. «یانگ[1] و دیگران» (۲۰۱۴) مدلی برای ارزیابی قابلیت اطمینان این دانشِ اشتراکی عرضه کرده‌اند که بازخوردی و دوطرفه است و دو جزء دارد: قابلیت اطمینان به منبع و قابلیت اطمینان به کاربر.

در سال ۲۰۱۵ دیدگاه و درک کاربران از ویژگی‌های قابلیت اطمینان، مانند دقت[2]، مقبولیت[3]، پوشش[4]، روزآمدی[5]، هدفمندی، ثبات، اعتبار، صحت، دست اول / دوم بودن[6] و خوانایی[7] تحلیل شد (Donaldson & Conway, 2015)

بررسی‌های فوق نشان می‌دهد قابلیت اطمینان در حوزه علم اطلاع‌رسانی از دیرباز مطرح بوده است. با مطالعه این منابع و دیگر منابع مرتبط در باب قابلیت اطمینان در نظام‌های رقمی، می‌توان معیارهای خرد و کلان برای آرشیوهای دیجیتال را استخراج و پیشنهاد کرد که در بخش‌های بعد تعیین، تبیین و دسته‌بندی شده‌اند.

---

1. Yang
2. Accuracy
3. Believability
4. Coverage
5. Currency
6. First-hand/Primary
7. Legibility/Readability

یافته‌های مربوط به قابلیت اطمینان در حفاظت دیجیتال

در سال ۱۹۵۲، اولین بار وزارت دفاع آمریکا گروهی را مأمور بررسی قابلیت اطمینان تجهیزات و لوازم الکتریکی کرد. فعالیت این گروه سرآغازی برای فعالیت سایر انجمن‌ها و جوامع در این زمینه شد و امروزه استانداردهای فراوانی برای تعیین و ارزیابی وسایل، تجهیزات و نظام‌های مختلف تدوین شده است.

در ۱۹۶۷، در کمپانی آلن بوبکوک[1] و در بحث از قابلیت اطمینان نظام‌های پردازش کامپیوتری، بر چهار حوزه تمرکز شده است:

۱. قابلیت اعتماد[2]

۲. یکپارچگی[3]

۳. امنیت[4]

۴. محرمانگی.[5]

در سال ۱۹۸۸، مرکز ملی امنیت کامپیوتری[6] در آمریکا، راهنمایی تدوین کرد که در آن، روش‌های ارزیابی و سنجش نظام‌های مطمئن، با تأکید بر پردازش اطلاعات نظامی شناسایی شد. این مرکز در سال ۱۹۹۲ در دستنامه‌ای، در تعریف نظام کامپیوتری مطمئن، به تضمین سخت‌افزاری و نرم‌افزاری تأکید کرد. در این سند، سازه «اعتماد» با مفاهیم قابل‌محاسبه‌بودن،[7] امنیت[8] و ارتباط[9] (در مفهوم تعامل بین شخص و ماشین)

---

1. Allen-Bobcock
2. Reliability
3. Integrity
4. Security
5. Privacy
6. National Computer Security Center (NCSC)
7. Audit ability
8. Security
9. Communication

همراه بود (RLG-OCLC[1], 2002).

در سال ۱۹۹۶، قابلیت اطمینان در پیشینه‌های الکترونیکی مسئلهٔ بسیار مهمی در کانادا شد. برای انجام مأموریتی،گزارش‌های پایگاه خودکار مرکز ملی اموردفاعی[2] باید بررسی می‌شد. نتیجهٔ این بررسی نشان داد بسیاری از پیشینه‌های الکترونیکی دچار نقص شده است؛ به‌عنوان مثال، شماره سریال‌های تعدادی از اسناد از بین رفته بود. بنابراین، بخش دفاع ملی نتوانسته بود صحت پیشینه‌ها را تضمین کند و این اقدام‌ها باید انجام می‌شد:

۱. وارسی و کنترل اطلاعاتی که باید وارد شود و نحوه ورود آنها برای تضمین صحّت پیشینه‌ها؛

۲. تمهید نظام پایگاه داده‌ای و نرم‌افزاری مناسب برای انجام دقیق فرایند ورود اطلاعات در هر فیلد و استخدام کارکنانی آموزش‌دیده برای این کار؛

۳. افزایش امنیت نظام براساس استانداردهایی مطابق با امنیت ملی و محدودکردن دسترسی به افرادی مشخص با گذرواژه و حساب کاربری و استفاده از فیلدهای امنیتی برای شناسایی افرادی که داده‌ها را وارد یا حذف می‌کنند.

«استفیک»[3] در سال ۱۹۹۷ به‌منظور حمایت از پدیدآورندگان و ناشران در برابر کپی‌برداری‌های غیرقانونی، دربارهٔ روش‌های تضمین امنیت و تغییرناپذیری منابع در وب صحبت به‌میان آورد و علاوه بر مفاهیم تعامل، امنیت و انطباق[4] در نظام‌های مطمئن، به تعیین هویّت و کنترل کپی‌برداری نیز تأکید کرد.

«هدستروم»[5] (۱۹۹۸) روش‌های متعددی برای بهبود نظام‌های مطمئن در

---

1. Research Library Group – Online Cataloging Library Center
2. National Defense Operation Center (NDOC)
3. Stefik
4. Compliance
5. Hedstrom

کتابخانه‌های دیجیتال و کامپیوتری پیشنهاد کرد. از دید وی، نظام‌هایی که در آنها خطرها، سودها و هزینه‌ها به تعادل رسیده‌اند، قواعدی مرکب از خط‌مشی‌ها و استانداردها دارند و مطمئن هستند.

