The Role of Digital Forensics in Modern Accounting Practices

Dr Hetal Jignesh Lavantra
Assistant professor
B.com. (sf) & M.com department
C. P. patel & F. H. Shah Commerce College, Anand (Autonomous)

Abstract

It is interesting to note that the modern accounting systems have undergone a dramatic change due to the rapid advancement of digital technologies. This has led to a situation in which digitalization has not only enhanced the availability, accuracy, and efficiency of financial data, but it has also led to a rise in cases of data manipulation, financial fraud, and cybercrime. However, digital forensics is one of the most important tools for addressing these concerns with specific techniques for locating, analysing, and preserving digital evidence. This paper focuses on the role played by digital forensics in modern accounting systems, with specific reference to its application in detecting fraud, investigating financial crimes, preserving evidence, ensuring compliance, and improving cybersecurity.

Digital forensics enables auditors and accountants to identify suspicious transactions, retrieve hidden data, and verify the accuracy of financial data. In cases where digital evidence is required to be preserved and presented in a manner consistent with applicable laws, digital forensics is also essential for litigation support. Moreover, with regulatory bodies increasingly requiring organizations to use digital forensics for ensuring compliance with applicable financial reporting regulations and data protection laws, it is essential for organizations to incorporate digital forensics in their accounting systems for improving their internal controls, risk management capabilities, and defences against cybercrime.

Based on the findings in the study, digital forensics plays a highly significant role in making the financial reporting systems transparent, accountable, and trustworthy in nature. By bridging the gap between accounting and technology, digital forensics helps professional's combat misconduct in a digital economy. In short, digital forensics is a defensive and offensive tool for building trust in a digital economy.

Keywords: Digital forensics, forensic accounting, cybercrime, financial fraud, accounting information systems, digital evidence.

Introduction

Accounting Information Technology (AIS), cloud computing, online financial platforms, and enterprise resource planning software are digital technologies considered very important in the field of accounting. They make people more efficient but more vulnerable to committing or being victims of financial fraud, data breaches, cybercrimes, etc.

Digital forensics is a branch of forensic science that involves the search, preservation, study, and presentation of digital evidence. It is a very important aspect in keeping digital information secure and assisting in investigations. This paper will discuss the contribution of digital forensics to the improvement of modern accounting.

The primary objectives of digital forensics inquiry, a branch of forensic science, are to locate, analyse, and examine digital evidence stored in computers and digital devices. Digital evidence recovered from a variety of sources is identified, protected, analysed, and presented to help reconstruct what happened in a crime or to prevent unauthorized acts from interfering with planned operations. There are several steps in the digital forensics investigative process: seizure, acquisition, analysis, and reporting.

This branch of forensic science is very important in law enforcement investigations, trials, internal investigations, tribunals, and other areas where the data recovered in the research is required. In order to use digital evidence in court, it must be recovered from sources like computers, mobile phones, servers, networks, etc. through methods scientifically tested. This branch has gained a strong reputation in the

field due to the increasing popularity of digital media in storing information and the rise in cybercrimes worldwide.

Conceptual Framework

1. Digital Forensics

Digital forensics is a scientific process for:

• Determining digital evidence
• Maintaining the integrity of data
• Analysing documents in electronic form
• Making presentations during court hearings

This might include cloud forensics, computer forensics, network forensics, and database forensics. This information, together with what the accountants know concerning computer forensics, will now enable them to make a good judgment concerning their future activities and the way in which the investigation will be carried out. PC, server, Internet, social media, cyber game chips, network operations centre, BBS, server architecture...All aspects of the Internet can therefore be considered to be included in computer forensics or digital investigation.

"Computer forensics is one of the abecedarian capacities a forensic accountant must develop in order to execute their duties efficiently."

Using scientific ways for investigating digital crimes, Digital Forensics (DF) finds trends in cybercrime and obtains Implicit Digital substantiation (PDE) for use in court.

