

Analysis on Fraud Detection for Internet Service

Tae Kyung Kim¹, Hyung Jin Lim² and Jae Hoon Nah³

¹*Dept. Liberal Art, Seoul Theological Univ.
101 Sosabon2-dong, Sosa-gu, Bucheon-City, Kyonggi, Korea*

²*Financial Security Agency
143, Uisadang-daero, Youngdeungpo-gu, Seoul, Korea*

³*Electronics and Telecommunications Research Institute
Gajeong-ro, Yuseong-gu, Daejeon, Korea*

¹*tkkim@stu.ac.kr, ²hjlilim@fsa.or.kr, ³jhnah@etri.re.kr*

Abstract

In this paper, we proposed the model which can support fraud detection in ICT application service. Fraud detection service monitors and analyzes user activity and behavior at the application level (rather than at the system, database or network level) and watches what transpires inside and across accounts, using any channel available to a user. It also analyzes behavior among related users, accounts or other entities, looking for organized criminal activity, corruption or misuse. This model can be used in e-banking, e-payment, e-government and enterprise remote access, etc.

Keywords: *Fraud Detection, Monitoring, Measurement*

1. Introduction

Online banking and e-commerce have been experiencing rapid growth over the past few years and show tremendous promise of growth even in the future [1]. Many fraudsters and malicious users are able to commit their crimes by opening new online accounts at unsuspecting enterprises by illegitimately taking over customer accounts and posing as those customers, or by conducting high-risk (e.g., involving high-monetary-value or highly sensitive information) transactions using stolen payment account information[2]. By accessing and using relatively basic information, a criminal can take over existing financial accounts (existing card fraud or existing non-card fraud) or use a victim's personal information to create new accounts (new account fraud). A criminal can commit identity fraud numerous ways, including making an unauthorized withdrawal of funds from an account or making fraudulent purchases with a credit card and creating new accounts (e.g., banking, telephone, utility, loans).

Aside from e-financial service, malware-based attacks have been responsible for targeted attacks in many types of companies and vertical industries. They are becoming a major concern and are increasingly delivered through targeted spear-phishing e-mails and through malware-infected objects like advertisements that unknowing users click on. For example, these methods were used to infect multiple organizations.

Organizations in many commercial and government sectors face significant risks of data loss, inappropriate account access, and inappropriate transaction activity from external and internal sources. Targeted malware can often bypass existing protection technologies, and the resulting data breaches are not detected until a long time has passed and significant data exfiltration has occurred. The evidence of malicious activity is usually hiding in plain sight,

and is undetected because of a lack of monitoring capability and an inability to discern a pattern of abnormal application activity or data access from normal activity patterns. Also, in case of bank customer may not even know that a fraud has been committed until users see an account that you did not open on user's credit report, or until a debt collector contacts you for payment[3].

Malware-based attacks against bank customers and company employees are levying severe reputational and financial damage on their victims. They are fast becoming a prevalent tool for attacking customer and corporate accounts, and stealing sensitive information or funds. Therefore, unless it makes business processes and organization are properly structured to effectively manage fraud detection systems, important alarms and alerts could be ignored. Finally, it can be used to take over user accounts, or to perpetrate fraud or theft of server-based assets.

In Chapter 2 measurement architecture for fraud detection is described. Monitoring architecture, detection architecture and response architecture are showed in Chapter 3,4 and 5. Finally, Chapter 6 concludes this paper.

2. Measurement architecture for fraud detection

When it comes to comprehensively counteract identity fraud, it fraud prevention required requires to a three-part approach to addressing this problem: prevention monitoring, detection and incident response. These measures include steps to take in order to prevent find suspicious activity fraud from happened various event data in the first place; actions to detect frauds earlier in the event that it happens; and what to do to resolve fraud if suspicious activities were detected user become a victim.

2.1. Monitoring

It can monitor fraud by looking for anomalies in user activity and behavior at the application level, as well as the system, database or network level, and watches what transpires inside and across accounts using any channel available to a user. It also monitors and analyzes user or account behavior and associated transactions and identifies anomalous behavior, using rules or statistical models. It may also use continuously updated profiles of users and accounts, as well as peer groups for comparing transactions and identifying the suspect ones.

