Electronic Financial Fraud: Abstract, Definitions, Vulnerabilities, Issues and Causes

In financial systems, data undergoes many phases of processing such as retrieving phase, data analysis and management phase, decision making and reporting phase, making the data flow very comprehensive and complicated. Financial decisions are directly affected by offer and demand information which is relayed through gateways from numerous intangible sources or sensors distributed all over the financial universe. The communication of this information is generally defined as follows: unicast (one to one), multicast (many to many) and broadcast (one to many) generating massive amounts of heterogeneous data dumped in huge databases, the security of which is defined by 3 basic categories: data itself, storage of data and the access of data.

Nowadays intangible sources of data, distributed sensors and gateways are titled as IoT which is defined as the interconnection of any device that communicates any type of digital data. IoT is facing an obvious and critical challenge in the area of security and privacy. The explosion of IoT devices needs security to respond to this huge phenomenon growth. Financial world has to take in consideration the evolution of the dark malicious side claiming AI and machine learning. The main goal of organizations is to increase production and maximize profit which can be achieved with IoT, but IoT provides EASEABILITY (ease of use) but not FEASABILITY (authenticity and security in other words) more speed loss security. The enormous amount of raw unprocessed heterogeneous data retrieved from IoT sensor can have a vast impact on many domains in firms especially on the world of finance.

By the year 2020, the number of IoT devices is expected to be 25 billion, a lot of which will be processing very sensitive data including financial. Along with the rapid growth of IoT application and devices, cyber-attacks will also be improved and pose a more serious threat to security and privacy than ever before. The major attacks in IoT for the year 2020 are expected to be as follows:

- IoT authentication
- IoT encryption
- IoT PKI
- IoT security analytics
- IoT API security

In future research papers we will conduct more detailed in-depth study of the anatomy of each of these attack profiles to determine a possible algorithm of these attacks evolution.

Our goal is to establish some type of a smart system to guess and predict future attack profiles… Behavior based analogy. Since malicious code is implementing AI and machine learning, it is too hard to establish an ever-mutating signature of attack.

Electronic Finance, Fraud, Internet of Things IoT, Intrusion Detection/Prevention Systems IDS & IPS, Machine Learning, Deep Learning, Artificial Intelligence, Digital Signature, Digital Profile.
1. INTRODUCTION

The communication of information system is generally defined as follows:

1. Unicast which is a device to device communication as in Client-Server or Server to Server

2. Multicast where multiple communication occurs between multiple devices simultaneously, as in multi-distributed partial financial database backups to and from various locations (Wall Street, stock options)

3. Broadcast which is one to all as in corporate higher management updates broadcasted to all remote distributed branches.

In finance, as a general concept the price is defined by offer and demand, now imagine that this offer and demand information is relayed through gateways from numerous intangible sources or sensors distributed all over the financial universe.

In financial systems, data flow is usually very comprehensive and complicated, where data under goes many phases of processing and as general concept:

1) Retrieving phase: typically, and in ideal situation data is homogenously analyzed, processed stored and retrieved from one source. Nowadays with the IoT, massive blocks of heterogeneous data from distributed sensors are relayed through gateways, remote databases lastly to the main database for analysis processing and reporting.

2) Data analysis and management: as mentioned before huge blocks of heterogeneous data is retrieved, transferred and stored in different databases which creates huge obstacles for direct data processing and analysis. This forced financial institutions to implement different technologies to sort, filter, process, store, and manage these huge blocks. As an example, financial organizations use SQL Management Studio, SAS, and MySQL and complicated MIS. When it comes to MIS solutions financial institutions should use branded software form well known technologies to avoid bugs in Open Source programs that could lead to huge losses.

3) Decision making and reporting these models are implemented to make smart decisions based on the processed and analyzed data subsequently reporting to an external institution or to another department.

2. BIG DATA AND SECURITY

As such, we can divide the "big data security" into 3 basic categories: the data itself, the storage of the data, and the access to the data.

In terms of the data itself, we're typically asking: where is the data coming from? Sometimes it's IoT, other times it's not. This largely depends on the individual case scenarios. In any case, we need to make sure the data sources can deliver efficiently with a reliable uptime (disruptive attack prevention).

In addition, we need to ensure that the data communication occurs on a secure layer. For instance, how is the communication between the data source and the data processing taking place? What type of encryption system is used? How is edge verification handled? Etc...

Next, the data storage. Here we typically ask not only where the data stored is stored, but also how is the data parsed and stored. Does the data exist on a single edge node, or is it replicated across multiple hosts (such as cloud-based solutions, for instance) Is it possible that the data is exposed, by accident or by design, through incorrect storage? Is the data itself encrypted at any level? How are the security keys handled and stored? What kind of safeguards are installed to prevent data loss? Is physical security being addressed?

