Global Scientific JOURNALS

GSJ: Volume 7, Issue 7, July 2019, Online: ISSN 2320-9186
www.globalscientificjournal.com

CLOUD-BASED FRAUD CONTROL IN PROJECT MONITORING

ABAS A.[1] and Sule Shehu[2]
[1]abas.aliu@gmail.com
[1 and 2]DEPARTMENT OF COMPUTER SCIENCE, AUCHI POLYTECHNIC, AUCHI, EDO STATE

ABSTRACT

This paper identifies the alarming and the essence of fraud in project construction. It also identifies the importance of data protection, deployment and strengths in cloud-based project monitoring. Most projects are delayed or not completed by the initial contractor due to inability to control fraud and monitor the execution of the project. There is urgent need for understanding the technological cloud-based computing which has a lion's share in increasing the efficiency, control fraud and output of every project monitoring. Areas of fraud by construction contractors were identified with the preventive mechanism. Also set of recommendations for organizations and project owners who will provide and manage this technological cloud-based computing were made.

Keywords: Cloud-based, fraud control and project monitoring

Introduction

A common understanding of "cloud computing" is continuously evolving, and the terminology and concepts used to define it often need clarifying. Press coverage can be vague or may not fully capture the extent of what cloud computing entails or represents, sometimes reporting how companies are making their solutions available in the "cloud"(Dialogic C., 2010).

"Cloud computing" was coined for what happens when applications and services are moved into the internet "cloud." Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications (Dialogic C., 2010).

Fraud is very much a part of every business and projects are no different. Actually, there are more chances in project fraud than other type of business frauds especially when it comes to engineering and construction projects. Project fraud often originates because employees don't want to report bad news or information that can harm them politically or career wise. It also often results from poor planning and supervision that leads to project rework, placing the project further behind (Bassam S,2013).

Projects are investments that organizations undertake to achieve their strategic objectives, regardless of the industry, size and type of projects. When a project is approved for execution, the investment that had been allocated for the project would take into consideration the revenue that this project will generate when completed as well as the level of risk that the project has. Failing to achieve the estimated return of investment would result in unrecoverable losses to the project owner. Of course, the return of investment is not necessarily that always be

measured in monetary figures but also in terms of other tangible and intangible benefits.

The technology behind cloud-based has become user friendly and user access point in fraud control and project monitoring. This will enable every organisations that are interested for the monitoring of their project to avoid fraud and the delay of project completion.

Cloud computing

Cloud computing is the use of computing resources that are delivered as a service over the Internet. This means that software, hardware and network resources are centrally managed. The end user will not need to install any software locally on his computer (Thorvald W., 2013).

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications.

Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

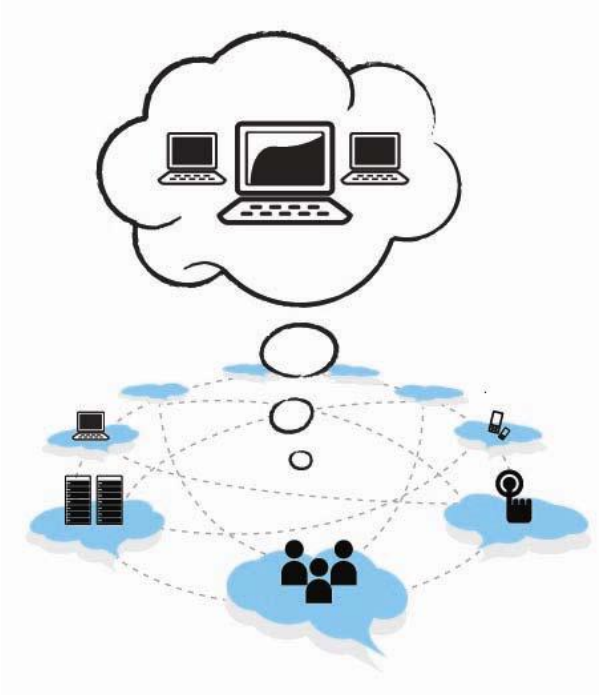

Fig 1: Structure of Cloud-based Computing

Construction in the Cloud

Gordon Ritter, 2013 published an article titled "How to Tell if You're in a Cloud-Friendly Industry". In it, Ritter ranks industries that are more or less conducive to Software-as-a-Service (SaaS) strategies and factors that make them so.

