

Investigating Trusted Records for Employment and Education

Rayan M. Ghamri^a, Nawfal F. Fadhel^b and Gary B. Wills^c

School of Electronics and Computer Science, University of Southampton, U.K.

Keywords: Trusted Records, Education, Verifying Records, Employment, Framework, Records Sharing.

Abstract: Employment uses trusted records such as award certificates as a part of hiring procedures. Some countries practices for employment history reference; either a service certificate or systems based on pension records which are based on number of years of employment that are also can be used for pension eligibility. However, there is an increase on the number of issued award certificates which are, in most cases, do not follow an agreed standard, which increases challenges for an authenticated record sharing. Moreover, employment systems are not required to share employment history nor to accommodate record requests educational institutes. Additionally, public employment systems are by design isolated from interaction with private sector. The research suggest that distributed systems would reduce costs for verifying and authenticating records while being flexible on allocating trusted records such as employment history, awarded certificates and resumes.

1 INTRODUCTION

The general practice, to verify an awarded certificate, candidates are required to provide their official documents to validate any claim on their personal resume. Also, employees must get some type of certificate to verify the length of the job with job duties and experienced gained. This means any employment experience outside the organisation is hardly recognised. Which consequently makes it difficult for individuals to build a resume without a proper managed employment history. At the same-time employers can not verify any job seeker claims. The existing practice to verify employment record requires different departments to manually and physically provide references. Such records are either: (1) authenticated records issued through official organisations or agencies, or (2) non-authenticated records that are provided by individuals who are responsible for the accuracy of records such as resumes. Unfortunately, some individuals provide inaccurate information which create a burden on hiring companies to verify the provided information.

The challenge presented here is how to improve information sharing between education and employment. To understand the research problem this research investigated published work relevant to

problems that can be solved or improved by using technological factors. The research also presented several attempt by (Andrews, 2011; Atzori, 2017, 2018; Lemieux, 2016, 2017; Otte et al., 2017; Wang et al., 2018) to address the trusted records issue using distributed systems. The technological factors, are either related to e-government since the main stakeholder is the government sector; Or related to information security and sharing. These factors are measurable and are applicable using distributed systems for information sharing verifying records.

Finally this paper grouped similar themed factors and proposed a framework for Trusted records for employment and education.

2 BACKGROUND

Award certificates are important documents in education and professional development, and are essential for career development. And, due to their importance, these records are, or at least should be stored in long-lasting tamper-proof ledgers. This paper focuses on Award certificates for qualifications and academic titles that can be confirmed by a traceable issuer to validate whether or not the qualifications are true. Usual paper certificates are difficult to fake due to the built-in security features which provide the person holding the certificates (usually) with full control over them. Grech and Camilleri (2017) explored the

^a <https://orcid.org/0000-0002-4215-779X>

^b <https://orcid.org/0000-0002-1129-5217>

^c <https://orcid.org/0000-0001-5771-4088>

notion that certificates could be store and shared with whomever authorised them. However, paper certificates have some disadvantages. Problems include:

- Single point of failure, e.g. the certificate is valid but cannot be verified.
- Register keeping requires a manual process which uses human resources.
- Producing a paper certificate costs around €20, while a highly-secure certificate costs €150.
- Once the certificate has been issued, there is no way to revoke it.
- There is a need for the involvement of third parties to manually and individually verify resumé claims, which is a time consuming process.

When it comes to digitised award certificates in public and private schools systems, they have a sharing procedure. However, when it comes to employment history in public sector and private sector, there are limited to their own sector and is not shared between companies or institutions. Therefore, we can conclude that the **research problem statement** in trusted records is:

Employment sectors and educational institutes does not share information between organisations outside their own sector and Public sector only gets their information stored in government systems . There are also social factors that are unique to each culture when it comes to introducing new technologies related to e-government.

2.1 Issues

This paper addresses the finding from the literature reviews in a from of issues and their categories as show in table 1. Factors were categorised in their relevance to their findings through adoption and acceptance models. However, Acceptance and Adoption models do not cover sharing record, therefore a trusted system for records sharing was introduced. The issue categories are defines as follows.

