Smart Banking Using IoT

Rani S. Lande
Computer Science & Engineering Department
Prof Ram Meghe College of Engineering and Management, Badnera
Amravati, India
rani.lande@prmceam.ac.in

Susmita A. Meshram
Electronics & Telecommunication Department
Prof Ram Meghe College of Engineering and Management, Badnera
Amravati, India
susmita.meshram@prmceam.ac.in

Pranita P. Deshmukh
Computer Science & Engineering Department
Prof Ram Meghe Institute of Technology and Research, Badnera
Amravati, India
ppadeshmukh@mitra.ac.in

***Abstract*—Today, everything is associated, wireless, or being wired up. The change in ordinary working models is demand of changing time. The expanded utilization of gadgets and web by clients has prompted an expansion in IoT information. IoT change lives and changes the way business is attempted. The paper presents use and significance of IoT in banking and financial Sector. Banks need to convert IoT information into profitable data and thus increase their market share and provide better services to the clients. This study endeavours to cover issues such as banking frauds and early detection of fraud using IoT**.

Keywords— ***Big Data, Financial Services, Cloud, Internet of Things, Data Mining.***

I. Introduction

In recent years, instances of financial fraud have regularly been reported in India. Although banking frauds in India have regularly been treated as cost of doing business, post liberalization the frequency, complexity and cost of banking frauds have extended manifold resulting in a very extreme motive of subject for regulators, including the Reserve Bank of India (RBI). RBI, the regulator of banks in India, defines fraud as “A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank”[1].

In the last three years, Public Sector Banks (PSBs) in India have lost a total of Rs. 22,743 crore, resulting from various banking frauds [1]. With various measures initiated through the RBI, numbers of banking fraud cases have declined, but amount of money lost has increased in these years. Prima facie, an initial research in these instances has discovered involvement of not handiest midlevel employees, however additionally of the senior most management has become reflected in the case of Syndicate Bank and Indian Bank. Prima facie, an initial research this increases serious situation over the effectiveness of company governance at the best echelons of these banks. In addition, there has been a rising trend of Non-Performing Assets (NPAs), especially for the PSBs, thereby critically impacting their profitability. Several causes have been attributed to risky NPAs, consisting of worldwide and domestic slow down, however there is some evidence of a relationship between frauds and NPAs as well.

The robustness of a country’s banking and financial system helps determine its production and consumption of products and services. It is an instantaneous indicator of the well-being and living standards of its citizens. Therefore, if the banking system is plagued with excessive levels of NPAs then it is a motive of worry, because it reflects financial distress of borrower clients, or inefficiencies in transmission mechanisms. Indian financial system suffers to a first rate extent from those issues, and this served as the prime motivation for us to carry out this particular examine of frauds in the Indian banking system and analyzing, controlling frauds from unique angles.

The Internet of Things (IoT) has officially moved beyond hype. IoT is now widely known and defined - basically putting data-gathering sensors on machines, products and people, and making the data available on the Internet - and companies are already using IoT to drive upgrades in operational performance, customer experience and product pricing. Gartner predicts 25 billion IoT data-gathering endpoints hooked up international by 2020.

While IoT is delivering on its promise in a wide range of industries, many bankers are still struggling to find the value in finance, an enterprise in large part constructed on intangibles. We see two primary IoT opportunities for banks:

- Direct use of sensor data (location, activities, habits) to better engage customers and assess creditworthiness.

- Partnering with companies that manufacture or integrate sensors into merchandise to provide payment services for device-initiated transactions.

A. Internet of Things

“The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.”

An entire IoT system integrates four distinct components: sensors/devices, connectivity, data processing, and a user interface. Below briefly explain each component and what it does.

1) Sensors/Devices

First, sensors or devices acquire data from their environment. This could be as simple as a temperature analyzing or as complicated as a complete video feed.

978-1-5386-2599-6/18/$31.00 ©2018 IEEE

“Sensors/Devices,” due to the fact more than one sensors may be bundled collectively or sensors can be part of a device that does extra than just sense things. For example, phone is a device that has more than one sensors (digicam, accelerometer, GPS, and so forth), but phone isn't always only a sensor.