In the top tier of 'cloud-friendliness', Ritter places healthcare and education. He indicates that SaaS solutions help healthcare companies stay current in a strongly regulated industry, while educational institutions require applications that are designed for non-desk workers and leverage big data.

In the second tier, Ritter ranks retail, utilities, transportation, real estate, construction, and insurance, citing a mobile workforce, visual elements and big data as key drivers of SaaS adoption.

Banking and government are relegated to the third tier, due principally to privacy concerns and the high cost of migrating applications from heavily invested legacy systems.

Factors of Cloud-friendliness

Ritter's eight factors that determine cloud-friendliness are intuitively logical:

1. **Dynamic regulatory environment** – SaaS platforms enable rapid and 'auditable' deployment of new features and functionality to comply with regulatory changes.
2. **Dissatisfaction with incumbents** – vertically specialized solutions in the cloud reveals the low flexibility and value of horizontal software and systems on premise.
3. **High industry concentration** – SaaS solutions for industries in which fewer than 50 companies represent more than 80% of total revenue allow higher efficiency in sales and marketing and lower customer acquisition costs (Gordon R, 2013).
4. **Mobile workforce** – industry-specific, mobile cloud applications available on smartphones and tablets are particularly appealing to vertical segments with high percentages of non-desk workers.
5. **Value in data –** certain industries require access to and analysis of huge volumes of data – big data – and SaaS architectures are especially effective in managing large data sets and capturing new data streams for end-user behavior and other revenue-enhancing intelligence.
6. **SaaS platform alignment** – the ability to leverage existing commercial cloud platforms speeds time to market and enables companies to focus on industry-specific applications rather than underlying infrastructure.
7. **Industries with little to no cyclicality** – many SaaS businesses generate recurring revenue and companies migrating their solutions to the cloud may require an initial IT investment, both of which are potentially problematic in cyclical environments. A key virtue of SaaS is speed and simplicity in delivering application updates and revisions to users.
8. **Visually dependent** – industries that rely heavily on visual representations have found that cloud platforms are best suited to the integration of visual

images and can leverage the power of high-quality cameras on mobile devices for capturing and distributing images.

The Architecture, Engineering and Construction industry meets most, if not all, of the above criteria for cloud-friendliness.

Cloud-based Deployment Models

Deploying cloud computing can differ depending on requirements, and the following four deployment models have been identified (**Dialogic C., 2010)**, each with specific characteristics that support the needs of the services and users of the clouds in particular ways (see Figure 2).

- **Private Cloud** — The cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises.
- **Community Cloud** — The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The operation may be in-house or with a third party on the premises.
- **Public Cloud** — The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.
- **Hybrid Cloud** — The cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data in an organization, and also the need to offer services in the cloud (**Dialogic C., 2010)**.