«بلومنتال»[1] (۱۹۹۹) ابعاد قابلیت اطمینان در نظام‌های اطلاعاتی را بدین‌ترتیب برمی‌شمارد:

- امنیت اطلاعات
- محرمانگی داده‌های خصوصی
- ایمنی نظام[2]
- قابلیت اعتماد.

از نظر وی راه‌حل‌های قابلیت اطمینان منوط به درنظرگرفتن افراد، فناوری و خطّ مشی است.

سه محقق دانشگاه استنفورد، گام‌های ضروری برای اجرای آرشیو دیجیتال قابل اطمینان را به تفصیل بیان کرده‌اند. آنان در حفاظت اشیای دیجیتال، با تأکید بر راهبردهای تکثیر[3] در ذخیره‌سازی، به زیرساخت‌های سخت‌افزاری، نرم‌افزاری و سازمانی پرداخته‌اند. راهبرد تکثیر از حذف و دستکاری توسط کاربران جلوگیری می‌کند. این‌کار با تدوین خط‌مشی‌های نسخه‌برداری و تهیهٔ نسخهٔ پشتیبان امکان‌پذیر می‌شود. در پژوهش‌های آنان، علاوه بر تعامل و امنیت، به تکثیر در نظام‌های مطمئن هم اشاره شده است. تعامل از دیدگاه آنان مبادلات بین بخش‌های مختلف نظام است و کارهایی که در یک نظام مطمئن می‌توان انجام داد، عبارتند از:

- آشکارسازی[4] و ذخیرهٔ مجدد[5] اطلاعات خراب‌شده یا ازبین‌رفته؛

---

1. Blumenthal
2. System safety
3. Replication
4. Detection
5. Restore

- ارتباط بین بخش‌های نظام؛
- امنیت کاربر، مدیریت مالکیت فکری و فرایند پرس‌وجو؛[1]
- امکانات ورود و خروج برای انتقال اشیا به خارج و داخل مکان ذخیره‌سازی[2] (Cooper; Crespo & Garcia-Molina, 2001).

آنها کار را ادامه دادند و مزیّت‌های مشارکت در تکثیر در شبکه‌های نظیربه‌نظیر را بررسی کردند. آنان چالش‌های برآورد قابلیت اطمینان هر نظام را بررسی و عوامل زیر را در رفع این چالش‌ها مدّ نظر قرار دادند:

- بسامد خطاهای قبلی (از بین رفتن داده‌ها) برای پیش‌بینی خطاهای آینده؛
- استفاده از سخت‌افزار مطمئن؛
- وجود اقدام‌های امنیتی موفق؛
- اعتبار.

پژوهشگران دانشگاه فناوری کوئینزلند درباره ابزارهای ارزیابی نظام‌های قابل اطمینان مطالعه کردند. از نظر آنان، ارزیابی امنیت وتعیین سطح تضمین اهمیت زیادی دارد. بنابراین، آنان برکمّی‌کردن قابلیت اطمینان تأکید کرده‌اند (Jøsang, & Knapskog, 1998).

فدراسیون کتابخانه دیجیتال در سال ۲۰۰۰ م هفت معیار برای قابل‌اطمینان‌بودنِ واسپارگاه‌های آرشیوی با تأکید بر مجله‌های دیجیتالِ علمی، به‌عنوان اشیای دیجیتال تعریف کرد. در مقابل، دربارهٔ چگونگیِ انجام کارهای مربوط به حفاظت قابل اطمینان سکوت کرد و پژوهش‌های بیشتر را بنیاد اندرو ملون[3] برعهده گرفت. از منظر این فدراسیون، آرشیو دیجیتال مطمئن:

---

1. Query
2. Store
3. Andrew W. Mellon Foundation

- حداقل الزام‌های مورد توافق ناشران مجله‌ها و کتابخانه‌های پژوهشی را برآورده می‌کند؛
- با توجه به نیازهای ناشران مجله‌ها و کتابخانه‌ها، مأموریت خود را به وضوح تعریف می‌کند که در آن دامنه و ماهیت منابع کاملا مشخص شده باشد؛
- براساس توافق‌هایی که در آنها مسئولیت‌های طرفین در باب انواع منابع، قالب‌ها، رسانه‌ها، ابرداده و روش انتقال مشخص شده است، منابع را از ناشران می‌گیرد؛
- به‌منظور تضمین حفاظت طولانی‌مدت، کنترل کافی بر اطلاعات دریافت‌شده دارد؛
- براساس خط‌مشی‌های مستند تضمین می‌کند اطلاعات در برابر حوادث غیرمترقبه حفاظت می‌شود؛
- تضمین می‌کند اطلاعات حفاظت‌شده برای کتابخانه‌ها تحت شرایط مذاکره‌شده با ناشر، در دسترس است؛
- بخشی از یک شبکهٔ جامع و یکپارچه است و شبکه‌ای بودن امکانات بیشتری در اختیار آنها قرار می‌دهد (Greenstein & Marcum, 2000).

آژانس پروژه‌های تحقیقاتیِ پیشرفتهٔ دفاعی ایالات متحده[1] نیز در سال ۲۰۰۱، در برنامه‌ریزی برای نظام‌های قابل اطمینان، به قابلیت سنجش و به‌صرفه‌بودن اقتصادی آنها اشاره کرده است.