2.2. Detection

It also requires the detection capability to mine, dissect and analyze large volumes of data using complex relationship and rule screening, defined by the business, to prevent fraud[4]. It can be used for insider fraud detection and external fraud detection. For fraud detection capability support, it can and should profile various entities, such as users, accounts, households, PCs, mobile handsets and kiosks, to spot abnormal transaction behavior from that entity. Fraud detection uses rule-based policies that are based on human judgment and knowledge and/or predictive mathematical models to score the likelihood of fraud for a given transaction.

2.3. Response

After incidents have occurred, it must make various precaution activities and response of suspicious activities and incident alerts. A variety of complementary monitoring and detection

technologies can help enterprises better detect suspicious user activity; recognize patterns of inappropriate resource access or fraudulent account activity.

2.4. Architecture considerations

Implementing fraud detection system for ICT applications can be considered using one of three architectures:

Fraud-detection modules built into the application server (e.g. Web), Listening and/or monitoring of the online application, and Programmatic interfaces into the legacy application. Business rules and processes are more important determinants of an application's effectiveness.

- A fraud-detection module sitting inside the application server

Rules maintained by the enterprise are applied by the filter to any HTTP request (for example, login or payment) before the transaction hits the application. Transactions can be stopped and/or redirected to a transaction-verification routine in real time through execution of the module's fraud rules. Several vendors provide plug-ins to application servers is directly embedded with a preprocessor.

- Listening and/or monitoring of the ICT application (listening mode)

In this mode, the application listens to or "sniffs" input files or HTTP network traffic (for example, log), or reads data using application server plug-ins installed at each server. Data is read in real-time (network "sniffer" approach) or near real (application server listener approach) and either fed to another fraud-management application or reconstructed into a format on which fraud rules can be applied. In the latter case, suspect transactions are queued for fraud analyst follow up. Customized application programming interfaces (APIs) can be integrated so that transactions are redirected to challenge/response verification.

- Programmatic interfaces into the legacy application (inline integration mode)

In this case, APIs are used to pass all transactions through fraud detection before a transaction is processed. Transaction flow is controlled, so a user can be challenged in real time if a suspect transaction is detected. Changes in business rules require changes to the core application. APIs are mainly based on Web services. APIs also make it harder to switch vendor specific solutions.

Generally, using APIs for fraud detection gives enterprises/organization direct control over transaction flow, but requires significant integration work, and must be constantly updated when the core application changes. Application servers which require not intervening real time in user transactions will prefer the second approach, which is the easiest to pull out and replace.

3. Monitoring architecture

Monitoring capability establishes user and data context is needed for early attack and breach detection, and enables data access and activity monitoring. Privileged user and sensitive data access monitoring is also a common requirement for compliance reporting.

It needs to implement security information and event management to gain broad-scope monitoring of user activity and resource access across the network, systems, databases and applications, and augment event data with context about users, assets,

threats and vulnerabilities to improve the effectiveness of security monitoring for breach detection. Also, It needs to selectively augment general security monitoring with additional capabilities such as advanced threat monitoring, based on the level of risk and capability to implement and effectively operate the fraud detection and response system.

Fraud detection system also collects event data in near real time in a way that enables immediate analysis. Real-time monitoring capability is important for threat management to track and analyze the progression of an attack across components and systems and for user activity monitoring to track and analyze the activity of a user across applications, or to track and analyze a series of related transactions or data access events. Also, real-time monitoring capability should support batch data collection for cases where real-time collection is not practical or is not needed.