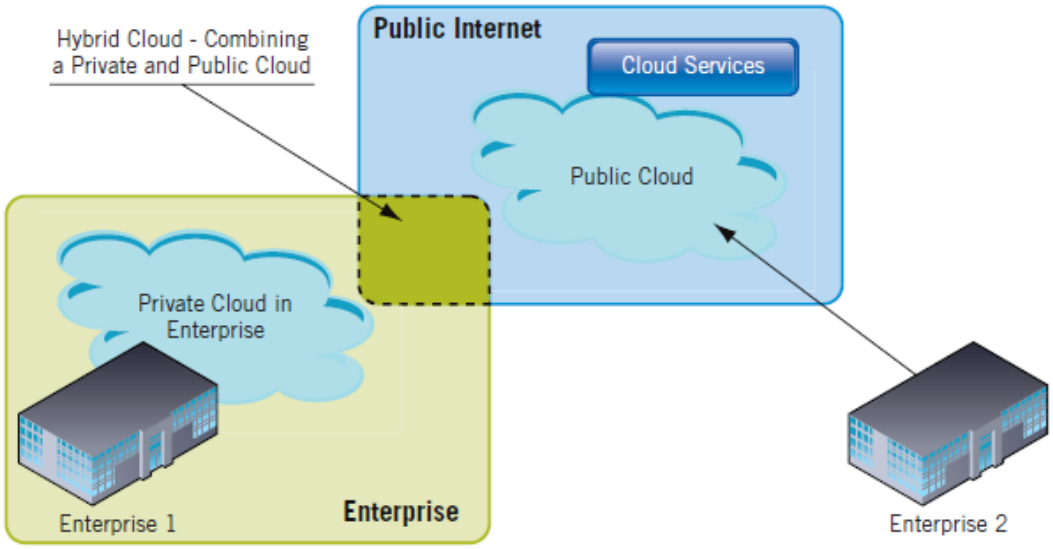

Fig. 2: Public, Private and Hybrid Cloud Deployment, (source Dialogic)

Benefits of cloud project monitoring

- It enables project teams to meet compliance and reporting requirements proactively rather than after the fact.
- AEC professionals are frequently on site and elsewhere away from their offices. They need to be able to create, capture, review, update, and approve project information at any time, from anywhere.
- It enables inspectors on site to verbally and visually capture defects and safety issues for resolution by subcontractors. Mobility improves project team efficiency and productivity while reducing risk and keeps projects moving around barriers of time and distance toward successful delivery.
- Big data is driving big changes throughout the AEC industry. Projects are generating terabytes of data, with multi-dimensional Building Information Modeling (BIM) files, tens of thousands of documents and drawings in multiple versions, and hundreds of thousands of correspondence items – plus photos and videos. The project software are designed to scale with projects such that any number of files, of any size, can be shared,

distributed and revised among diverse project teams whose members may be scattered across different geographies.

- Also, with a complete audit trail and analytical tools, owners, developers, contractors, and project managers can benchmark the performance of their projects for continuous improvements in efficiency, accountability and risk management.

Fraud control

Fraud can be defined as 'dishonestly obtaining a benefit by deception or other means'. Fraud control refers to the integrated set of activities to prevent, detect, investigate and respond to fraud and to the supporting processes such as staff training and the prosecution and penalisation of offenders (ANAO, 2011).

Project Fraud

Project fraud is the misrepresentation of a project's mission or progress to secure project financing, reporting wrong project progress to hide project delays and/or budget overrun, wrong forecasting for expected project cost at completion to avoid reporting lower project profitability, overestimating the value of anticipated changes to the project scope to increase the project value, misuse of project resources, and/or improper dealings with project vendors for personal enrichment, substituting specified equipments and materials with lower quality alternatives, among many others (Bassam S., 2013).

Types of Project Fraud

The most common types of project fraud includes over-reported and unsubstantiated business case or feasibility studies, unsubstantiated project decisions, under-reported initial estimates of project lifecycle costs, under-reported initial estimates of project maintenance costs, setting unrealistic project completion dates, unbalancing the project cost estimate, under-reported costs, over

reported schedule progress, over-reported quality progress, project asset misuse, vendor conflict of interest and kickbacks, vendor "overselling" of their capabilities, inappropriate vendor charges (Bassam S., 2013).

Those project frauds occur to direct the decision makers to take certain decisions that if they would have the correct information instead of what had been passed, those decisions could have not been taken. For example, over-reported and unsubstantiated business case or feasibility studies would lead the decision maker for selecting the wrong project investments

Alarming Fraud Statistics in Project Construction

Grant Thornton International, a global advisory firm, recently issued a report on fraud in the construction industry in Australia, Canada, India, the U.S., and the U.K (Tod B., 2013). The statistics are sobering:

- 3.4% of all fraud cases reported over a two-year period were in construction(ACFE, 2013)
- The median average loss was US$300,000 (TOD B., 2013).
- Fraud impacts 10% of the industry's total revenues in the U.K.(CILACF)
- Applying these data points to global construction and its projected growth suggests that fraud and corruption could account for US$860 billion today and $1.5 trillion by 2025.(GCPOEGC)

Grant Thornton adds an accelerating factor: "As the global economy recovers, activity across the construction industry will increase. This will bring more opportunities for fraud." (Tod B, 2013)

Construction Projects: Where Fraud Occurs

The report, titled Time for a New Direction: Fighting Fraud in Construction, identifies eight types of fraud most commonly found in its research (TOD B., 2013):

- Billing fraud
- Bid/contract rigging
- Bribery/corruption
- Fictitious vendors
- Change order manipulation
- Theft or substitution of materials
- False representation
- Money laundering/tax avoidance.