در سال ۲۰۰۲ گروه کتابخانه‌های پژوهشی (سی.آر.ال.)[2] با همکاری مرکز کتابخانه‌ای فهرست‌نویسی پیوسته[3] (او.سی.ال.سی) در آمریکا، با این هدف که آرشیوهای دیجیتال بتوانند منابع ملی-فرهنگی و پژوهشی را به‌صورت تضمینی و دائم حفاظت کنند،

1. The US Defense Advanced Research Projects Agency (DARPA)
2. Research Library Group (RLG)
3. Online Cataloging Library Center (OCLC)

چارچوبی از ویژگی ها و مسئولیت‌ها[1] را در این راستا تدوین کرد. این چارچوب از نظام اطلاعات آرشیوی باز[2] به‌عنوان ابزار برنامه‌ریزی حفاظت دیجیتال پیروی می‌کند و بر ویژگی‌های فناورانه و سازمانی تأکید دارد. براساس گزارش این گروه، آرشیو دیجیتالِ مطمئن آن است که هدفش فراهم‌کردن دسترسی بلندمدت و قابل اطمینان به منابع دیجیتالِی‌شده، تحت نظام مدیریتی برای جامعه‌ای مشخص در حال و آینده باشد. ویژگی‌های آرشیوهای دیجیتال مطمئن از این منظر عبارتند از:

- پیروی از مدل مرجع نظام اطلاعاتی آرشیوی باز؛
- پذیرش مسئولیت‌های اجرایی نظام؛[3]
- موفقیت سازمانی؛[4]
- دوام‌پذیری مالی؛[5]
- تناسب روش‌ها و فناوری‌ها؛
- امنیت نظام؛
- پاسخگوبودن[6] (RLG-OCLC, 2002).

در سال ۲۰۰۳ گروه کتابخانه‌های پژوهشی به‌طور مشترک با مدیریت آرشیوها و مدارک ملی[7] در آمریکا، گروهی را به‌منظور ارزیابی وضعیت آرشیوهای دیجیتال به‌وجود آورد. آنها با هدف ارزیابی قابلیت اطمینان در ذخیره‌سازی، توسعه، مبادله و فراهم‌کردن دسترسی به مجموعه‌های دیجیتال، معیارهایی را تدوین کردند. این معیارها برای ارزیابی آرشیوهای دیجیتال سازمانی، کتابخانه‌های ملی و نظایر آنها نیز به کار می‌رود

---

1. Trusted Digital Repositories (TDR): Attributes and Responsibilities
2. Open Archiving Information System (OAIS)
3. Administration responsibility
4. Organizational viability
5. Financial sustainability
6. Accountability
7. National Archive and Records Administration (NARA)

.(CRL[1] & OCLC, 2007)

«گلادنی»[2] (۲۰۰۶) «تی دی او» (شیءِ دیجیتال مطمئن)[3] را پیشنهاد داد که روشی است برای تضمین اصالت رکوردهای اشیای دیجیتال. وی برای رسیدن به این هدف، راه‌حل‌هایی را به شرح زیر پیشنهاد کرد:

- وجود فراهم‌آورندگانی که آثار را بسته‌بندی، ذخیره، جستجوپذیر و دسترس‌پذیر کنند؛
- وجود سازوکارهای تکثیر برای جلوگیری از زوال آخرین نسخه‌های موجود آثار؛
- وجود طرحی برای بسته‌بندی هر اثر، همراه با ابرداده‌هایی نظیر منشأ[4] هر اثر، پیوندهای مطمئن به آثار مشابه، هستی‌شناسی‌ها، نرم‌افزارهای تفسیر[5] و ...؛
- اختصاص ابرداده‌های کتاب‌شناختیِ استاندارد و هستی‌شناسی‌های خاصّ موضوعیِ تعریف‌شده و استانداردشده توسط افراد متخصص؛
- وجود طرح رمزگذاری رشته‌های بیتی[6] به‌منظور اینکه محتوا در هر ایستگاه رایانه‌ای قابل نمایش و خواندن باشد، نه صرفاً در رایانه‌ای خاص.

«او. سی. اِل. سی» (۲۰۰۶) چهار راهبرد برای حفاظت دیجیتال مطمئن تصویب کرده است:

- بررسی خطرهای از بین رفتنِ داده در اثر تغییرات فناوری، نظیر تحول در قالب‌های فایل و برنامه‌های کاربردی نرم‌افزاری؛
- بررسی اشیا با محتوای دیجیتال به‌منظور تعیین نوع و کیفیت تبدیل قالب فایل یا سایر کارهای حفاظتی؛

---

1. Center for Research Libraries
2. Gladney
3. TDO: Trustworthy Digital Object
4. Provenance
5. Rendering
6. Bit-string encoding

- تعیین ابرداده‌های مورد نیاز هر شیء و چگونگی اختصاص دادن آنها به این شیء؛
- فراهم‌کردن دسترسی به محتوا.

«استورر[1] و دیگران» (۲۰۰۷) نظام ذخیرهٔ بلندمدت، امن و قابل بازیابی به نام POTSHARDS را به‌وجود آوردند که دسترسی بلندمدت، امنیت و بازیابی رکوردها را تضمین می‌کرد. به‌عقیدهٔ آنان، سیستم امنیتی رمزگذاری[2] برای ذخیره‌سازی طولانی‌مدت داده‌ها مناسب نیست زیرا اگر کلید رمزپردازی به هر دلیلی از بین برود، خود داده نیز از بین خواهد رفت. بنابراین، در روش پیشنهادی آنها، هر شی به n سهم تبدیل می‌شود که هر کدام، در آرشیوهای جداگانه قرار می‌گیرد و برای بازیابی و بازسازی آنها از نشانگر تقریبی[3] استفاده می‌شود . این نشانگر روابط بین قطعات تقسیم‌شده در آرشیوها را مخفی نگه می‌دارد.