Facilitating Issues. These issues were the social issues that are related to technical and organisational boundaries which must be addressed to implement a system. Issues such as, financial barriers which can be understood as if the organisation is not willing to spend money, there will not be any system for records sharing. Commitment is another issue coming from the management taking responsibility on suspending an implementation. Cooperation and collaboration is another issues especially in the public sector which start

Table 1: Categories of the Issues.

Category	Issues
Facilitating	Financial Barriers Issues [1, 2, 3, 4, 5, 6]
	Top Management Commitment Issues [3,4,7,8]
	Cooperation and Collaboration Issues [7,10]
	Outdated Infrastructure Issues [3,4,9]
	Training and Experience Issues [3,4,10]
	Job assignments Issues [4,5,6]
Implementation	Security Issues [1,2,8,11,12]
	Reliability Issues [11,13,14]
	Scalability Issues [1,2,15]
	Usability Issues [9,10]
	Flexibility Issues [4,7,8,9,10,16,17]
	Storage Issues [1,9]
Trust	Trust Issues [1,4,7,11,12,14]
	Privacy Issues [1,11,12,13,18]
	Operation Conditions Issues [19]
	Unverified Information Issues [1,13,18,19]
	Centralisation Issues [1,11,12,18,19]
	Changeable Information Issues [7,18]
Security	Confidentiality Issues [20]
	Authenticity Issues [13,14,20]
	Data Availability Issues [1,13,20]
	Encryption Issues [9,13,20]
	Integrity Issues [14,20]

[1] Wang et al. (2018) [2] Angraal et al. (2017) [3] Alassim et al. (2017) [4] Alfarraj et al. (2013) [5] Assad (2002) [6] Assad (2000) [7] Ølnes et al. (2017) [8] Ahram et al. (2017) [9] Ølnes (2016) [10] Ølnes and Jansen (2017) [11] Wang et al. (2017) [12] Atzori (2017) [13] Alketbi et al. (2018) [14] Lemieux (2016) [15] Biswas and Muthukkumarasamy (2017) [16] Wang et al. (2016) [17] Woodside et al. (2017) [18] Rizal Batubara et al. (2018) [19] Andrian et al. (2019) [20] Fadhel et al. (2014).

from the financial department throughout employee up to the management, it requires many departments. Outdated infrastructures which can be a major issues in implementing new systems. Untrained employees with limited computational skills, could be an issue for not having the right skills to practice implementing new systems. Job assignment could be an issue for hiring the wrong person at the wrong positions while not addressing all the job requirement.

Implementation Issues. These issues are major concern for system administrators to implement any new system. Their concerns can be examined in a form of questions that raise issues which needs to be addressed before implementing any new system. The admin requires new systems to be capable of being secure, reliable, scalable, usable, flexible and can be stored without many challenges.

Trust Issues. Trust is another major issue, the proposed framework limits the trust into to trust in the new system that can handle information sharing. Privacy would be an issue because the proposed system suggests sharing private information. Operation conditions is an issues, for example, while

executing an operation, it might be wrong or altered, a need for a mechanism to validate operation is required. Unverified information is another issue, finding how can a system verify the information through algorithm is something that must be looked at. Centralised structure means single ownership and single one point of failure. not resistance to change is another issue because once, adding traceability to assure immutability is a must.

Security Issues. Confidentiality, authenticity, availability, integrity and encryption are issues related to security practices.

3 TRUSTED RECORDS

Trust can has different meanings and definitions, however, this research will focus on trust in computer science. This paper examined trusted records from three perspectives.

3.1 Information Security Prospective

Security is essential in records sharing. However, there is no clear understanding between security clearance levels (Top Secret, Secret, Private and Public) and the meta data that needs to be share about the records themselves. Fadhel et al. (2014), authors discussed the importance of security and how record provenance is an essential part for protecting records. Authors related general computer security principles to conventional archival records. These security principles are information security, information authenticity and information exchange (McCONNELL, 1994).

In conclusion, these principles and their components presents a holistic approach to information security. Any claim of trust can be challenged using these components which will be used in validating this research into trusted records.

3.2 Information Sharing Prospective

A technology-based system focused on record keeping in a permanent way with authenticated fingerprints of certificates and other educational records should be presented to support learning history. An educational system that has implemented a record sharing is a great use case which will illustrate issuing, validating and sharing certificates. In this paper we have reviewed a number of these studies as shown in Table 1.