However, whether it’s a standalone sensor or a full device, in this first step data is being collected from the environment through something.

2) Connectivity

Next, that data is sent to the cloud, but it needs a way to get there!

The sensors/devices can be connected to the cloud through an expansion of strategies which includes: mobile, satellite, WiFi, Bluetooth, low-power wide-area networks (LPWAN), or connecting directly to the internet via ethernet.

Each option has tradeoffs between power consumption, range and bandwidth [6]. Choosing which connectivity option is best comes down to the particular IoT application, but all of them accomplish the same task: getting data to the cloud.

3) Data Processing

Once the information gets to the cloud, software program performs a few form of processing on it.

This could be quite simple, consisting of checking that the temperature reading is within an acceptable range. Or it can additionally be very complicated, which includes the usage of, such as using computer vision on video to identify objects (such as intruders in house).

But what happens when the temperature is too high or if there may be an intruder in your house? That’s where the user comes in.

4) User Interface

Next, the information is made useful to the end-user in some way. This could be via an alert to the user (electronic mail, text, notification, and so forth). For example, a text alert when the temperature is too excessive in the company’s cold storage.

Also, a user might have an interface that allows them to proactively take a look at in on the system. For example, a user might want to check the video feeds in their residence via a phone app or a web browser.

However, it’s not always a one-way street. Depending on the IoT application, the user may also be capable to perform an action and have an affect the system. For example, the user might remotely adjust the temperature in the cold storage through an app on their phone.

And some actions are performed automatically. Rather than waiting for you to adjust the temperature, the system could do it automatically via predefined rules. And rather than just call you to alert you of an intruder, the IoT system could also automatically notify relevant authorities.

How an IoT System Actually Works: An IoT system consists of sensors/devices which “communicate” to the cloud through some kind of connectivity. Once the data receives to the cloud, software processes it and then might decide to perform an action, such as sending an alert or automatically adjusting the sensors/devices without the need for the user.

But if the user input is needed or if the user simply wants to check in on the system, a user interface allows them to accomplish that. Any adjustments or actions that the user makes are then sent in the opposite direction through the system: from the user interface, to the cloud, and back to the sensors/devices to make some kind of change.

Data retrieving, analysis e-management is usually known as complex task in financial contexts. In an Internet of Things (IoT) system data-flow processes represent the knowledge base used in mathematical models for credits and financial products. IoT frameworks are very suitable to this kind of contexts for several reasons, in particular:

i) The diffusion of sophisticated tools (smart phones, tablets and smart watches);

ii) The possibility of real time data; ii) efficient communication models among devices. As it concerns the point

There are some common models:

a) Device-to-Device Communications, i.e. two or more devices that directly connect and communicate between one another;

b) Device-to-Cloud Communications, where the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic;

c) Device-to-Gateway Model, where there is an application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation.

One of the main opened problems related to IoT systems is a derivative effect, i.e. many financial transactions are based on information from intangible sources and only indirectly form real objects (for this reason, scientists research new methods for the improving of IoT sensors and the analysis of the their data).

B. Internet of Things in Banking

The Bank is a place that implies very excessive degree protection. In day to day life every person are concerned in banking transaction. Banks have been investing heavily in IoT technologies. Financial institutions have an average IoT banking budget of $117.4 million, about 0.4% of the revenue. Banks have always been quick in adapting new technologies. They have realized the potential of IoT banking in providing unimaginable levels of data and customer insights. IoT banking helps provide tailor-made services to customers, extend suggestions and latest offers on a regular basis, based on their transaction trends. By developing applications with IoT banking to estimate month-end balances for customers, analyze spending patterns and provide savings, investment and financial planning suggestions.

