IICMR Paper

Cloud Computing and Database Management

Name : Yash Yeole

Email Address : yashyeole17@gmail.com

Name : Venketesh karhade

Email Address :

venkateshkarhade629@gmail.com

Name : Yash Dhande

Email Address : yashdhande99@gmail.com

Designation : Student's

Institute Name : Institute of Industrial and Computer Management and Research, Nigdi Pune

Affiliation : Savitribai Phule Pune University

Collage Address : HS-2, Pradhikaran campus, behind Tukaram Garden, Sector 27A, Pradhikaran, Pune, Maharashtra 411044.

Topic : Trust in records and the view of records and archives as authoritative sources.

Abstract : Cloud computing has been trustworthy and has a central tenet of the European Union cloud strategy for nearly a decade. In this topic we discusses the origins of computing and specifically how the goals of cloud computing - security and privacy, reliability, and business integrity are represented in computer science research. We call for further inter- and multi-disciplinary research on trustworthy cloud computing that reflect a more holistic view of trust.

1. Introduction :

1.1 Background study:

In 2002, Bill Gates, in an email to Microsoft employees, presaged a future where computing would be "an integral and indispensable part of almost everything we do". Microsoft published a white paper defining what would ultimately become a seminal white paper for cloud computing.

Recognizing that trust is a complex concept. Explored trustworthy cloud computing from three perspectives -

- The user’s perspective goals.
- The mechanisms employed by industry to meet the goals.
- The way in which an organisation conducts its operations to deliver the components execution.

While in 2002, cloud computing was not the dominant computing paradigm it is today, these perspectives reflect the dominant themes in computer science research on trust in cloud computing.

Improving the confidence and perception of trustworthiness is critical for the adoption of cloud computing, and has been a central tenet of the European Union cloud strategy for nearly a decade (European Commission 2020).

1.2 Statement of Problem :

Many times records are neglected when authorities are in search of vital information for a particular purpose. This is because of the abundance of information online and offline. Also management prefer to create new information or record rather than refer from records or archives available. The research also seeks ways of creating trust in records and archives, making them an authentic source of data and information for all kinds of activities.

1.3 Objectives :

The objective of trust must be identified before the requirements and obligations of the trust relationship can be articulated. We can examine trust issues from the perspective of those acting, or of that which is acted upon.

On the Internet, the object of trust may be a service provider, a business or organization responsible for creating and presenting information in the form of records or for managing the information about us that we provide online in the course of some personal or business transaction with it. These are actors whom we must evaluate for their trustworthiness in relation to ourselves. In contrast, the object of trust may be the information we access, or the records or data on which we rely or which we provide.

1.4 Scope :

This project is mainly for all institutions, the central government, hospitals, libraries, businesses and organizations, e-government that make use of records and archives. It also encompasses creating security software and hardware to protect both archives and records for it to achieve the needed authenticity.

1.5 Limitations :

This research explored the relationship between practice and belief in establishing and assessing authenticity of digital records among a sample of records professionals. Overall, respondents adopt a pragmatic approach to authenticity based on resources, sensitivity of the records, and organizational framework. In research of across variables of profession, sector, and legal system these professionals rely most heavily on social indicators of authenticity in daily work, but exercise greater trust and reliance on technical indicators in the process or expectation of authenticating records. Experience of authenticating records affected belief in the value of indicators, with those who had never had to authenticate records placing higher faith in technical indicators. Interviewees generally agreed that the traditional archival model of record authenticity still held in the digital environment, but required adaptation. Although the research did not originally intend to explore in depth the function of legal system as an independent variable, the findings that did emerge open up an interesting line of inquiry for further study.

2. Literature Review:

1) Data ownership and control :

Cloud computing often involves storing data on servers own and managed by third-party providers. This can create challenges in terms of data ownership and control, as organizations may not have full access to or control over their data. This can make it difficult to establish trust in the accuracy and completeness of records stored in the cloud.

2) Data security :

Cloud computing providers gives security measures to protect data stored on their servers, including encryption , firewalls, and access controls. However, security incidents can still occur, which can undermine trust in the integrity of records stored in the cloud.

3) Compliance and Regulation :

Depending on the industry and there may be specific regulations and compliance requirements related to data management and security. Organizations that store records in the cloud must ensure that they comply with these requirements, which can be challenging when data is stored across multiple servers and locations.

4) Data portability :

In today’s world organizations are more depends on cloud computing for data storage and management, they are also consider how to maintain the portability and accessibility of their data over time. This can

be especially important for records that must be preserved for long periods of time.

2.2 Summary of Literature Review :

This paper presents a review of the literature about authenticity of records, beginning with the foundational literature in order to frame current writing on authenticity of digital records. The concept of authenticity of records is fundamental to archival science and digital preservation research investigates the nature of digital objects, including records and data, and the attributes. While much research has been and continues to be conducted into the protection of authenticity in the context of requirements for digital preservation, current means of evaluating authenticity for records professionals still do not offer quantifiable measures, and generalizable models that can reduce the problem to concrete, atomistic elements are elusive.

3.1 Methodology :

1) Risk assessment:

While conducting a risk assessment is a crucial step in establishing trust in records stored in the cloud. This involves identifying potential risks in the cloud environment, such as data breaches, cyber-attacks, or unauthorized access. A risk assessment can help organizations develop strategies to decrease these risks and improve the security and reliability of their records.

2) Encryption and access controls:

For Implementing strong encryption and access controls is critical to ensuring the security and confidentiality of records stored in the cloud. Encryption can prevent unauthorized access to data, while access controls can restrict access to sensitive information to authorized personnel only.

4) Block chain technology :

The use of block chain technology in cloud computing provide an additional layer of trust and security to the records stored in the cloud. Block chain can provide a decentralized and transparent system for recording and verifying transactions of data, which can enhance the trustworthiness and authenticity of records stored in the cloud.

5) Periodic audits :

Conducting periodic audits of cloud service providers can help organizations ensure that their records are being managed and secured in accordance with established policies and standards. Audits can help identify areas for improvement and provide reassurance that records stored in the cloud are being properly managed and protected.

3.2 Research Design:

The internet first personal data collectors were websites and applications. By tracking users' activities online, marketers could deliver targeted advertising and content. More recently, intelligent technology in physical products has allowed companies in many industries to collect new types of information, including users' locations and behaviour. The personalization this data allows, such as constant adaptation to user's preferences, has become central to the product experience.

4.1 : Conclusion and Recommendations :

Most of the people want to be able to operate in an online environment where they can assume trust. This requirement should therefore be considered a priority by the international community. Solutions should take responsibility off the shoulders of the individual whenever possible, and they need to provide for authentic, reliable, and accurate records and data that exist in a balance between transparency and security.

4.2 Results :

Records has serious consequences for administrative accountability, citizen rights, collective memory, and historical knowledge, all of which are shaped, tacitly, subtly, sometimes unconsciously, yet profoundly by the naturalized, largely invisible. The proper records management can go a very long way to make these file very valuable in decision making in various libraries, organization, business, governmental agencies, etc.

5. References

David Weinberger (2009) "JOHO the Blog" http://www.hyperorg.com/blogger/2009/07/19/transparencyis-the-new-objectivity/

David Weinberger (2009) "JOHO the Blog" http://www.hyperorg.com/blogger/2009/07/19/transparencyis-the-new-objectivity/

www.researchgate.net

ACA. 1999. "Code of Ethics | The Association of Canadian Archivists." http://archivists.ca/content/code-ethics

Cook, Michael. 1986. The Management of Information from Archives. Aldershot, Hants, England ; Brookfield, Vt., U.S.A: Gower.