Grant Thornton cites project complexity and project team diversity as fraud risks:

"The larger the number of stakeholders involved in a project, the more opportunities there are for fraud…In addition to perpetration from inside the company, suppliers such as contractors, sub-contractors and even lending organisations must be considered risks to be addressed as part of a company's fraud exposure management policy."

Fraud Prevention and the Role of Technology

Clearly, organizational cultures, value systems and zero-tolerance policies from the board and executive levels down – communicated broadly and unequivocally throughout the project team from day one – play a critical role in fraud prevention.

However, as Grant Thornton Australia partner Chris Watson told ConstructionIndustryNews.net:

"There are two sides to one coin and any fraud survey will say the same thing: poor controls are the single biggest factor for allowing fraud to occur and good controls are the single biggest factor for preventing and detecting fraud in an organisation – it's that lack of control or oversight that is the issue for most of these organisations."(Chris W. 2013)

In its report, Grant Thornton recommends that project owners and managers implement "mitigating, preventative and detective controls," capture fraud risks in

a register, institute policies to mitigate identified risks, and use technology for data-intensive procedures.

Grant Thornton quoted *"Technology can be a powerful tool in preventing and investigating fraud. Once policies are in place, technology can take much of the work out of implementation."*

Safe in the Cloud

In simple terms, cloud computing is a method of storing files and data in a centralized networking that can be reached from anywhere and by any type of device. This includes mobile phones, tablets, laptops and desktops. The notion of the "cloud" is because this data is placed in a network where say someone in NYC could access as well as someone in California (Efraudprevention, 2013).

Here are some tips to protect your data in the cloud:

- **Look for a Secure Web Address**: Before shopping online or giving any sort of personal information, look at the URL—if the website is secure connection enabled, it will have an 's' after the 'http' portion of the URL. An 'https' URL tells you the website has an SSL license, meaning your information is scrambled as it travels across the internet.
- **Don't Provide Personal Information**: Don't put anything in the cloud you would not want others to see, especially the government or a private litigant. A credible website will never need sensitive personal information, like your social security, PIN, or bank account numbers. If a site you don't trust asks you for anything personal, don't trust it! It could be a phishing scam trying to gain access to your personal information. Pay close attention if the cloud provider reserves rights to use, disclose, or make public your information.
- **Create Strong Passwords**: Make long passwords with at least eight or more characters. For added security, include punctuation, symbols and a

mix of upper and lowercase letters. Don't ever use the same password for all of your accounts and change them at least once a month.

- **Check for Site Updates**: Credible websites are updated often with security measures. Look around to see when the site was last updated. If it's been more than a couple of months, you might not trust the site.
- **Leaving the Cloud**: Know exactly what happens when you remove your data from the cloud provider. Does the cloud provider still retain rights to your information? If so, consider whether that makes a difference to you.
- **Delete Cookies Often:** Cookies are small files designed to track your web activity. When you enter information into a site, such as a user name and password, the site uses cookies to remember your information so you don't have to enter it the next time you visit. Hackers can use cookies to gain access to your accounts, so you should delete them often. Deleting cookies differs depending on which browser you use, but it's usually found in your browser's privacy settings.

Cloud-based Network Monitoring

The fact remains that you must monitor the entire network to make sure everything is working properly and to find and repair problems when something isn't.

Advantages of Cloud-based Network Monitoring

The cloud-based network monitoring comes in to play. It's definitely something you need in your toolkit if you don't want large slabs of your network breaking off and floating away in the air.