رسیدگی به زیرساخت‌های آرشیوسازی دیجیتال، با ایجاد مدل مرجع نظام اطلاعاتی آرشیوی باز[4] سازماندهی شد. این نظام اطلاعاتی آرشیوی متشکل از افراد و سیستم‌هایی است که مسئولیت حفاظت اطلاعات و دسترس‌پذیرکردن آن را برای جامعه‌ای معیّن در مدت‌زمان طولانی برعهده دارد (CCSDS, 2002). لازم به ذکر است، نظام اطلاعاتی آرشیوی باز را کمیتهٔ فنی بیستمِ کمیتهٔ مشاور نظام داده و فضا ـ که مربوط به وسایل فضایی و هواپیماست ـ وکمیتهٔ فرعی ۱۳ این کمیته ـ که مربوط به نظام‌های انتقالِ اطلاعات و داده‌های فضایی است ـ تدوین کرده است.

برنامهٔ ملیِ حفاظت دیجیتال و زیرساخت اطلاعات اِلکترونیکی ایالات متحده[5] نیز

---

1. Storer
2. Encryption
3. Approximate pointer
4. Open Archival Information System (OAIS): Reference Model
5. National Digital Information Infrastructure and Digital Preservation Program (NDIIPP)

از جمله تلاش‌های ملی در راستای حفاظت دیجیتال است. نظام‌های حفاظت دیجیتالِ دیگری نظیر نظام آرشیوسازی اطلاعات دیجیتال (دیاس)،[1] و نظام حفاظت رقمی لاکس[2] به‌وجود آمدند که همگی بر مبنای نظام اطلاعاتی آرشیوی باز هستند.

به‌علاوه، در بحث قابلیت اطمینان در آرشیوهای دیجیتال، سه مسئلهٔ «تضمین سندیت»[3] اطلاعات دیجیتال، جلب رضایت کاربر و تضمین قابلیت اطمینان فراهم آورندگان خدمات[4] مورد توجه است (RLG_OCLC, 2002).

در چند سال گذشته، سازمان‌های متعدد کوشش‌هایی را برای بهسازی معیارهای ارزیابی تدوین‌شده انجام داده‌اند و بازنگری و تجدیدنظرهایی در این معیارها شده است. برای نمونه، فرایند بازنگری در معیارهای اطمینان‌پذیری آرشیوهای دیجیتال گروه کتابخانه‌های پژوهشی که با همکاری مدیریت آرشیوها و مدارک ملی در ایالات متحده آمریکا ادامه یافت، منجر به ایجاد ابزاری به نام «وارسی و تأیید آرشیوهای مطمئن: سیاهه بازبینی معیارها (تراک)»[5] شد که برای اندازه‌گیری قابلیت اطمینان آرشیوها و مخازن دیجیتال به‌کار می‌رفت (CRL-OCLC, 2007). تجدیدنظر در این معیارهای ارزیابی همچنان ادامه یافت و این معیارها در سال ۲۰۱۰ ویرایش شد.

هستهٔ اصلیِ معیارهای اطمینان‌پذیری براساس معیارهای سه سازمان کارگروه نستر،[6] مرکز کتابخانه‌های پژوهشی و مرکز حفاظت دیجیتال بود که به این هسته اولیه استاندارد ایزو، کمیته فنی ۲۰ و کمیته فرعی ۱۳[7] نیز اضافه شد. بنابراین، سه سازمان

---

1. Digital Information Archiving System (DIAS)
2. Lockss Digital Preservation System
3. Authentication
4. Service Providers
5. Trustworthy Repositories Audit and Certification: Criteria Checklist (TRAC)
6. Nester Working Group The Digital Curation Centre (DCC)
7. ISO/TC20/SC13

نام‌برده از کار تجدیدنظر در معیارهای ارزیابی آرشیوهای دیجیتالِ حمایت کردند. قابلیت‌های هر مجموعه به کمک این ابزار، با معیارهای اصلی مقایسه و در نهایت، آرشیو در سطح بین‌المللی به رسمیت شناخته می‌شود (CRL-OCLC, 2007).

در سال ۲۰۱۲، ابزار «وارسی و تأیید آرشیوهای مطمئن: سیاهه بازبینی معیارها» به استاندارد ایزو ۱۶۳۶۳ تبدیل شد. براساس این سیاهه، در سال ۲۰۰۶ تا ۲۰۰۷ ابزار دیگری به‌نام «روش وارسی واسپارگاه دیجیتال مبتنی برارزیابی ریسک»[1] به‌وجود آمد که برعکس سیاههٔ وارسیِ قبلی، وسیله‌ای برای وارسی و شناسایی نقاط قوّت و ضعف به‌وسیله خود سازمان بود و مدیران حفاظت دیجیتال خطرها و ریسک‌ها را در شش مرحله به کمک آن شناسایی و مدیریت می‌کردند. این ابزار را مرکز حفاظت دیجیتال[2] و حفاظت دیجیتال اروپا[3] پدید آوردند (Mchugh, Ruusalepp & Hofman, 2007).