Based on the literature review and 1, it was clearly shown that the distributed ledger is presenting itself as a technological solution to trusting records. It also shows the importance of this technology in protecting award certificates from being forged and maintaining verification procedures even without the certificate issuer because of the decentralised nature of distributed ledgers Gräther et al. (2018).

Distributed Ledgers and Blockchain usage is no longer limited to financial aspects, and can now be found in many types of applications. This logic has emerged because all systems need technology to ensure safety and to provide integrity (Andrian et al., 2019). Another paper by, Lemieux (2016), explored the values of blockchain technology as a solution to create and protect trustworthy digital records. The analysis of the results of said study implied that blockchain can be used to amend security issues that are related to integrity, while it also guarantees the reliability of the information because it validates transitions.

3.3 HR Management Prospective

The authenticity of human resource information is an important factor which affects the cost and efficiency of human resource management. The risk is produced by “information asymmetry”; in other words, information failure. (Wang et al., 2017) suggested that the solution be built on combining encryptions technologies with internet distributed technology to establish a model for human resource management that would increase the authenticity of human resource information to solve discrimination and provide authentic and effective decision support information to the human resource management of an organisation. According to (Wang et al., 2017) Past papers have suggested a distributed ledger technology to record human resource information in an accounting book. Pat papers have also underlined the importance of combining information technology with the human resource management concept. In addition, these papers demonstrated the importance the authenticity of human resource information by illustrating a survey which shows that over 70% of job applicants hide details or present fraudulent inaccurate information during the hiring process, while explicitly mentioned that this can be achieved through a fake resumé, fake diplomas, fake certificates of qualifications and other exaggerations of their capabilities. However, this study mentioned that there will be personal data that will be involved and shared, but nothing on privacy and how to solve it.

4 RESEARCH METHOD

A qualitative and quantitative mixed methodology was used to achieve the research objectives (Johnson and Onwuegbuzie, 2004). More specifically, this study employed the triangulation research technique to achieve its goals (Carugi, 2016). The triangulation research technique helps to paint and visualise the research topics while validating and confirming the results. This research employs three methods in total: literature review, expert reviews and surveys. The below figure explains the techniques.

In order to confirm the framework, the next step will focus on the triangulation technique methods, namely literature review, expert reviews and surveys. The first step is to interview experts and request feedback on the proposed framework; once this has been completed, the next step will be to build questionnaires and distribute them. The results and findings will be analysed and, according to the framework, will be verified or updated. The role of the experts is to confirm the framework and provide feedback, derived from their experience in the field, on which relevant factors should be added, updated and modified.

In engineering and science, there are important values to consider while conducting a research (Shaw, 2002). Values are: Define interesting questions related to the field and topics. What could be the answers that could help to find the anticipated results, while thinking about what research methods would produce the anticipated results. How can demonstrate valid results by giving the right evidence and, also how to distinguish good results from bad results. In conclusion, based on research that was done on ICSE 2002 which was based on the submitted abstracts. Questions were focused on methods through development and analysis, then results that were found through a procedure or analytical model, then finally verified through examples, experience research (Shaw, 2002). For this research, there will be interview with questions given to the experts to provide a review, then the results will help to improve the framework, which will be later validated through surveys and testing a designed software.

Using the proposed framework would help information sharing and trust through a verified record. The proposed framework would reduce the amount of time needed to verify provided information; indeed, this would result in a decrease in the redundant processing of information. Any provided information shall be used for verification only. Verifications would occur through the framework and trust system, without the need to store any irrelevant personal information on unnecessary systems.

5 FRAMEWORK

The overall objective of this paper is to address the research problem represented in section 2. Trying to solve this research problem will lead to supporting unemployed individuals in record keeping their qualifications and empower them in finding employment. This research may have impact on other areas. However, this paper focuses on trusted Records for employment and education. The proposed framework is about records sharing and not records keeping. The proposed framework provides organisation the means to integrate it into existing systems. The records are already stored and managed by the government and this backend system is related to information management.