"Digital forensics is a science for the collection, confirmation, identification, and interpretation of digital evidence from digital sources using scientifically proven methods in a way that supports the investigation of crimes under investigation, attempts to assist in green behaviours that may interfere with planned activities or to reconstruct illegal activities."

Given the increase in the use of digital technologies, forensic accountants are focusing their efforts on e-discovery and computer forensics. There are four important pretensions of the digital forensic process, namely substantiation recovery, preservation, donation, and discovery. Such should be the order, visibility, condensation, and narration of all digital substantiation.

2. Modern Accounting Practices

Today’s accounting world looks pretty different than it did even a decade ago. Now, everything runs through digital tools—think computerized bookkeeping, cloud-based software, electronic financial reports, and online payments. On top of that, a lot of companies use ERP systems to tie all their financial management together. All these technologies leave behind digital audit trails, which turn out to be crucial when you need to dig into the numbers for a forensic investigation.

Role of Digital Forensics in Modern Accounting

1. Fraud Detection and Investigation

Digital forensics aids in identifying:

Cooked financial records, Unauthorized Transactions, Identity theft, Money laundering, Payroll Fraud.

Forensic specialists review deleted files, transaction histories, metadata and system logs to locate fraudulent activity.

2. Preservation of Digital Evidence

The guide is important to maintaining the evidence's integrity in financial investigations. Forensic digital methods guarantee: Data is accurately imaged and the chain of custody is recorded. When digital evidence is preserved, it can be presented in a court to avoid evidence contamination.

3. Making internal controls stronger

Digital forensics gives internal audits a real boost. It tracks who’s accessing what, spots system issues, finds weak points in how things are run, and comes up with smarter ways to manage risk.

4. Investigating cybercrime

Modern accounting systems face all sorts of cyber threats—ransomware attacks, phishing scams, hackers poking around in financial databases, and big security breaches. Digital forensics experts step in to track down IP addresses, analyse network activity, and recover lost data.

5. Making it easier to follow the rules

There are strict rules about protecting data and reporting finances. Staying compliant means keeping records straight and transparent. Digital forensics helps make that happen by making sure audit guidelines are followed, verifying financial statements, and catching anyone who tries to break the rules.

Tools and Techniques Used in Digital Forensics for Accounting

Software for data recovery

In order to retrieve erased, concealed, corrupted, or unreadable data from digital storage media, data recovery software is employed. In digital forensics, this is crucial in order to recover data which could have been erased intentionally. It works at the sector level; the storage medium is scanned. Using file signatures, erased files are recovered.

Retrieves data from file systems which have been damaged. Fragments of files which are partially overwritten are recovered.

Some of its most common traits are:

• Ability to scan deeply.
• Getting back to partitions.
• Cutting files.
• Getting data from formatted disks.

Tools for looking at logs.

These tools scan network, application, and system logs to detect any unauthorized access, security issues, or suspicious activity. In the reconstruction of incidents, logs are crucial.

It evaluates to Attempts to log in Events which involve file access.

• System malfunctions Logs of network traffic.
• Activities which are related to firewalls.

Software for forensic imaging.

Digital forensics makes an exact copy of the digital storage medium, bit for bit. It keeps the evidence safe while it is being looked at. The basic idea behind it is to make images of the digital storage medium in bit streams.

Its goal is:

- To protect the evidence's integrity.
- To make analysis safe.
- To stay legal.
- To write blockers.
- Chain of custody.

Tools for analysing databases Database forensic tools examine structured data kept in databases to find concealed information, tampering, or illegal quests. Among its conditioning are Restoring cancelled documents, Chancing traces of SQL injection, Analysing sale records, Feting abuse of honour. Block chain sale tracking tools to find illegal fiscal overflows, block chain forensic tools follow bitcoin deals across distributed checks. These technologies relate portmanteau addresses with realities using analytics and clustering because block chain is transparent but pseudonymous.