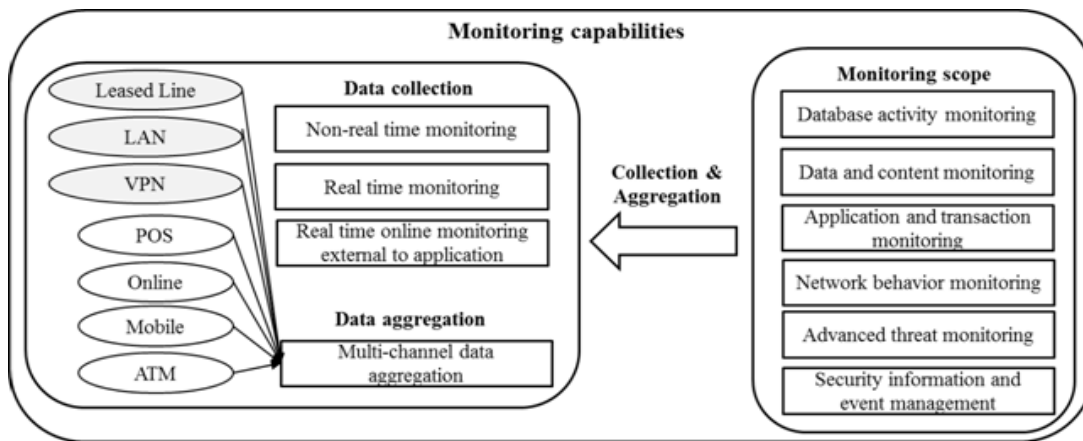


Figure 1. Monitoring Capabilities of Fraud Detection System

3.1. Data aggregation and collection

Data aggregation and collection are supported for a wide variety of log data sources, including network and security devices; server, database and application logs; the output of security-relevant applications, such as vulnerability assessment and database activity monitors; and the output of relevant identity and access management technologies, such as enterprise directories, user provisioning and access management systems.

- Non-Real time monitoring

It requires manual or automated reviewing of log files. Non-real time monitoring may provide rapid deployment option for post-transaction analysis with longer clearance periods and can remove ability to stop transactions at point of completion. It should support batch data collection for cases where real-time collection is not practical or is not needed.

- Real time monitoring

It is to monitor all transactions (*e.g.*, http) in real time using a web server filter. This function could monitor without additional hardware using a low impact web server filter. It's possible to implement no application changes required to see any real-time transaction data. Real Time online monitoring external to application function: It is to monitor all HTTP web transactions in real time via internal application integration. This function could consume cost

and time intensive to deploy and maintain because it needs extensive application modification to monitor specific transaction points.

- Real time online monitoring external to application

It is to monitor all HTTP Web transactions in real time via external application. This function has no impact to application for sniffer and Web filter approach but application filter is inline to application, which may introduce risk to application reliability. It's possible to implement no application changes required to see any real-time transaction data.

- Multi-channel data aggregation

This means that transaction data from other channels can be fully incorporated in the monitoring and fraud detection process. It also looks for suspect user or account behavior, but it also offers the benefit of looking across channels and products and correlating alerts and activities for each user, account or entity. It enables the analysis of relationships among internal and/or external entities and their attributes (for example, users, accounts, account attributes, machines and machine attributes) to detect organized or collusive criminal activities or misuse.

3.2. Data source

Fraud detection system can detect malicious activity in a constant stream of discrete events that are usually associated with an authorized user and are generated from multiple network, system and application sources. Monitoring capabilities include integration with multiple sources to obtain suspicious and incident events.

- Data and content monitoring

The capabilities are often used to limit information leaks, such as credit card numbers, personally identifiable information, and document- or database-based intellectual property, including function through content monitoring function and filtering and data loss prevention (DLP) function.

Content monitoring and filtering are used to protect content in motion (through network monitoring or filtering), at rest (via storage scanning) and in use (through endpoint agents). Most functions also include capabilities to scan stored content on the network for policy violations (for example, a credit card number on an unapproved server), finding violations of corporate policies around the appropriate use of content and data.

DLP tools can discover, monitor and actively block the movement or access to sensitive data by using content inspection and contextual analysis techniques to apply one or more policies at the time of use. DLP is limited by an organization's ability to define sensitive content, its structures or other identifying characteristics.

Although these functions are extremely useful in limiting accidental exposure or those caused by bad business processes, there are many non-monitored activities that can be used by a malicious attacker or insider (such as camera phones, voice mail, paper and pen) to circumvent content-aware solutions.

- Application and transaction monitoring

Monitoring capability includes application monitoring because application weaknesses are frequently exploited in targeted attacks, and abnormal application activity may be the only signal of a successful breach or of fraudulent activity. The ability to parse activity streams from packaged applications enables application-layer monitoring for those components, and

the ability to define and parse activity streams for custom applications enables application-layer monitoring for in-house developed applications.