Developing a new framework for sharing trusted records will aid the Ministry of Education internal and external communications between educational institutes and employment organisations; Communications that would contain trusted records such as degrees, qualifications, credentials, diplomas, course records, transcripts, recommendations, equivalency diplomas and alike. Also, the framework will enable trust chains that assures information is coming from a government-trusted authenticated origin and that the information has the proper authenticity, custody and integrity, which would enhance trust. This means, any verifier will become a part of the trust chain. Adding an extra layer of assurance using the trust chain concept would help to improve citizens' digital information through e-government services and non-government services. Moreover, it would help to preserve privacy by providing personal information only after permission has been granted.

Implementing the suggested framework would only share information between the stakeholder listed in section 5. Also, the proposed framework is designed to assist in the examination Facilitating Conditions, Implementing Conditions, Trusted Chain Authentication and Security Principles (FITS) which affect the investigation for the factors of authenticated records sharing.

5.1 Framework Factor: Facilitating Conditions

This factor can be explained as the components that are needed to be presented to enable the use of the proposed trusted system. These components can be organisational and technical infrastructures which needs to be available.

Financial Barriers. At organisational level, top management must be willing to spend money

to invest in records sharing. Providing benefits would help favouring a decision of implementing. It is a significant barrier for having it has three obstacles; limited spending on ICT, expensive cost of running ICT and high cost from service telecommunication providers (Wang et al., 2018; Angraal et al., 2017; Alassim et al., 2017; Alfarraj et al., 2013; Assad, 2002, 2000).

Top Management Commitment. Top management plays an important part by taking responsibility on accelerating or suspending an implementation (Ølnes et al., 2017; Ahram et al., 2017; Alassim et al., 2017; Alfarraj et al., 2013).

Cooperation and Collaboration. This is a major issue with public sector, to successfully implement the suggested system, there would be a need of cooperation and collaboration from many departments such as; cooperation and collaboration between the ministries and government sectors, cooperation of financial department for funding, cooperation with researchers to find related issues to implementation and cooperation of top management (Alassim et al., 2017; Alfarraj et al., 2013; Alfarraj and Alhussain, 2013).

Outdated Infrastructure. There are limitation related to the outdated infrastructure, this be shown as a legacy system which could be outdated computer systems. This is a part hardware and another part is the software. Updated infrastructure enables the government agencies in accelerating daily tasks by using the technology to save time and effort (Ølnes, 2016; Alassim et al., 2017; Alfarraj et al., 2013).

Learning to Build Skills. One part is the ability of employees to learn to build new skills. Another part is the employers if they are willing to fund learning and development for their employees (Alassim et al., 2017; Alfarraj et al., 2013; Ølnes and Jansen, 2017).

Job Assignments. Employees assessment should be practiced during hiring with assigning employees with the right background and training to be in line with the job assignments (Alfarraj et al., 2013; Assad, 2002, 2000).

5.2 Framework Factor: Implementing Conditions

These are components that are related to the system administrators and IT department. They are components in a form of questions.

Security: is the new system secure? is there any added value? how can you confirm the system

is more secure than the current practice? (Wang et al., 2018, 2017; Atzori, 2017; Ahram et al., 2017; Angraal et al., 2017).

Reliability: the information is reliable because creating records comes from only authorised personal which in most cases are the organisation who issued the information. This means opening the verification process of records to everyone who has authorisation. In other words, there is no independent isolated verification to complete a record. Moreover, records must be relatively safe and are able to prevent human subjective and artificial records modification. Reliability will answer these questions: Can the user depend on the system achieve its tasks? Can it function under given conditions while maintaining accurate records? (Wang et al., 2017; Alketbi et al., 2018; Lemieux, 2016)

Scalability: can the new system function quick enough not to have scalability issues that slows the system? (Wang et al., 2018; Biswas and Muthukkumarasamy, 2017; Angraal et al., 2017).

Usability: is the system user friendly? can it be used with different software and hardware? can the new system achieve its objectives? (Ølnes, 2016; Ølnes and Jansen, 2017).

Flexibility: is the new system flexible enough to be implemented with the current infrastructure without many software and hardware changes? is it flexible enough to work with different operating systems and different users? Ahram et al. (2017); Ølnes (2016); Ølnes et al. (2017); Ølnes and Jansen (2017); Wang et al. (2016); Woodside et al. (2017); Alfarraj et al. (2013).