C. Big Data

Over the last few years, we have seen a plethora of Internet of Things (IoT) solutions, products and services, making their way into the industry's market-place. All such solution will capture a huge amount of data touching on the surroundings, as well as their users. The objective of the IoT is to learn more and to serve better the system users. Some of these solutions may additionally store the statistics on the devices (‘things’), and others may store in the Cloud. The actual cost of gathering information comes through facts processing and aggregation in huge-scale where new knowledge can be extracted. However, such procedures can also lead to user privacy issues.

The Internet of Things (IoT) [12] is a network of networks, in which, typically, a large range of objects/things/sensors/devices are connected through the information and communications infrastructure to provide value-added services. The IoT permits people and things to be connected Anytime, Anyplace, with Anything and Anyone, preferably using Any path/network and Any service. It is predicted that, by 2020, there will be 50 to 100 billion devices connected to the Internet [10]. These devices will generate Big Data [11] that desires to be analyzed for knowledge extraction. Even though data collected by individual devices may not provide sufficient information, aggregated data from number of physical devices and virtual sensors (e.g. social media such as Facebook, Twitter) can provide a wealth of knowledge for essential application areas including disaster management, customer sentiment analysis, smart cities, and bio-surveillance.

There is no clear definition for Big Data [11]. It is defined based on a number of its characteristics. The big data does not mean the size. There are three characteristics that can be used to define big data, as also known as 3V’s: volume, variety, and velocity. Volume relates to size of the data such as terabytes (TB), petabytes (PB), zettabytes (ZB), etc. Variety means the types of data. In addition, difference sources will produce big data such as sensors, devices, social networks, the web, mobile phones, etc. Velocity means how frequently the data is generated (e.g. every millisecond, second, minute, hour, day, week, month, year).

Creating Knowledge and Big Data: In an IoT world there will exists a vast amount of raw data being continuously gathered. It might be vital to develop techniques that convert these raw facts into usable knowledge. For instance, in the medical area, raw streams of sensor values must be converted into semantically meaningful activities performed by or about a person who includes eating, poor respiration, or exhibiting signs of depression. Main challenges for information interpretation and the formation of knowledge include addressing noisy, physical world data and developing new inference techniques that do not suffer the limitations of Bayesian or Dempster-Shafer schemes. These barriers include the need to recognize a priori probabilities and the cost of computations. Rule based systems may be used, but may also be too ad hoc for few applications.

The amount of collected data will be enormous. It may be predicted that a very large number of real-time sensor data streams will exist, that it will be common for a given stream of data to be used in many different ways for many different inference purposes, that the data provenance and how it was processed must be known, and that privacy and security must be applied. Data mining techniques are expected to provide the creation of important knowledge from all this data. Enabling streams to act as primitives for unexpected future inferences is an interesting research problem. In addition, the overall system solution must deal with the fact that no inference method is 100% correct. Consequently, uncertainty in interpreted data can easily cause users not to trust the system.

Trust is one vital component of the usefulness of big data. Security and privacy are essential elements of trust and these are discussed in their own sections. However, as a basis for trust it is also necessary to develop new in-field sensor calibration techniques and reliable transport protocols. Without these basic underlying system-level capabilities further inference might be operating with wrong or too much missing data, resulting in wrong conclusions. If these wrong conclusions drive actuators then serious safety problems can occur. One approach is to ensure that all inferred information is accompanied by a confidence level in the form of a probability that the information is correct or incorrect and use that information to guarantee safe actuator operation. In many applications, informing users how information was derived is necessary. Another principal mission is making good (control) decisions using the created knowledge. However, in making decisions it is necessary to minimize the number of false negatives and false positives and guarantee safety; otherwise the system will be dismissed as unreliable.

Many IoT applications will be designed to work for a particular person. It is important to perform correct data association making sure that the collected data and subsequent inferences are associated with the correct individual or individuals. This is a very challenging problem for many situations. When users are wearing RFIDs or when cameras with pattern recognition are used then the problem is solved (except for the privacy issues). However, in many other situations it will be necessary to combine a set of current sensor readings with a trace of the recent past readings and utilize a history of a given user’s activities and personal characteristics to arrive at an accurate data assignment. More research is necessary on this problem.