براساس استاندارد ایزو ۱۶۳۶۳، قابلیت اطمینان آرشیوها به سه سطح «زیرساخت سازمانی»، «مدیریت اشیای دیجیتال» و «زیرساخت فناوری» تقسیم می‌شود و هر سطح الزام‌هایی دارد. هریک از این الزام‌ها به تناسب دارای معیارهایی در باب محیط، مسئولیت‌های اجباری نظام، مدل عملکردی و اطلاعاتی، ساختار مفهومی اطلاعات و انواع بسته‌های اطلاعاتی است (جدول۱).

1. Digital Repository Audit Method Based on Risk Assessment
2. Digital Curation Center (DCC)
3. Digital Preservation Europe (DPE)

جدول۱. سطوح قابلیت اطمینان آرشیوهای دیجیتال و الزام‌های آن در استاندارد ایزو ۱۶۳۶۳

سطح	اِلزام‌های هر سطح
۱. زیرساخت سازمانی	شیوه اداره و دوام سازمانی[1]
	ساختار سازمانی و به کارگماری نیروی انسانی[2]
	چارچوب خط مشی و پاسخگویی درباره عملکرد[3]
	دوام‌پذیری مالی[4]
	قراردادها، اجازه‌نامه‌ها[5] و دیون[6]
۲. مدیریت اشیای دیجیتال	فراهم‌آوری محتوای دیجیتال (جذب)
	ایجاد بسته‌های آرشیوسازی (جذب)
	برنامه‌ریزی حفاظت
	ذخیره آرشیوی و حفاظت از بسته‌های اطلاعاتی آرشیوی
	مدیریت اطلاعات
	مدیریت دسترسی
۳. فناوری ها، زیرساخت فنی و امنیت	اِلزامات زیرساخت نظام
	فناوری‌های مناسب
	امنیت

بحث و نتیجه‌گیری

رسیدگی به زیرساخت‌های آرشیوسازی دیجیتال با ایجاد «مدل مرجع نظام اطلاعاتی آرشیوی باز» سازماندهی شد. بسیاری از آرشیوهای دیجیتال براساس این مدل به‌وجود آمدند و در آینده هم با این رویکرد پدید می‌آیند؛ ولی نکته‌ای که اهمیت دارد این است

1. organizational viability
2. staffing
3. Procedural accountability
4. Financial sustainability
5. licenses
6. liabilities

که به همان اندازه که به نظام حفاظت منابع دیجیتاِل نیاز است، داشتن برنامهٔ تأیید قابلیت اطمینان هم اهمیت دارد. این برنامه باید دربردارندهٔ معیارهایی برای ارزیابی و نیز سازوکارهایی برای سنجش باشد (RLG-OCLC, 2002). به‌هرحال، قابلیت اطمینان با تمرکز بر مرحلهٔ طراحی، سعی در ایجاد کیفیت از زمان طراحی تا زمان تولید و اجرا و تداوم آن دارد (عرب، ۱۳۷۷).

مطمئناً برای تضمین قابلیت اطمینان معیارهایی لازم است. از این میان، فرایند حسابرسی باید وجود داشته باشد و این فرایند کمّی توسط خود سازمان یا افرادی خارج از سازمان و به‌صورت دوره‌ای انجام شود. کمّی‌بودن بدین‌معناست که سطح اطمینان در هر نظام حفاظت دیجیتال مشخص شود. به‌عنوان مثال، «هاتی‌تراست»[1] واسپارگاهی برای حفاظت از محتوای دیجیتاِلی تولیدشدهٔ ۶۰ کتابخانهٔ پژوهشی در اروپا و ایاِلات متحده است. این واسپارگاه محتوای تولیدشده در پروژهٔ گوگل‌بوک[2] و طرح رقمی‌سازی آرشیو اینترنتی[3] را نیز حفاظت می‌کند. این واسپارگاه را دانشگاه‌های ایندیانا و میشیگان اداره می‌کنند. میزان اطمینان‌پذیری هاتی‌تراست را مرکز کتابخانه‌های پژوهشی در سال ۲۰۰۹ بررسی کرد. این واسپارگاه بر اساس گزارش‌ها، از پنج نمرهٔ حداکثری در سیاههٔ وارسی سی. آر. اِل، در زیرساخت سازمانی نمره۲ و در مدیریت اشیای دیجیتاِل نمرهٔ ۳ و در زیرساخت فناوری نمرهٔ ۴ را کسب کرد. فرایند بررسی تا سال ۲۰۱۱ به‌طول انجامید و اصلاحات لازم صورت گرفت و این واسپارگاه، در همین سال به‌عنوان واسپارگاه مطمئن شناخته شد (CRL, 2011).

آرشیو دیجیتال مطمئن باید دارای خط‌مشی‌هایی مستندشده و مورد توافق و همچنین دارای بیانیهٔ مأموریت واضحی باشد. بر اساس بررسی‌های انجام‌شده، معیارهای قابلیت اطمینان در آرشیوهای دیجیتال کم‌وبیش مشابه و بر اساس یک

---

1. Hathi Trust
2. Google Book
3. Internet Archive Digitalization Initiative

هستهٔ اولیه به‌وجود آمده‌اند و به‌مرور زمان کامل شده‌اند و به‌نظر می‌آید بتوان آنها را به سه دستهٔ کلّی تقسیم کرد:

۱.معیارهای مرتبط با کاربر

کاربران به دو دسته تقسیم می‌شوند: افراد دخیل در فرایند حفاظت دیجیتال در آرشیو و کاربران نهایی و استفاده‌کنندگان از نظام.