Storage: where would the shared records stored? where would be the physical related hardware stored? Wang et al. (2018).

5.3 Framework Factor: Trusted Chain Authentication

It is a necessary requirement for a system containing records to provide secure records that are trustworthy. This type of citizens record is often required to be recorded for long periods that might extend beyond the life span of a database system or a server. Records should be exchanged in a trusted, secure system. Based on Blockchain, for having an ongoing chain of authorised agreements starting from the issuer of the record. It contains algorithms to confirm the validity and authenticity of information It for a trustworthy system.

Trust. Having a trust in an organisation to handle personal information. Also, an organisation to have trust in a new system to store and practice sharing records (Wang et al., 2018; Ølnes, 2016; Lemieux, 2016; Atzori, 2017; Ølnes et al., 2017; Wang et al., 2017; Alfarraj et al., 2013).

Privacy: Blockchain has features of decentralisation and encryption while being resistant to change or modification. It strength privacy by allowing citizens to have control over their information to be shown for public access (for employment or sharing records) or private for government records (Wang et al., 2017, 2018; Rizal Batubara et al., 2018; Atzori, 2017; Alketbi et al., 2018).

Smart Contract. Smart contract is a code to perform an algorithm attached at the condition of an operation. This code is stored on the blockchain and it becomes active when it is about to execute an operation. It can be used in education and employment to validate a record and to authorise an update of a record (Andrian et al., 2019).

Consensus Mechanism. An ongoing algorithm that is aimed to verify information starting from the organisation that issues the record. It tools to ensure the records are valid and confirmand. These kinds of records will provide data consistency, fraud protection, information ownership, and immutable records. To achieve this, records should be securely sealed and recorded in the system; any proof of tampered data should be discarded or rejected (Wang et al., 2018; Rizal Batubara et al., 2018; Alketbi et al., 2018; Andrian et al., 2019).

Decentralisation. A decentralised structure will allow for historical/related record sharing in a secure environment in different organisations. There is no central ownership of the records, although information is validated by an authority. Once a record has been verified, it is stored (Wang et al., 2017, 2018; Rizal Batubara et al., 2018; Atzori, 2017; Andrian et al., 2019).

Immutability. Once the information is recorded, it will stay the same and should not change and should be traceable. Information can be changed, updated, and modified, but never deleted between ministries. Even if a system mentions that a record is not valid, has expired or is hidden, that record is always stored (Ølnes et al., 2017; Rizal Batubara et al., 2018).

5.4 Framework Factor: Security Principles

For this paper, there are three main components of security principle practices. Information Security, Information Authenticity and Information Exchange. Which are needed to be practiced and implemented assure a secure environment for sharing records of citizens. Information Security requires the CIA model which are, Confidentiality, Integrity and Availability. Information Authenticity requires Authentication, integrity and non-repudiation. Information Exchange requires Authentication, Authorisation and Accounting. Some components were mentioned under different factors, and some could be inherited and achieved by different factors. The following components were not addressed by any of the previous factors in the suggested framework.

Authenticity. Authenticity as a security principle is a different practice than having it for trust authentication. In this context, it means validating both parties which are the sender and receiver of the information. Also, verifying claimed identity to ensure communication and information are genuine (Alketbi et al., 2018; Lemieux, 2016; Fadhel et al., 2014).

Confidentiality. A property that only allows approved entities, parties or processes to receive information (Fadhel et al., 2014).

Cryptography and Digital Signatures: The digital cryptographic signature is used to demonstrate the authenticity of the information which use public-private key pairs. In a digital signature, the recipient encrypts the hash of the message using their private key, which can be sent along with the message to the receiver. The recipient also produces the original message's hash value, and authenticity can be checked against the hash value generated by decrypting the hash values sent by the sender using their public key (Ølnes, 2016; Alketbi et al., 2018; Fadhel et al., 2014).

Data Availability. The authenticated records should be available at all times whenever needed. A system that stores records or transactions in different systems would mean a reduction in single points of failure (Wang et al., 2018; Alketbi et al., 2018; Fadhel et al., 2014).