Finally, data access. The raw big data is rarely (if never) used as-is. There always has to be some logic code in-between the data itself and the end-user (dashboards, toolsets, etc...). The primary question here becomes one of authentication and authorization (noticing the distinction between the two). How is the communication between the end-user application and the raw data handled? Do end-users have access to non-regulated data? Is authorization properly handled as a distinct entity that authentication? Obviously, we can go into infinitely more details on each aspect, but this is a big-picture outline.

3. IOT AND FINANCE

As discussed above we can define IoT as the interconnection of any device that communicate any types of digital data which includes but not limited to digital service providers, clients requesting these services, gateways and distributed sensors used in weather, volcano, oceans ..., home appliances, GPS systems, portable smart devices and the count goes on and on. REF [1].

As a matter of fact, IoT is not a new concept, Human Machine interfacing has been a very dependent source of evolution, one may wonder how dependent our evolution has become on technology specifically IoT, self-driving cars and geospatial cell phones neither less we say about supply chain management.
as discussed previously in details of financial of data flow.

According to Val Srinivas; REF [1], "an obvious and critical challenge that the IoT industry is likely to face is in the area of security and privacy. With the explosion of devices, cybersecurity takes on a whole new dimension – not just for institutions but also for consumers Digital vulnerabilities are likely to expand exponentially".

The question now is how to respond to this huge phenomenon growth. IoT is already implemented in various fields like insurance in monitoring driver behavior, health and homeowners insurance and worker’s compensation in the commercial arena needless to mention how vital IoT is in banking and financial organizations.

Another some applications are distributed to monitor and take action on the consumer’s behalf are ATMs, credit/debit card and information in bank branches. The connection of financial services such as checking credit card or investment accounts to one or more household devices is a significant prospect which may be achieved.

The IoT technologies are serving banks functions, insurance companies and investment management shops through efficient and effective applications.

Cybersecurity may become a huge defying because of the deluge of new data is likely to tangle data management for financial services company and also innovations are not free of risks. Exponential growth of IoT is leading to inevitable dependence on it.

There is hardly any doubt that this growth and dependence will result in numerous vulnerabilities that have to be seriously addressed since the desire of organizations to increase production and profit while trying to handle the enormous amount of raw unprocessed heterogeneous data being retrieved from IoT sensors. Again back to rule of three thumbs more speed less security back in 2016, such disasters occurred when Mirai attack was launched against the backbone of the internet which could have been targeted at a global financial firms like Wall Street, Wells Fargo, etc... I don’t think we can even imagine the impact of such event on the world finance. When it comes to cybercrime and security, such organized crime has become so powerful as far as terrorism or state global weapon of mass distraction...STUX net.

The universe has to keep up with all of this evolution of the dark side taking in consideration the Artificial intelligence (AI), the machine learning (ML), and deep learning (DL) aspects, the speech here could be about petabytes \(1,125,899,906,842,624 \text{ bytes}\) of raw data being retrieved from the galaxy. Speaking of the devil, malicious code has evolved to concur AI and machine learning and it going to take an arm and a leg to keep up with it.

4. THE INTIMATE RELATIONSHIP BETWEEN FINANCE, IOT AND FRAUD

While the world is turning digital, everything is expressed with 0-1, these binaries are invading homes, sooner than banks, military, industry, manufacturing and space. For few understand what security is and how easy to this world can be compromised.

While IoT can be used to ease our existence, it can be abused too. Unfortunately, the focus in the development of IoT technologies tends to go towards the EASEABILITY (ease of use) rather than the FEASEABILITY (authentication and security), more speed less security. Due to the hunger for the profit, these IoT devices are massively produced with very low to no security, in other words to ease the process of communication and data transmission. Which definitely resulted in a massive vulnerable data architecture that made life so easy for malicious code to spread and nest in these devices, the simplest example of which the DDOS “Mirai” attack.

By the year 2020, by the estimates of Gartner 2018 REF [2], there should be close to 25 billion IoT devices a lot of which will be processing very sensitive data including financial.

IoT even has its own search engine that allows consumers to determine where and how IoT products are being used which allows a typical hacker to do the same instead though search for network and device vulnerabilities to exploit, thus leading to the theft and abuse of sensitive information therefore fraud. And that’s why the search engine Shodan was considered by many an easy tool set for hackers to exploit these vulnerabilities.