The capability also watches for suspect user activity in an application within a given access channel (for example, Web, phone or in-person, or across applications, access channels) or even organizations such as where "black lists" of bad IP addresses are shared across organizations. This can range from detecting abnormal access (for example, simultaneous access by one device from two disparate geographic locations) to a suspect transaction sequence (for example, a change in address followed by a high-value money transfer). By default, it can also spot unauthorized employee activities if done in an application that is monitored by the fraud detection application.

- Network behavior monitoring

The capability provides visibility into network operations based on traffic flows between systems, including source, destination, port, protocol, volume of data exchanged and user identity. The capability has applicability for security- and operations-related analysis. Also, the capability uses a combination of signature and anomaly detection to provide visibility into the state of the network and to identify deviations from baselines, which may indicate abnormal or suspicious behavior.

Security use cases include monitoring to detect the spread of worms, the unauthorized installation of applications and suspicious system access activity. Operation use cases include capacity planning and traffic analysis, including the capability to bind a user ID to traffic flow, or to address auditor requirements to track user access to critical systems. The capability has little visibility beyond Layer 3, so it can't directly detect system, database, content, file system or other object access issues.

4. Detection architecture

Fraud detection uses background server-based processes — transparent to users — that examine user access and behavior. It then compares this information to a profile of what's expected and considered "normal." It simultaneously evaluates a combination of risk factors to surface real fraud and keep false detection rates low. Suspect user transactions are re-verified in real time to assess their legitimacy or are suspended until fraud analysts have time to research their legitimacy.

Since fraud detection operates in the context of an application, it cannot detect rogue and potentially fraudulent processes that are external to the application. Fraud detection also cannot detect suspect behavior that is not defined to its engine because the rules are not aware of the activity pattern, the model has not learned enough to single it out or the application integration is not providing enough relevant data to the fraud risk assessment engine. To be effective detection, the analysis requires embedded knowledge for specific use cases, or the customer needs to provide this knowledge in the form of customized correlation rules and reports. Therefore, fraud detection system needs capabilities such as fraud pattern update, pre-defined rule library support, and real time rule processing.

Most capabilities require extensive model tuning, profile tuning or rule development before the applications are fully functional. These capabilities include monitoring all transactions, automated risk analysis and risk rating, user behavior profiling and learning, application service specific- and intelligent-fraud decision, cross-channel risk assessment.