Integrity: Authenticated records are stored in a sequential order in the form of a trust chain. Said chain includes all of the previous hashed stored transactions that led to the verified record. This helps to verify and track long-term digital transactions (Lemieux, 2016; Fadhel et al., 2014).

5.5 Framework Architecture

A Trust System for Records Sharing is a backend system that provide security, privacy, integrity and confidentiality of the shared information between different organisations. The system task is to share records and some limitation on storing information. Government agencies are the main participants with all the required information, any organisation own the date, will grant access on the data within the trusted system. The system allows the sharing of information between relevant organisations to employment and education. There will be users of the system, however there will be some protocols and algorithms on handling informant. Users would be individuals, employers, training institutes, academic institutes and human resources.

The protocol will provide different types of users with different types of permissions from administrators to view only users. (see Figure 1) illustrates The Architecture for the Framework.

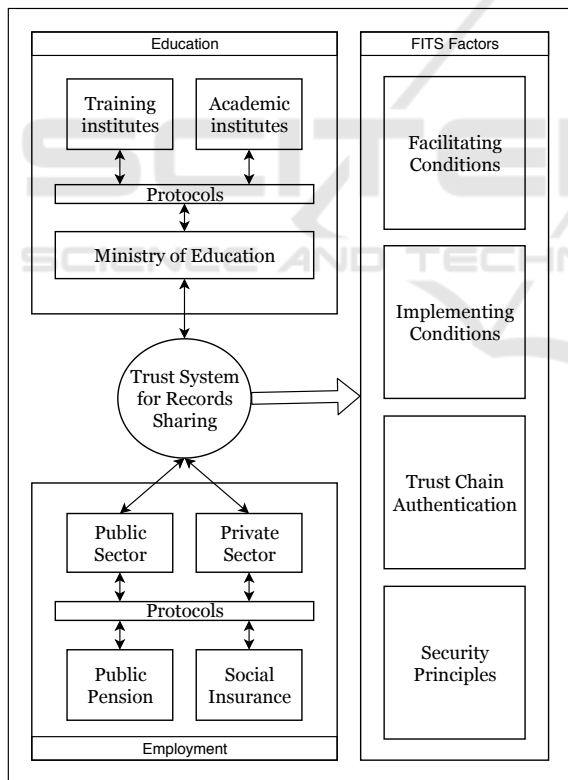


Figure 1: Architecture of Trust System for Records Sharing.

6 CONCLUSIONS

This paper is encouraged by the gap for authenticated records sharing between education and employment organisations.

There are many studies to show the capabilities of blockchain as a distributed ledger, however, there are not many that are applied into the e-government to support the government in records sharing for educational and employment organisations. Most studies suggest a further investigation on this technology because it is proven its capabilities in financial sector. There are some government agencies are using blockchain however it is more as identity management or traceability.

Introducing blockchain as an add on, back-end system to record information related to employment and education, it would strength e-government and assist the countries development vision. In other words, the use of blockchain into the public and private sectors would mean using only the blockchain capabilities that can be customised to be implemented anywhere that needs records sharing.

REFERENCES

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., and Amaba, B. (2017). Blockchain technology innovations. *2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017*, (2016):137–141.

Alassim, M., Alfayad, M., and Abbott-Halpin, E. (2017). Understanding factors influencing e-government implementation in Saudi Arabia from an organizational perspective. *International Journal of Information and Communication Engineering*, 11(7).

Alfarraj, O. and Alhussain, T. (2013). Making Sense of E-Government development in Saudi Arabia: A Qualitative Investigation. (1):59–71.

Alfarraj, O., Alhussain, T., and Abugabah, A. (2013). Understanding the factors influencing the development of eGovernment in Saudi Arabia: The use of grounded theory techniques. *International Journal of Information and Education Technology*, pages 319–324.

Alketbi, A., Nasir, Q., and Talib, M. A. (2018). Blockchain for government services-Use cases, security benefits and challenges. *2018 15th Learning and Technology Conference, L and T 2018*, pages 112–119.

Andrews, D. A. F. J. M. M. A. D. (2011). Trust and Trusted Computing Platforms. *Computer Science Journal*, Volume 1(Issue 2).