The paper is organized as follows: Section 1 discuss about the introduction of IOT and Big Data. Section 2, gives a details review of the focus of the paper. Section 3 talks about the materials and the methods to implement the proposed systems. Section 4 the conclusion.

II. LITERATURE REVIEW

As per the RBI, bank frauds can be classified into three broad categories: deposit related frauds, advances related frauds and services related frauds.

Deposit related frauds, which used to be significant in terms of numbers but not in size, have come down significantly in recent years, owing to a new system of payment, and introduction of cheque truncation system (CTS) by commercial banks, use of electronic transfer of fund, etc. Advances related fraud continue to be a major challenge in terms of amount involved (nearly 67 percent of total amount involved in frauds over last 4 years), posing a direct threat to the financial stability of banks. With ever-increasing use of technology in the banking system, cyber frauds have proliferated and are becoming even more sophisticated in terms of use of novel methods. Also, documentary credit (letter of credit) related frauds have surfaced causing a grave concern due to their implications on trade and related activities.

To maintain uniformity in fraud reporting, frauds have been classified by RBI based on their types and provisions of the Indian penal code, and reporting guidelines have been set for those according to RBI (2014a and 2015a).

Towards monitoring of frauds by the board of directors, a circular was issued as per RBI (2015b) to cooperative banks to set up a committee to oversee internal inspection and auditing, and plan on appropriate preventive actions, followed by review of efficacy of those actions. Impartial policy guidelines and whistle-blower policy are vital to empower employees to handle frauds.

RBI also issued a circular and introduced the concept of red flagged account (RFA), based on the presence of early warning signals (EWS), into the current framework, for early detection and prevention of frauds.

Gandhi (2014) discussed the prime causes of growing NPAs and recognized the absence of robust credit appraisal system, inefficient supervision post credit disbursal, and ineffective recovery mechanism as key barriers addressing those aspects.

Gandhi (2015) stressed on the basic principles that can go a long way in preventing fraud, namely the principles of knowing the customer and employees as well as partners. He also pointed out the significance of a robust appraisal mechanism and continuous monitoring. A. Motivation

One of the recommendations is suggested from many authors for an early detection of frauds.

Use of latest technology: The data collection mechanism in banks is very archaic and needs a revision. The banks should employ the best available IT systems and data analytics that allows to make sure effective implementation of the red flagged account (RFA) and early warning signals (EWS) framework advised by the RBI, which would help in a better profiling of customers by analyzing patterns of their transactions and rendering a near real time monitoring possible for banks. Also, the authors recommend that the Institute for Development and Research in Banking Technology (IDRBT) could consider incentivizing development of relevant software for commercial banks at affordable costs. This is vital to enhance their tracking and monitoring of suspicious and fraudulent transactions within the branches of their banks.

Internet, a innovative invention, is usually transforming into a few new type of hardware and software making it unavoidable for everybody. The form of communication that available now is either human-human or human-device, but the Internet of Things (IoT) promises a great future for the internet where the type of communication is machine-machine (M2M).

IoT is always evolving and is a hot research topic where opportunities are infinite.

III. METHODOLOGY

Banks are considering how Big Data could probably rework what they offer to customers and their relationship with them. This is named as “Bank of Things” and on this new global it is in all likelihood that banks will need to become the trusted:

• Custodian of the customer Data – supporting to control privacy and control sharing

• “Infomediary” – acting as an adviser between the customer and sellers

• Payments supervisor for the customer’s “matters”.

People now have the possibility to carry out a number of banking features with the assist of ATM machines and on-line / mobile banking applications. This has reduced the strain on financial institution employees as they ought to address fewer customers and might cognizance on different similarly important processes.

Most of the banking operations may be completed by customers with the help of Smartphone’s. ATMs can also be used to collect withdrawal and banking facts for all areas and higher selections for enhancement of offerings can be made extra judiciously.