There are many advantages to using cloud-based network monitoring. Here are the top eight:

1. **The means to stop broadband and switches overspend**. IT finds itself in a common state of fear of slow or full connections so it perpetually

overspends for more bandwidth and switches. Cloud-based network monitoring shows you actual traffic flow so you can plan – and buy – smarter.

2. **Greater scalability**. As more and more of your data and applications move to the cloud, you'll need to increase what you monitor in the cloud and perhaps the number of cloud providers (and their ISPs) too. The scalability of cloud-based network monitoring tools, then, is a great advantage.
3. **Threat detection**. Security is still an issue in cloud services, on-premise services, and in hybrid environments too. Cloud-based network monitoring gives you a means to detect threats beyond what your traditional network management system might find.
4. **Increased integration**. You've heard it said that IT has become almost exclusively integration specialists today and that becomes increasingly truer with the addition of more cloud services. In other words, it's no longer about keeping the lights on, but about making sure all the things work with all the other things. The good news is that many cloud-based network monitoring products are designed to integrate well with your existing performance and configuration programs.
5. **A better handle on your mobile traffic**. BYOD is here to stay. Unfortunately it can be tough to get a handle on how many such devices are on your network, what they are doing there, and their impact on your overall network traffic. A good cloud-based network monitoring system can nail all that down for you.
6. **Generally costs less**. To put it simply, you get solid network traffic analysis for less than you would typically spend for on-premise network management.
7. Comprehensive monitoring. In short, you get to see the entire network in one view as opposed to a collection of standalone views.

8. A means to evaluate cloud services performance. The ability to drill down and see how much of cloud services your company is actually using is priceless…or at least gives you the means for price containment. With cloud-based network monitoring you can see how much of cloud services were actually used versus the amount billed, and whether delivery met vendor promises, among other things.

Cloud computing is generally paid for through a fixed monthly fee. The user does not have to buy a software license but instead he rent it. This reduces the startup cost and distributes the costs over time instead. In cloud computing, the provider will normally continuously develop software and make new features available for you without adding cost, as opposed to buying the software and later having to pay for upgrades in order to keep full compatibility with new versions of the operating system for example. Software maintenance being taken care of by the provider saves the client expenses for local IT support (Thorvald W, 2013).

Important of cloud-based fraud control in project monitoring

- To collect and transmit information from field in real time to a central server.
- Cash flows or spent in each stages of project is captured and transferred from the site device to the centralized server
- Information from field will be collected using hand held devices/ mobile phones.
- Information collected can be a photo, video, audio, note or a survey/ inspection form.
- Fraud messages can be flag out from the centralized server when fraud occurred at the remote site.
- Information collected is to be stamped with Geo Coordinates and time.

- Information collected will be encrypted and instantly transferred from the device to the centralised server using network connectivity of the device.
- Information can be captured and transmitted by Field officers, inspection teams, Volunteers, NGOs etc.

Cloud Computing Infrastructure

The system process a lots of projects on a daily basis, from initial data entry to final intelligence analysis, managing diverse communication channels such as websites, mobile data, Email and SMS, providing a seamless and powerful environment for vigilance data processing, communication, monitoring and management (Raja S, 2009).

Such a system of state level scale requires sophisticated and scalable compute infrastructure. The advancements in cloud computing and data centre infrastructure make it possible to meet such requirements. Diagram below illustrates the cloud computing ecosystem,