Andrian, H. R., Kurniawan, N. B., and Suhardi (2019). Blockchain Technology and Implementation : A Systematic Literature Review. *2018 International Conference on Information Technology Systems and Innovation, ICITSI 2018 - Proceedings*, pages 370–374.

- Angraal, S., Krumholz, H. M., and Schulz, W. L. (2017). Blockchain technology: Applications in health care. *Circulation: Cardiovascular Quality and Outcomes*, 10(9):1–3.
- Assad, S. (2000). Recruitment Criteria and Training in Human Resources Development: A Case Study of Women Office Workers at an Institution of Higher Education in Saudi Arabia. *Journal of King Abdulaziz University-Economics and Administration*, 14(2):13–29.
- Assad, S. W. (2002). Sociological analysis of the administrative system in Saudi Arabia: In search of a culturally compatible model for reform. *International Journal of Commerce and Management*, 12(3-4):51–82.
- Atzori, M. (2017). Blockchain Technology and Decentralized Governance: Is the State Still Necessary? *Journal of Governance and Regulation*, 6(1):1–37.
- Atzori, M. (2018). Blockchain Governance and The Role of Trust Service Providers: The TrustedChain® Network. *The Journal of the British Blockchain Association*, 1(1):1–17.
- Biswas, K. and Muthukkumarasamy, V. (2017). Securing smart cities using blockchain technology. *Proceedings - 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016*, pages 1392–1393.
- Carugi, C. (2016). Experiences with systematic triangulation at the Global Environment Facility. *Evaluation and Program Planning*, 55:55–66.
- Fadhel, N. F., Crowder, R. M., Akeel, F., and Wills, G. B. (2014). Component for 3d printing provenance framework: Security properties components for provenance framework. In *World Congress on Internet Security (WorldCIS-2014)*, pages 91–96.
- Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., and Wendland, F. (2018). Blockchain for education: lifelong learning passport. In *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET).
- Grech, A. and Camilleri, A. F. (2017). Blockchain in education.
- Johnson, R. B. and Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher*, 33(7):14–26.
- Lemieux, V. (2017). Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems : An Archival Theoretic Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems :. *Future Technologies Conference (FTC) 2017*, (June):1–11.
- Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? *Records Management Journal*, 26(2):110–139.
- McCONNELL, J. M. (1994). National Training Standard for Information Systems Security (Infosec) Professionals. (4011):29.
- Ølnes, S. (2016). Beyond bitcoin enabling smart government using blockchain technology. In Scholl, H. J., Glassey, O., Janssen, M., Klievink, B., Lindgren, I., Parycek, P., Tambouris, E., Wimmer, M. A., Janowski, T., and Sá Soares, D., editors, *Electronic Government*, pages 253–264. Springer International Publishing, Cham.
- Ølnes, S. and Jansen, A. (2017). Blockchain Technology as a Support Infrastructure in e-Government. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10428 LNCS:V–VI.
- Ølnes, S., Ubacht, J., and Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, 34(3):355–364.
- Otte, P., de Vos, M., and Pouwelse, J. (2017). TrustChain: A Sybil-resistant scalable blockchain. *Future Generation Computer Systems*.
- Rizal Batubara, F., Jolien Ubacht, T., and Marijn Janssen, T. (2018). Challenges of Blockchain Technology Adoption for e-Government: A Systematic Literature Review. *Proceedings of 19th Annual International Conference on Digital Government Research*, page 9.
- Shaw, M. (2002). What makes good research in software engineering? *International Journal on Software Tools for Technology Transfer*, 4(1):1–7.
- Wang, H., Chen, K., and Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation*, 2(1).
- Wang, L., Liu, W., and Han, X. (2018). Blockchain-based government information resource sharing. *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS, 2017-December*:804–809.
- Wang, X., Feng, L., Zhang, H., Lyu, C., Wang, L., and You, Y. (2017). Human Resource Information Management Model based on Blockchain Technology. *Proceedings - 11th IEEE International Symposium on Service-Oriented System Engineering, SOSE 2017*, pages 168–173.
- Woodside, J. M., Augustine, F. K., and Giberson, W. (2017). Blockchain Technology Adoption Status and Strategies. *Journal of International Technology and Information Management*, 26(2):65–93.