Its goal

- Grouping of holdalls
- Looking at graphs of sales
- Evaluation of threats
- Feting services for mixing ways include making use of hunt terms Investigators can fleetly sift through vast quantities of data for material content by using keywords.

Types

- A perfect fit
- Wildcard search
- Use Boolean logic (AND, OR, NOT) to hunt
- Common phrases

Problems with Using Digital Forensics in Accounting

Digital forensics is important, but it has a lot of problems to solve:

1. Technology changes quickly

- Technology is changing quickly:
- Cloud-based accounting
- AI-powered financial systems
- Cryptocurrencies
- DeFi, which stands for decentralized finance
- Wallets that work online

CHALLENGE:

- Investigators need to stay up to date on their skills.
    - Forensic tools might not be needed for much longer. It might be hard to look at new financial technologies.

2. Barriers to data protection and encryption

- Every day, modern businesses make a lot of digital financial data, like:
- Data from the ERP system
- Transactions that happen through online banking
- Electronic invoices
- Emails
  Information from cloud accounting
- Transactions on the block chain

CHALLENGE:

- It takes a long time to sort through millions of transactions.
- It's hard to find useful evidence among useless data. • Needs advanced analytics and data mining tools.

3. Not enough skilled forensic professionals

To do digital forensic accounting, you need to know:

- Accounting rules
- Safety
- Analysis of databases
- Rules of law
- Analysing data

CHALLENGE:

- Not knowing enough about digital forensics and accounting.
- Getting certified and trained costs a lot.
- Bringing in outside forensic experts.

4. Forensic tools are very expensive

- Digital forensic tools cost a lot of money.
- Close
- FTK Platforms for analysing block chains
- Software for looking at logs

CHALLENGE:

- Small businesses can't afford high-end digital forensic tools.
- Longer investigations cost more.
- Needs a safe place.

5. Problems with the law and where it applies

It might be hard for auditing courts and other people to understand digital technology-based forensic conclusions.

CHALLENGE:

- Putting digital technology facts into a form that is easy for the law to understand.

- Putting digital findings into a form that is easy to understand legally.
- Making sure that digital data isn't misread.

Benefits of Digital Forensics in Modern Accounting

1. Makes finances more open

When you talk about financial transparency, you're really talking about being honest and upfront with everyone involved—giving clear, open info about the money. Digital forensics tools make this way easier. They let you dig into the full transaction history instead of just a small slice. You can spot if someone tried to hide, change, or erase entries. You can even double-check the facts by looking at the metadata. Plus, audit trails track any changes made to the accounting system. So, digital forensics helps businesses keep their financial reports accurate by putting transactions back in the right order. This way, there's less of a gap between what management knows and what they actually share with stakeholders.

2. Reduces fraud risks

Digital forensics really cuts down on fraud. People sometimes try to twist the numbers, steal, or mess with company operations. With digital forensics, you can keep an eye on every transaction as it happens, spot weird patterns or anything out of the ordinary, catch unauthorized access, and flag things like duplicate payments or fake employees and vendors. And honestly, just knowing that digital forensics is watching tends to keep people from trying anything shady in the first place.

3. Improves marketable governance

Marketable governance is all about the rules, programs, and habits a business uses to stay on track. Digital forensics plays a big role here. It makes sure financial reporting is solid, beefs up internal controls, and gives audit panels the digital proof they need. It also helps catch anyone trying to override proper procedures. All of this makes it easier for boards and oversight groups to keep things ethical and legal.

4. Strengthens stakeholder confidence

Shareholders, investors, employees, visitors, regulators—they all have something at stake in how an organization runs.

Their trust depends on what they see:

Is the company acting ethically?

Can it stay financially healthy?

People want proof, not just promises.

Here's what builds that trust:

- The company stays open about what its doing.
- It backs up numbers with real evidence.
- It makes cheating tough.
- It spots problems fast. When stakeholders see strong digital forensics in place, they believe the organization is reliable and well-managed.