الف) استفاده‌کنندگان از نظام: جامعهٔ استفاده‌کننده از آرشیو باید تعریف‌شده و دسترسی به اطلاعات برای آنان تضمین شود. در حفاظت طولانی‌مدت، در صورتی رضایت کاربر جلب می‌شود که مطمئن شود نظام از فناوری‌های در حالِ توسعه برای حفاظت و دسترسی بلندمدت در طول زمان استفاده می‌کند. آرشیوها باید بتوانند تغییرات سند دیجیتال در نظام را نمایش دهند.کاربر باید بفهمد سندی که از نظام آرشیو دریافت می‌کند، همان است که درخواست کرده است؛ یا سندی که به دست کاربر رسیده همان است که به نظام واسپاری شده است. آنان باید مطمئن شوند اطلاعات فاقد خطاست و حقوق مرتبط با محرمانگی آنها در نظام رعایت می‌شود. ضمناً، استفاده‌کنندگان باید مطمئن شوند حقّ مؤلف و مالکیت فکری در نظام رعایت می‌شود. از طرف دیگر، استفاده‌کنندگان باید مسئولیت‌های خود در برابر آرشیو را هم بدانند و با استفاده‌های مجاز و خط‌مشی‌ها و انواع اجازه‌نامه و کمّ‌وکیف دخل و تصرف در اطلاعات آگاه باشند .

بدین‌منظور، سازمان‌های آرشیوی باید با فراهم‌آورندگان خدماتی کار کنند که قابلیت اطمینان آنها تأیید شده باشد. این فراهم‌آورندگان خدمات باید بتوانند با سازمان به‌نحو مطلوب توافق کنند. در صورتی‌که فراهم‌آورندگان خدمات کارهای خود را با دقت انجام دهند، سازمان هم تمایل به ادامهٔ کار با آنها خواهد داشت. بنابراین سازمان‌ها ابزاری برای سنجش خدمات خود دارند و فراهم‌آورندگان خدمات نیز از استانداردها و بهترین شیوه‌های شناخته‌شده استفاده می‌کنند. معمولا تدوین ابزارهای سنجش خدمات

آرشیو بر اساس نحوهٔ عملکرد آرشیوهایی است که جامعهٔ کاربران از آنها رضایت دارند (آر. اِل. جی.- او. سی. اِل. سی، ۲۰۰۲). از طرف دیگر، هر تولیدکنندهٔ کالا و خدمات می‌داند موفقیتش به رضایت مشتریانش از محصول و خدمات او بستگی دارد. اگر در فرایند طراحی، تولید و توسعه به جلب رضایت کاربر توجه نشود، کیفیت و قابلیت اطمینان ضعیف می‌شود (معین‌زاد، ۱۳۸۰)

ب) **افراد درگیر در فرایند حفاظت دیجیتال:** این افراد باید کاملاً آموزش‌دیده باشند و تعدادشان کافی و آموزش آنان مطابق تغییرات فناورانه، به‌روز باشد. آنان باید بتوانند اطلاعات را از تولیدکنندگان بگیرند، کیفیت اطلاعات را تأیید کنند، بسته‌های اطلاعاتی آرشیوی مطابق با قالب‌بندی داده و استانداردهای سندپردازی تولید کنند، اطلاعات توصیفی به بسته‌های اطلاعاتی تولیدشده به‌منظور قرار گرفتن در پایگاه‌های آرشیوی اختصاص دهند و در روزآمدسازی مدیریت داده و ذخیرهٔ آرشیوی، متخصص و ماهر باشند. آنان باید در بحث ذخیره‌سازی با انواع رسانه‌های ذخیره‌سازی و تبدیلات، بررسی خطاهای خاص و عام و بهسازی خرابی‌های آرشیوی آشنا باشند و بتوانند هم به اطلاعات توصیفی و هم داده‌های مدیریتی، امکان دسترسی ایجاد کنند. همچنین به اشیای دیجیتال، شناسگر اختصاص دهند و در تمام مدت نیازهای جامعهٔ آرشیو را مدّنظر قرار دهند و مدام با آنها در ارتباط باشند. در تمام این موارد، نقش و مسئولیت‌های افراد کاملاً باید مشخص باشد.

۲. معیارهای فناورانه

این معیارها از این وجوه باید بررسی شوند:

الف) اطلاعات: قالب ، ساختار و محتوای اطلاعات باید به‌منظور عرضه به جامعهٔ تعریف‌شده، مشخص باشد.کاربران باید بدانند به‌دنبال چه اطلاعاتی در آرشیو باشند و به‌طور مستند برای آنها مشخص شده باشد چه قالب‌های متنی، صوتی، تصویری و ویدیویی را می‌توان دریافت کرد. همچنین این اطلاعات باید برای جامعهٔ استفاده‌کننده

درک‌شدنی و قابل استفاده باشد؛ یعنی کاربر بتواند با ابزارهای موجود اطلاعات را دریافت و تفسیر کند. اطلاعات نیز باید به‌روز، کامل و خوانا و باورپذیر و به‌دور از خطا باشد. در این زمینه باید خط‌مشی‌های تعهدآور برای تضمین وجود داشته باشد. مدت‌زمانی هم که از این اطلاعات محافظت می‌شود، باید تعیین شود.