According to the research done by Anna Fedorova published Wednesday October 17 2018 REF [3], the evolution of financial fraud in the UK forced the financial industry to search for solutions for these dilemmas by using biometrics and artificial intelligence. The latest data released by UK finance REF [4], indicates that customers of UK banks lost more than 500 million by stealing them in the first six months of 2018.

This loss was due to unauthorized financial transactions and authorized push payment scams.

Authorized fraud is usually done by social engineering tactics such as telephone, email, text messages and precisely social media. The statistics of authorized fraud indicates that there are new
advanced methods which make the fraudulent activity hard to impossible detect and prevent.

Also, authorized payment scams become dangerous since the customers cannot have legal protection to reimburse their losses.

The principal fraud strategy consultant at ACI Worldwide, Jay Floyd REF [5], indicates that the capability of banking industry must stop the fraud threat which is evolving also he adds that financial institutions can pre-empt and prevent fraud before a transaction happens by using overlay service like “Confirmation of payee”.

Floyd REF [5] says that industries in the UK make efforts to solve these problems by facilitating the cross-check between the account details and realize certainty for the payer; to provide a high level of inactivity of certainty to the payer some countries implement proxy databases. Unfortunately, as will be shown further that those solutions are not sufficient to detect and prevent advanced fraud methodologies.

Raising awareness and staying safe were included in the industry response, to develop an industry code for the reimbursement of scam victims a payment system regulator has been formed with the Home Office and the Consumer groups to steer them. To help firms acting more proactively on suspicion of fraud and deter criminals from accessing financial systems; never the less, that was not sufficient.

5. FRAUD DETECTION VS. BEST PRACTICES

Fraud detection is considered as a key area of focus including established rapid response scheme banking protocol, which allows branch staff to alert police and trade standards to dubious fraud happened. To improve customer security, financial companies are employing other digital innovations such as two factor authentication. IP filtering (Kyriba: treasury management tech firm) which make the client able to restrict login to selected IP addresses. As well as digital solutions like Swift’s 3 key REF [6].

Biometric technologies for customer authentication are one of the crucial fields of security that industry is making progress in it by focusing on fraud detection.

According to Ricky Knox, Tandem Money Ricky Knox, CEO of challenger bank Tandey Money, to secure customer accounts biometric authentication alternatives (facial recognition, fingerprint Scanner) are the great way.

Some financial firms allow their customers to access via biometric authentication like the challenger bank which offers all its services through a banking app as “Ricky Knox” said.

Also, to identify if the users are managing their accounts by themselves, they analyze the usage of user’s app across a range of data points. Briefly, these are behavioral biometric solutions. World of hacking is so huge, so financial firms must protect their systems and databases.

Many financial companies are going to artificial intelligence techniques to develop effective and innovative ways to detect and prevent fraud.

According to Mark Gazit, CEO of cybersecurity firm Theta Ray, banks whose using AI-powered threat detection systems are able to speedily analyze huge amounts of data, control on going transactions permanently and identify fraud when it’s happening or even before; While in an era, when cyber/financial crime powered by AI was considered as same as traditional crime banks were unable to lean on old ways to identify suspected behavior, because criminals can make their crimes like legitimate transactions.

To help financial organizations detect suspicious activities before happening and to prevent financial fraud including money laundering Theta Ray offers a self-learning program “machine learning”.

According to Imam Hoque who is the chief product officer at big data analytics firm Quantexa, AI technology can construe and interpret wide data sets to derive actionable intelligence.

AI helps to connect data sets together, to create a more precise image of accounts kept and binding activity together.

To process more data than a human, to make predictions, to enable decisions to be made rightly and 24/7, all these are missions of machine learning.

To tackle financial fraud and decrease risk in financial industry we should bring data together, analyze it and use it to gain insights.

Hackers did not stop at Shodan, they incorporated AI, ML and DL to further the intelligence of their malicious code.

Machine learning algorithms watch hacker’s behavior and adopt to their evolving tactics and vice-versa. Top ISPs and various global service providers including google, Microsoft, Amazon are nowadays incorporating advanced AI, ML and DL technologies to adapt and self-educate the new ever evolving malicious code. The past static defense with “rule-based” policies cannot keep up with that smart malicious code especially when we are talking about petabytes of retrieved data as mentioned above.
hence manual work is not match and out of the question.

It is not about post-detection of malicious event anymore rather than analyzing massive data to detect suspicious activity before it accures.

We will never be able to fully stop malware and prevent it from compromising our data structure but we know for a fact that with AI, ML and DL we are building smarter systems to even detect how malicious code may mutate.