A IoT solutions help to track customer data across a plethora of devices. This data may be used to discover their spending habits and specifics about withdrawals and deposits. This information may be used by banks to tweak pricing and reward programs of credit / debit cards and different services in order that they may be able to optimize their profits whilst making the customer feel more comfortable with their policies.

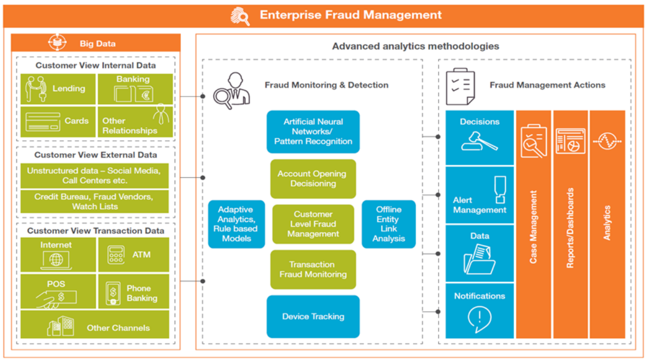
Enterprise Fraud Management
Big Data
Customer View Internal Data
Lending
Banking
Cards
Other Relationships
Customer View External Data
Unstructured data – Social Media, Call Centers etc.
Credit Bureau, Fraud Vendors, Watch Lists
Customer View Transaction Data
Internet
ATM
POS
Phone Banking
Other Channels
Advanced analytics methodologies
Fraud Monitoring & Detection
Artificial Neural Networks/ Pattern Recognition
Account Opening Decisioning
Adaptive Analytics, Rule based Models
Customer Level Fraud Management
Offline Entity Link Analysis
Transaction Fraud Monitoring
Device Tracking
Fraud Management Actions
Decisions
Alert Management
Data
Notifications
Case Management
Reports/Dashboards
Analytics

Fig: Enterprise Fraud Management

IV. CONCLUSION

The frauds may be primarily due to lack of adequate supervision of top management, defective incentive mechanism in place for employees; collusion between the staff, corporate borrowers and third party agencies; weak regulatory system; lack of appropriate tools and technologies in place to detect early warning signals of a fraud; lack of expertise of bank employees and customers; and lack of coordination among different banks across India and abroad.

The delays in legal procedures for reporting, and various loopholes in system have been considered some of the main motives of frauds and NPAs.

This paper has taken initial step towards use of IoT for early detection of frauds.

REFERENCES

[1] Charan Singh and Ravi kant et al. Mar-2016. Frauds in the Indian Banking Industry. IIMB WP-505.

[2] Capgemini -Fraud Solutions for Financial Services

[3] Govinda K. and Saravanaguru R.A.K. 2016 Review on IoT Technologies. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 4 pp 2848-2853.

[4] Mr. Lokesh M. Giripunje and Suchita Sudke et. al Nov-2017 International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887 Volume 5 Issue XI.

[5] Salvatore Cuomo and Federica Sica et. al , 2017. Analysis of a data-flow in a Financial IoT System, The 2nd International Workshop on Data Mining in IoT Syatems(DaMIS2017).

[6] https://www.iotforall.com/connecting-the-internet-of-things

[7] https://www.bankdirector.com/index.php/issues/technology/can-bank-tap-internet-things/

[8] Charith Perera (Australian National University) and Rajiv Ranjan (CSIRO Digital Productivity Flagship) et. al. Privacy of Big Data in the Internet of Things Era

[9] D. McAuley, R. Mortier and J. Goulding, “The Dataware manifesto,” in Communication Systems and Networks (COMSNETS), 2011 Third International Conference on, 2011.

[10] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos,2013. “Context Aware Computing for The Internet of Things: A Survey,” Communications Surveys Tutorials, IEEE, vol. 16, no. 1, pp. 414-454.

[11] A. Zaslavsky, C. Perera and D. Georgakopoulos,2012. “Sensing as a Service and Big Data,” in International Conference on Advances in Cloud Computing (ACC-2012), Bangalore, India.

[12] L. Atzori, A. Iera and G. Morabito, oct-2010. “The Internet of Things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787-2805.