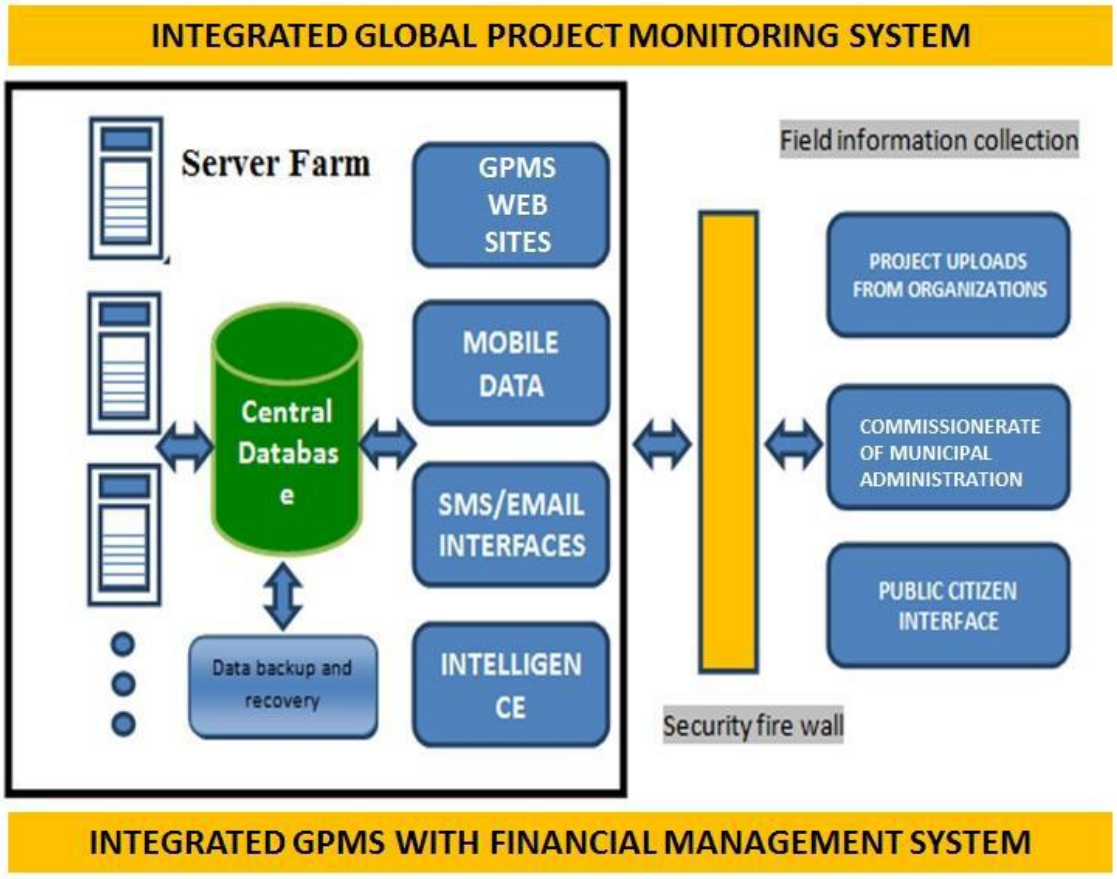

Fig. 3: Integrated Global Project Monitoring System (source Raja)

ESSENCE OF FRAUD IN PROJECT EXECUTION

The Federal Ministry of Water Resources (FMWR), and its agencies, mismanaged a large chunk of the N30billion it was allocated, between 2006 and 2008, as part of the Millennium Development Goals (MDG) funds (Premium Times,2012).

PREMIUM TIMES' ongoing investigations into the utilization of Nigeria's MDG funds show that the ministry, just like its Health counterpart, has mismanaged billions of naira that should have used to provide potable water for some of the over 60 million Nigerians who have no access to clean water.

A 2012 report by the World Health Organization and the United Nations Children's Fund, established that 66 million Nigerians lack access to water. Because almost half the population lacks access to good water, water-borne diseases remain rampant in this oil-rich West African nation, with diseases like

dysentery, cholera, typhoid fever and others killing hundreds every year (Premium Times, 2012).

Of the N99.9billion budgeted for the MDGs in 2006, the headquarters of the FMWR was allocated N9.42 billion naira. In 2007, the ministry got 10 per cent of the N109 billion; while it got 10.8 billion of the N111 billion allocated in 2008 (Premium Times, 2012).

As independent monitors and evaluators from the office of the OSSAP-MDGs stated in their reports for 2006, 2007 and 2008, that most of the projects for which the water resources ministry got funds were like that of Erin Omu. Most of them were phantom projects (Premium Times, 2012).

Again in 2007, another N1billion was approved for the Ogun-Osun RBDA for projects including the Igbojaiye dam. While the Igbojaiye dam was again not constructed, only 16 per cent of the other 105 rural water projects were done.