Speaking of mutation malicious code can be nowadays defined as follows: WORM, a smart computer worm as usually know consist of five modules/components:

The main module/payload which is the malicious portion of the worm that is intended to destroy/manipulate data. CMC/command and control the portion of the worm hackers use to communicate with infected hosts and to manage activities and operations. Anti-detection, the portion that hides / masquerades the malicious signature/identify of the malicious payload to evade detection by anti-viruses, firewalls. Propagation, the portion that works on scanning, neighboring hosts in the network where the infected device resides to spread and infect the network. Update, the portion of the code responsible for mutating the worm if any signature has been found and flagged.

The problem with static defense was very often the denial of legitimate user’s services they should be able to access due to the fact that those filtering rules were based on source location of request.

AI, ML and DL implemented in new majors can now depend on dynamic rules of detect and differentiate legitimate from illegitimate based on digital characteristics of the users activity.

Digital characteristics are an essential part of building the digital profile about the user. Some other aspects of this profile are personal references, locations, operating systems used, user agents, digital certificates, public encryption keys, cookies, behavior like speed of typing, search preferences and interests, usually identified by add-ware plugins widely used by major service providers, Google, Yahoo, Amazon, Hotmail...Etc. According to Margaret Rous (ref), digital profiling is used in marketing, enterprise security, criminal justice and recruitment, among other areas.

Our goal is to produce and maintain self-updating, self-learning solution that can keep up with hackers intelligence, learn their mentality and even possible ways of thinking...stay at least, one step ahead of them. This is where implementing powerful honeypots with up to date vulnerabilities to analyze the actions of intruders and may be somehow understand their behaviors and establish their digital profile.

The essence of the digital profile and e-behavior is to teach our smart solution to detect an impostor (identity thief) even after a successful authentication by monitoring and analyzing their actions and comparing it against the already established profile of the legitimate owner of that account which may include even the length of the session, type of data acquired, user agent, its sensitivity level if the current source of session is suspicious as unknown proxy server or a hop of known malicious origins. (Note: IDS, IPS)

Our journey to the destined solution is long and hard, since it should constantly evolve by producing smart decisions based on the vast volume of ongoing acquired data hence the bigger the digital profile is the smarter and more accurate the decision will be.

Never the less, hackers, offensive AI, ML and DL probably can produce patterns that could really undergo our solution analysis and still look legit.

6. CONCLUSION AND PROPOSED SOLUTION

As a conclusion, this research is targeted at designing a unique solution that will implement both: IDS/IPS to detect any known patterns/signatures of malicious nature and suspicious activities.

Strict Biometric Authentication Solution with Deep Learning capabilities to build a profound legitimate digital user profile with various mentioned patterns to compare against any patterns of pre-established malicious ones.

Biometrics can certainly include various combinations of face recognition, retina/iris scan, finger print, etc.

Such patterns may include, upon necessity, source IP/MAC addresses, user agent (or a specific mobile/PC application with pre-defined hash value based on combination of user’s Biometrics and hardware Physical Information like CPU Serial Number, MAC address, etc.), geolocation, digital behavior as in speed keyboard strokes, mouse clicks, cursor movement, and length of the session, type of data acquired, its sensitivity level, and current source of session if suspicious as known proxy servers or a hop of known malicious origins.

The next step will be to complete the design and setup of the proposed solution based on open source technology, to implement the billed as a one stop-shop: gateway/proxy/hub that will simultaneously provide IDS/IPS.
It is worth to make a point that we are not trying to reinvent the wheel, but as we spent numerous hours with reviewing best practices in modern technologies, we found that these services are mainly stand-alone solutions offered separately and never in one solution. Now let’s imagine a financial institution where customers need to remotely connect and manage their accounts online, security and privacy would be a major concern here with the well-known attacks in this domain, attacks like man in the middle attack MITM, or identity theft through spoofing, spear phishing and pharming, replay attacks, session hijacking, even cryptography attacks and the count goes on and on.

Outsourcing complicated services in modern world is very common while financial institutions like banks, insurance, trade companies mainly specialize in finance operations, accounting, auditing and unless they invest millions of dollars in full time security operations, departments with fully dedicated squads and costly ongoing training they will not be able to keep up with the ever evolving malicious activities and attacks. Here’s our suggestion, our solution will be able to offer these institutions a service where the solution, as a cloud service accessible from anywhere.

7. REFERENCES

The “Internet of Things” and the Financial Services industry, Val Srinivas, Banking&Securities research leader, Deloitte Services, on January 22, 2014. (references)

ACFE (Association of Certified fraud examiners). Financial firms tackle fraud with AI and biometrics, Anna Federova on Wednesday, October 17, 2018