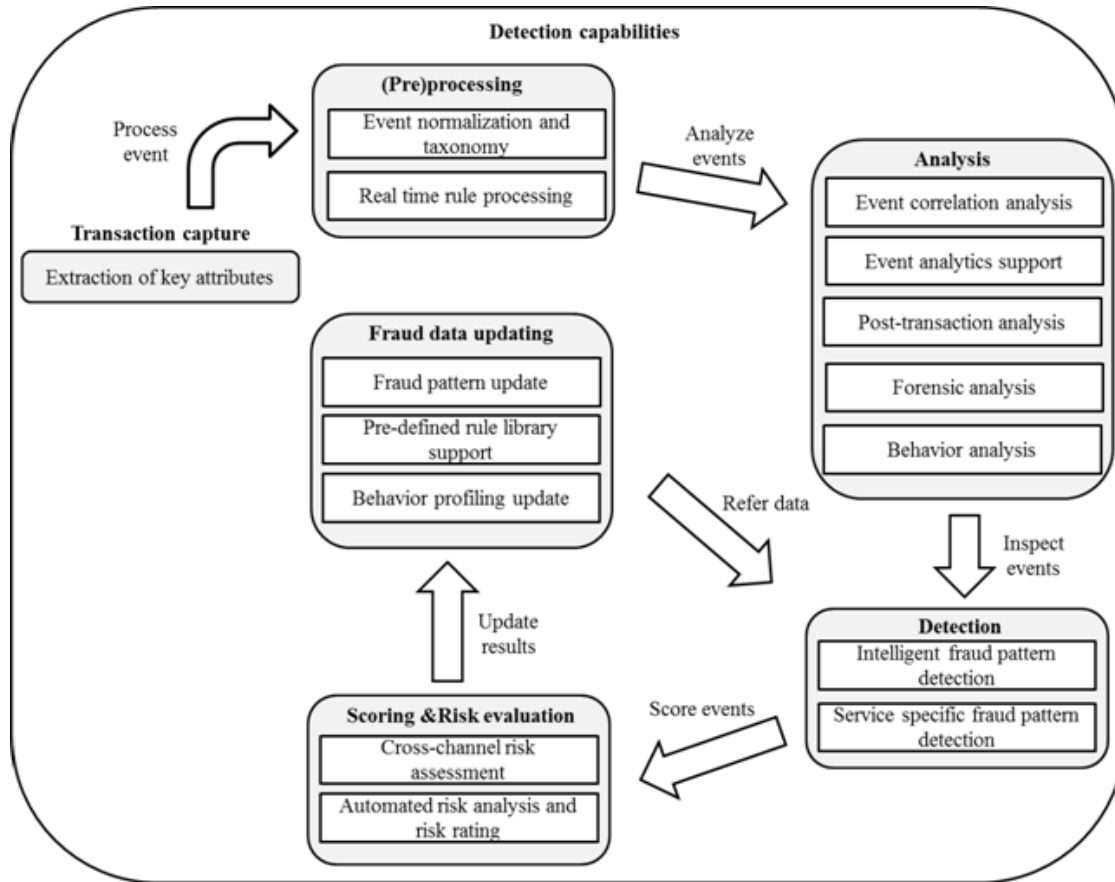
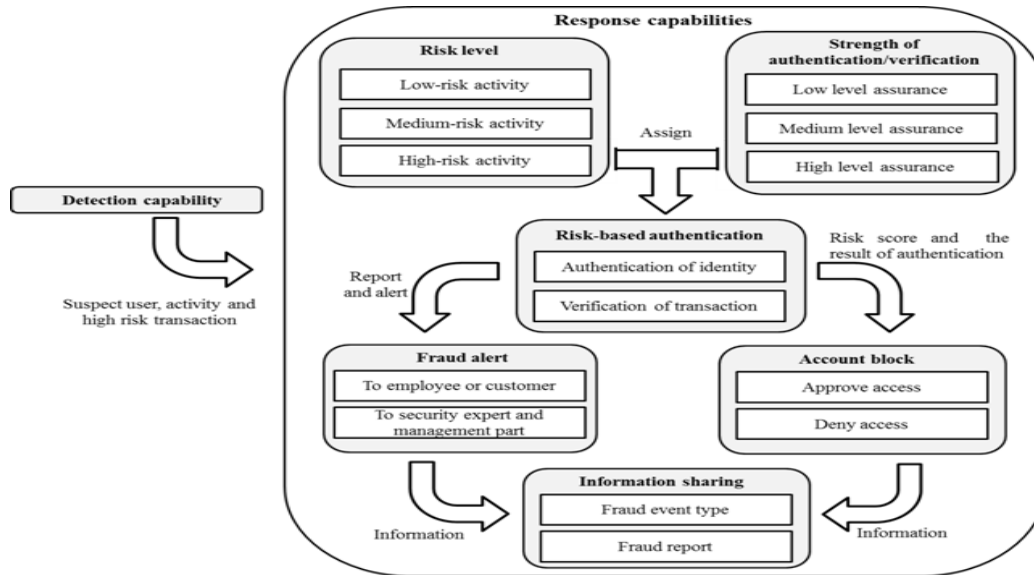


Figure 2. Detection Capabilities of Fraud Detection System

5. Response architecture

Fraud detection system requires automotive triggering fraud alerts, account block, stepped-up applicant verification of a particular transaction that has been tagged as suspect for incident response. All online account applications or high-risk anonymous transactions should go through a set of initial screening procedures, starting with authentication events as the result of the initial identity-proofing procedure to the application usage and application logs. The initial screening procedure includes basic fraud detection, such as client device identification and verification of basic identity data, such as name, email address, geo-location analysis, telephone number validation, credit card fraud detection, credit bureau report validation and/or identity scoring.

The suspect transactions that don't pass the initial identity-proofing steps, should be routed to a fraud investigation team, and queued for manual or automated additional screening. Then, fraud detection system can use a risk-based and layered identity-proofing approach that steps up the identity vetting if suspect users and high-risk transactions are prompted, for additional screening.