The construction of the dam finally commenced in August 2009, after officials have pocket a large portion of the funds released for the project.

The ministry's refusal to provide relevant information and documents by the FMWR and its parastatals continued till 2010. This was reflected in the 2008 report which was concluded in 2010 by the M&E team (Premium Times, 2012).

This shows a lot of urge amount of money that goes into the hands of people that never be used for its purposes. This happened with the use of traditional method of project monitoring system.

Project Monitoring System

Project monitoring is about transforming vision into reality, an integrated application that covers execution processes in a holistic manner. It facilitates effective project management and tracking of project completion status. Enables the proper planning, tracking and monitoring of work orders and provide visibility to various stake holders

Preventing Fraud by Construction Contractors

The good news for preventing fraud by construction contractors is that scrutiny in several key areas can help reduce the risk of fraud by construction contractors. The areas include bidding, direct costs, indirect labor and equipment burden, and overhead (Jeffrey et al., 2011)

Conclusion

Every project that begins must have an end; the cloud-based technology has the necessary resources for organizations or project owners to access and control the rate of fraud in project execution. This will enhance the organization with the advantages of efficiency, timely completion of project, identify area of fraud and cost saving.

Recommendations

In view of the numerous advantages associated with the use of cloud-based fraud control in project monitoring, the following recommendations were made:

- To ensure and protect integrity of files transfer
- The organization or contract owners should prevent the contractors access to the vital page files
- IT personnel should ensure effective network services at the remote sit
- Enforce service level agreement with the sit IT operator
- Fraud awareness and penalty agreement should reach before awarding project.

References

Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud and Abuse: 2013 Global Fraud Study, http://www.acfe.com/rttn.aspx

Bassam S. (2013): Can a Professional project management stop project Fraud? At http://www.globalknowledge.com.sa/about-us/Knowledge_Center/Article/Professional-Project-Management/ accessed Dec 2013

Chartered Institute of Loss Adjusters, Construction Fraud, http://www.cila.co.uk/files/Construction/ConstructionFraudbyNeilMillerEDITED.pdf

Chris W., 2013 at www.constructionIndustryNews.net; accessed December 2013

City of London, "Code of Practice for Deconstruction and Construction Sites, accessed 20http://www.cityoflondon.gov.uk/business/environmental-health/environmental-protection/Documents/Code%20of%20Practice%206th%20Ed.pdf the of May 213

Dialogic ;2013, a White paper on Introduction to Cloud Computing; Montreal, Quebec, Canada at www.dialogic.com, accessed Dec, 2013

Efraudprevention 2013, Stay safe in the Cloud, at www.efraudprevention.net accessed January, 2014

Global Construction Perspectives and Oxford Economics, Global Construction 2025, http://www.globalconstruction2025.com

Gordon R. (2013): "How to Tell if You're in a Cloud-Friendly Industry; at www. aconex.com/blogs/2013/11/construction-in-the-cloud; accessed January,2014

Jeffrey N. A, Joel K. B, Ann R. C (2011): Preventing Fraud by Construction Contractors; WHITE PAPER 1; at http://www.horne-llp.com/media/168400/white%20paper%20preventing%20fraud_final; accessed January, 2014

Raja S. (2009): Globaljet Monitoring System, Indian Centre for Social Transformation; at www.gpmswiki.org accessed Dec. 2013

Premium Times June 27 2012: [Investigation]: The Massive MDG Fraud (2): How Nigeria's Water Minister Steals Billions, then leave the Tap dry: from Premium Times News Paper; at www.premiumtimes.com accessed Jan. 2014.

Thorvald W. (2013): Cloud Computing for Noise Monitoring, Gunersbratan Lierskogan, Noway ; at www.norsonic.com/.../PDF.../Cloudcomputingfornoisemonitoring.pd accessed Dec2013

Tod Bottar (2013): Construction Project Fraud: Alarming Statistics and Preventative Measure; at http://www.aconex.com/blogs/2013/11/construction-project-fraud-statistics-prevention.html accessed Dec. 2013