ب) **زیرساخت‌های اطلاعاتی:** این مورد شامل شبکه، نرم‌افزار و سخت‌افزار و استانداردهای محتوا و دسترسی و تضمین یکپارچگی اسناد، امنیت، راهبردهای حفاظتی و... است. آرشیو باید آمادگی برای حوادث داشته باشد، طرح‌های بهبود و بازسازی را به‌صورت مکتوب درآورد که شامل حداقل یک نسخه پشتیبان از همه اطلاعات حفاظت‌شده به انضمام یک نسخهٔ نگهداری‌شده خارج از محل اصلی باشد.

۳. معیارهای مبتنی بر وجه اقتصادی

موفقیت یک برنامهٔ حفاظت دیجیتال به بودجه‌بندی و صرفهٔ اقتصادی آن بستگی زیادی دارد زیرا در پیش‌بینی طرح‌های حفاظت دیجیتال در طول زمان نیاز به صرف هزینه‌های گزاف است؛ به‌عنوان مثال، هزینه‌های ذخیره‌سازی و تبدیل رسانه‌ای و قالب‌بندی مجدد. برنامه‌ریزی کوتاه‌مدت و درازمدت مالی به‌منظور اینکه آرشیو در طول زمان دوام بیاورد و پویا بماند لازم است. طرح و برنامه‌های مالی را حداقل سالیانه باید بازبینی کرد. هزینه‌ها و درآمدها هم باید تعادل داشته باشند تا حفاظت دیجیتال از نظر مالی مقرون به صرفه باشد.

در مجموع، قابلیت اطمینان در متون مربوط به علم اطلاع‌رسانی در مورد منابع چاپی وجود داشته و با دیجیتالی‌شدن منابع به حوزهٔ حفاظت دیجیتال، آرشیوها و کتابخانه‌های دیجیتال توسعه پیدا کرده و به‌نظر می‌رسد در آینده به سمت کتابداری موبایلی حرکت کند. به‌هرحال، معیارهای بررسی‌شده در اینجا می‌تواند بالقوه در ساختن ابزاری همه‌جانبه برای وارسی اطمینان‌پذیری آرشیوهای دیجیتال سودمند باشد.

منابع

- پارکر، سیبل .پی (۱۳۷۲). *فرهنگ تشریحی علوم مهندسی مک‌گروهیل*، تهران: دانشیار.
- سلیمانی، مسعود (۱۳۷۵). *واژه‌نامهٔ مدیریت کیفیت*: شامل واژه‌ها و اصطلاحات کیفیت. تهران: مؤسسهٔ مطالعات سازمان گسترش و نوسازی ایران.
- عرب، نجم‌الدین (۱۳۷۷). «مقدمه‌ای بر قابلیت اطمینان و ارزیابی استانداردهای مختلف»، *نشریه صنعت برق*، دوره۳، ش۲۳و۲۴، ۶-۱۱.
- معین‌زاد، حسین (۱۳۸۰). «مدیریت قابلیت اطمینان»، *پیام مدیریت موفق*، ش۱۶.

- Alhaqbani, B., & Fidge, C. (2009, December).A time-variant medical data trustworthiness assessment model.In *Proceedings of the 11th international conference on e-Health networking, applications and services* (pp. 130-137). IEEE Press.
- Amoroso, E., Taylor, C., Watson, J., & Weiss, J. (1994).A process-oriented methodology for assessing and improving software trustworthiness.In *Proceedings of the 2nd ACM Conference on Computer and communications security* (pp. 39-50).ACM.
- Blumenthal, M. S. (1999). The politics and policies of enhancing trustworthiness for information systems.*Communication Law and Policy*, *4*(4), 513-555.
- Cassell, J., & Bickmore, T. (2000).External manifestations of trustworthiness in the interface.*Communications of the ACM*, *43*(12), 50-56.
- The Center for Research Libraries(CRL) &OCLC (2007). *Trustworthy Repositories Audit & Certification: Criteria and Checklist*. Chicago, Illinois, Retrieved octobr, 10, 2015 from http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf
- Center for research Libraries(2011).Certification Report on the HathiTrust Digital Repository Retrieved 7, December 2015, from http://www.crl.edu/sites/default/files/attachments/pages/CRL%20HathiTrust%20 2011_final.pdf
- Consultative Committee for Space Data Systems (CCSDS) (2002). Reference Model for an Open Archival Information System (OAIS), Washington, DC,Retrieved October, 10, 2015 from http://public.ccsds.org/publications/archive/650x0b1.pdf
- Cooper, Brian; Crespo, Arturo; Garcia-Molina, Hector (2000).Implementing a Reliable Digital ObjectArchive.*Proceedings of the Fourth European Conference on Research and Development in DigitalLibraries (ECDL)* Retrieved September,11, 2015 From dbpubs.stanford.edu/pub/2000-28.
- Cooper, Brian; Garcia-Molina, Hector (2001).Creating trading networks of digital archives.*1st ACM/IEEEjoint Conference on Digital Libraries.*Retrieved December, 14, 2015 from dbpubs.stanford.edu/pub/2001-23.
- Defense Advanced Research Projects Agency (DARPA) (2001). *Composable High Assurance*
- *Trusted Systems, CBD Reference* Retrieved September, 11, 2015 from www.darpa.mil/ito/Solicitations/CBD_01-24.html.