- Risk-based authentication

The higher the risk, as determined, for example, by a fraud detection system, the more costly and inconvenient to the customer the identity-proofing measures are required. Several approaches are available when more authentications are needed.

- Fraud alerts

Fraud alert is typically the result of a combination of a risk score and some rules that act on that score. Detailed alerts include transaction attributes and activity description and could be notified via email, pager configurable by rule, severity, admin user. Fraud alerts could be sent to security expert or customer/user according to measured risk level. Then, the security expert could investigate the perceived risk in more detail, while fraud alert to the customer/user can use to alert potential lenders that their identity may have been stolen.

- Account block

Account block is applied to user accounts when suspicious activity detected. The user can be approved or denied access based on the assigned score and the institution's tolerance limits. Users who do not score adequately to warrant full access can be allowed limited access or be required to provide more authentications to gain full access or be permitted to perform certain high-risk transactions. In case of not satisfied, the user can re-started stepped verification procedure or blocked promptly.

- Information sharing

Fraud detection system should ensure that they effectively coordinate portions of their incident response activities with appropriate partners of organization. Information sharing can take place directly between enterprise and customers or between organization and employee because the same threats and attacks often affect multiple organizations or services simultaneously.

The most important aspect of incident response coordination is information sharing, where different organizations share threat, attack, and vulnerability information with each other so that each organization's knowledge benefits the other. The purpose of information sharing is

to enable any organization that has detected fraud to share this information, either internally or with other potential victim organizations.

6. Conclusions

Recently many fraud detection techniques involving sophisticated screening of transactions to tracking customer behavior and spending patterns are being deployed by both banks as well as merchant companies. Some of the techniques include Address Verification Systems (AVS), Card Verification Method (CVS), Personal Identification Number (PIN), Rule-based systems and Biometrics. Effective internet fraud detection applies controls at the front end, through stronger authentication, and at the back end, through cross-industry, multichannel behavior-pattern recognition. This requires participation and data sharing across industries and service providers, and will be the primary challenge for successful implementations.

There is currently no standard for fraud detection system. Therefore, we suggested the fraud detection model. This model can be helpful to protect fraud activities in internet environments.

Acknowledgements

This research was supported by the ICT Standardization program of MISP(The Ministry of Science, ICT & Future Planning).

References

- [1] J. T. S. Quah and M. Sriganesh, "Real Time Credit Card Fraud Detection using Computational Intelligence", *Expert Systems with Applications*, vol. 35, no. 4, (2008) November.
- [2] B. Zhang, Y. Zhou, C. Faloutsos, "Toward a Comprehensive Model in Internet Auction Fraud Detection", *Proceedings of the 41st Hawaii International Conference on System Sciences*, (2008).
- [3] L. Delamaire, H. Abdou and J. Pointon, "Credit card fraud and detection techniques: a review", *Banks and Bank Systems*, vol. 4, no. 2, (2009).
- [4] K. B. Bignell, "Authentication in an Internet Banking Environment; Towards Developing a Strategy for Fraud Detection", *International Conference on Internet Surveillance and Protection*, (2006).

Authors



Tae Kyung Kim

1997 : Dankook University, Korea (BS in mathematics education)
2001 : Sungkyunkwan University, Korea (MS in Computer Science)
2005 : Sungkyunkwan University, Korea (PhD in Computer Science)
2008 - Present : Seoul Theological University, Korea (Professor)
Research interests: Network Security, Network QoS, Cloud Computing, and COP



Hyung-Jin Lim

1998 : Hallym University, Korea (BS in Computer Engineering)
2001 : Sungkyunkwan University, Korea (MS in Computer Science)
2006 : Sungkyunkwan University, Korea (PhD in Computer Science)
2007 - Present : Financial Security Agency, Korea (Senior Researcher)
Research interests : ID management, Multi-factor Authentication and financial information security



Jae Hoon Nah

1985 : Chung-Ang University, Korea (BS in Computer Science)

1987 : Chung-Ang University, Korea (MS in Computer Science)

2005 : HANKUK University of Foreign Studies, Korea (PhD in Computer Science)

1987 - Present : Electronics and Telecommunications Research Institute, Korea (Senior Researcher)

Research interests: IPv6/MIPv6, P2P, IPTV, and Mashup Web Security