5. Supports action and resolves disputes

Financial problems can get messy—fraud, broken contracts, even company collapse. Shareholders clash. Digital forensics steps in to help sort it out:

- It delivers digital proof that holds up in court.
- It tracks evidence carefully, so nothing gets lost or tampered with.
- It uncovers financial records people tried to hide or erase.
- It rebuilds trade histories for court cases.

Forensic accountants don't just gather facts—they make complicated issues clear, so judges and juries actually get what's going on.

Conclusion

Digital forensics isn't just a fancy add-on to accounting anymore—it's essential. As finance goes digital, the risks of fraud and cybercrime climb. Adding digital forensics to accounting protects financial data and keeps reporting honest. In the end, it's not just a crime-fighting tool. For modern accounting, it's a must-have.

References

1. H. A. Javaid, "Improving Fraud Detection and Risk Assessment in Financial Service using Predictive Analytics and Data Mining," Integrated Journal of Science and Technology, vol. 1, no. 8, 2024.
2. A. Qatawneh, "The role of organizational culture in supporting better accounting information systems outcomes. Cogent Economics & Finance, 11 (1), 2164669," ed, 2023.
3. P. Sharma, "Leveraging generative artificial intelligence for real-time fraud detection in banking systems," International Journal of Innovative Research in Science, Engineering and Technology, vol. 11, no. 12, pp. 1234-1245, 2023.
4. A. M. Qatawneh, "Risks of adopting automated AIS applications on the quality of internal auditing," Journal: WSEAS Transactions On Business And Economics, pp. 763-779, 2021.
5. E. Tariq et al., "How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks," International Journal of Data and Network Science, vol. 8, no. 1, pp. 69-76, 2024. 6. A. Qatawneh, A. Lutfi, and T. Al Barrak, "Effect of artificial intelligence (AI) on financial decision-making: mediating role of financial technologies (Fin-Tech)," HighTech and Innovation Journal, vol. 5, no. 3, pp. 759-773, 2024.
6. M. Khan, "Ethics of Assessment in Higher Education–an Analysis of AI and Contemporary Teaching," EasyChair, 2516-2314, 2023.
7. A. Musunuri, "Leveraging AI and Deep Learning for E-Commerce Customer Segmentation," International Journal of Innovative Research in Science, Engineering and Technology, vol. 12, no. 6, 2023.
8. A. Ukato, O. O. Sofoluwe, D. D. Jambol, and O. J. Ochulor, "Optimizing maintenance logistics on offshore platforms with AI: Current strategies and future innovations," World Journal of Advanced Research and Reviews, vol. 22, no. 1, pp. 1920-1929, 2024.
9. I. Ikram and Z. Huma, "An Explainable AI Approach to Intrusion Detection Using Interpretable Machine Learning Models," Euro Vantage journals of Artificial intelligence, vol. 1, no. 2, pp. 57-66, 2024.
10. C. Li, Y. Tang, and K. Xu, "Investigating the impact AI on Corporate financial and operating flexibility of Retail Enterprises in China," Economic and Financial Research Letters, vol. 5, no. 1, 2025.
11. P. Agarwal and A. Gupta, "Cybersecurity Strategies for Safe ERP/CRM Implementation," in 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT), 2024: IEEE, pp. 1-6.
12. H. Allam, J. Dempere, V. Akre, D. Parakash, N. Mazher, and J. Ahamed, "Artificial intelligence in education: an argument of Chat-GPT use in education," in 2023 9th International Conference on Information Technology Trends (ITT), 2023: IEEE, pp. 151-156.
13. L. Ghafoor and M. Khan, "A Threat Detection Model of Cyber-security through Artificial Intelligence."
14. S. Al-Sakini, H. Awawdeh, I. Awamleh, and A. Qatawneh, "Impact of IFRS (9) on the size of loan loss provisions: An applied study on Jordanian commercial banks during 2015-2019. Accounting, 7 (7), 1601-1610," ed, 2021.