- Digital Curation Centre &DigitalPreservationEurop (, "*DCC and DPE Digital Repository Audit Method Based on Risk Assessment,* v1.0". Retrieved October, 10, 2015 From http://www.repositoryaudit.eu/
- Digital Library Federation (2000).*Minimum Criteria for an Archival Repository of Digital*. Retrieved September, 11, 2015 from *old.diglib.org/preserve/criteria.htm*
- Donaldson, D. R., & Conway, P. (2015). User conceptions of trustworthiness for digital archival documents.*Journal of the Association for Information Science and Technology*.
- Duranti, L. (1995). Reliability and authenticity: The concepts and their implications. Archivaria, 39, 5–10.
- Gladney, H. M. (2006). Principles for digital preservation.*Communications of the ACM*, *49*(2), 111-116. Retrieved November, 11, 2015 from http://americanarchivist.org/doi/pdf/10.17723/aarc.72.2.g513766100731832
- Greenstein, D., & Marcum, D. (2000).Minimum criteria for an archival repository of digital scholarly journals.*Version*, 1, 15.
- Hedstrom, Margaret(1998).Building Recordkeeping Systems: Archivists are Not Alone on the Wild Frontier.*Archivaria*: pages 44-71.
- Jøsang, A.; Knapskog, S.J. (1998).*A Metric for Trusted Systems* .Retrieved September, 7, 2015 from citeseer.nj.nec.com/ 129647.html.
- Kahle, Brewster (1996). Preserving the internet. Retrieved September, 7, 2015 from www.sciamdigital.com/gsp_qpdf.cfm?ISSUEID_CHAR...
- Kelton, K., Fleischmann, K.R., & Wallace, W.A. (2008). Trust in digital information. Journal of the American Society for Information Science and Technology, 59(3), 363–374
- Kim, J., & Moon, J. Y. (1998). Designing towards emotional usability in customer interfaces—trustworthiness of cyber-banking system interfaces. *Interacting with computers*, *10*(1), 1-29.
- Kirchhoff, Amy etAl *(2010).Becoming a certified trustworthy digital repository: the portico experience.*Retrieved 7, December , 2015 fromhttp://www.ifs.tuwien.ac.at/dp/ipres2010/papers/Kirchhoff-35.pdf
- MCHUGH, M. A., RUUSALEPP, M. R., & HOFMAN, M. H. (2007).Digital Repository Audit Method Based on Risk Assessment (DRAMBORA).
- MacNeil, H. (2000). Trusting records: Legal, historical and diplomatic perspectives. Dordrecht, London: Kluwer Academic
- National Computer Security Center (NCSC) *(1988). A Guide to Understanding Audit in Trusted Systems* .Retrieved September, 15, 2015 from www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-001-2.html.
- National Computer Security Center(1992) *Guidelines for Writing Trusted Facility Manuals, NCSC-TG-016,* Yellow-Green Book Retrieved September, 15, 2015 fromwww.fas.org/irp/nsa/rainbow/tg016.htm
- Nestor Working Group (2006). Catalogue of Criteria for Trusted Digital Repositories, Version 1. Retrieved September, 15, 2015 from edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf
- Noble, Thomas FX (1990).Literacy and the papal government in late antiquity and the early middle ages.*The uses of literacy in early mediaeval Europe*, 82-

108.
- Online Computer Library Center, Inc. (2006). OCLC Digital Archive Preservation Policyand supporting Documentation, p-5 7. September, 15, 2015from http://archive.ifla.org/IV/ifla63/63kuny1.pdf 8.http://en.wikipedia.org/wiki/Digital_preservation 9. http://www.uky.edu/-kieran/DL/hedstrom.html
- Portz, K. S. (2000). The effect of webtrust on the perceived trustworthiness of a web site and the utilization of electronic commerce.
- RLG-OCLC (2002). Trusted Digital Repositories: Attributes and Responsibilities(TDR). Retrieved September, 15, 2015 from www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf
- RLG-OCLC (2003).Audit checklist for certifying digital repositories Retrieved September, 15, 2015 from www.edtechpost.ca/.../rlg-nara-audit-checklist-for-certifying-digital-.
- RLG-OCLC. (2002). Trusted Digital Repositories: Attributes and Responsibilities.Retrieved September, 15, 2015 fromhttp://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf
- Stefik, Mark (1997). Trusted Systems.*Scientific American.*Retrieved September, 7, 2011 from www.sciam.com/0397issue/0397stefik.html
- Stefik, Mark (1997). Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge us toRethink Digital Publishing. *Berkeley Technology Law Journal* 12, no.1 Retrieved September, 11, 2015 fromwww.law.berkeley.edu/journals/btlj/articles/12_1/Stefik/html/text.html.
- Schmidt, Lisa M. (2009).Preserving the H-Net Academic Electronic Mail Lists. Retrieved 7, December , 2015 from http://www2.archivists.org/sites/all/files/Case11Final.pdf
- Steinhart, Gail; Dietrich, Dianne; Green, Ann (2007). Establishing Trust in a Chain of Preservation: The TRAC Checklist Applied to a Data Staging Repository (DataStaR). D-lib Magazine. Vol.15, no, 9-10.
- Storer, M. W., Greenan, K. M., Miller, E. L., & Voruganti, K. (2007, February). Secure archival storage with potshards. In *FAST'07: Proceedings of the 5th conference on USENIX Conference on File and Storage Technologies* (pp. 11-11).
- Van Mulken, S., André, E., & Müller, J. (1999).An empirical study on the trustworthiness of life-like interface agents. In *HCI (2)* (pp. 152-156).
- Yang, X., Qiu, Q., Yu, S., & Tahir, H. (2014).Designing a trust evaluation model for open-knowledge communities.*British Journal of Educational Technology*, *45*(5), 880-901.