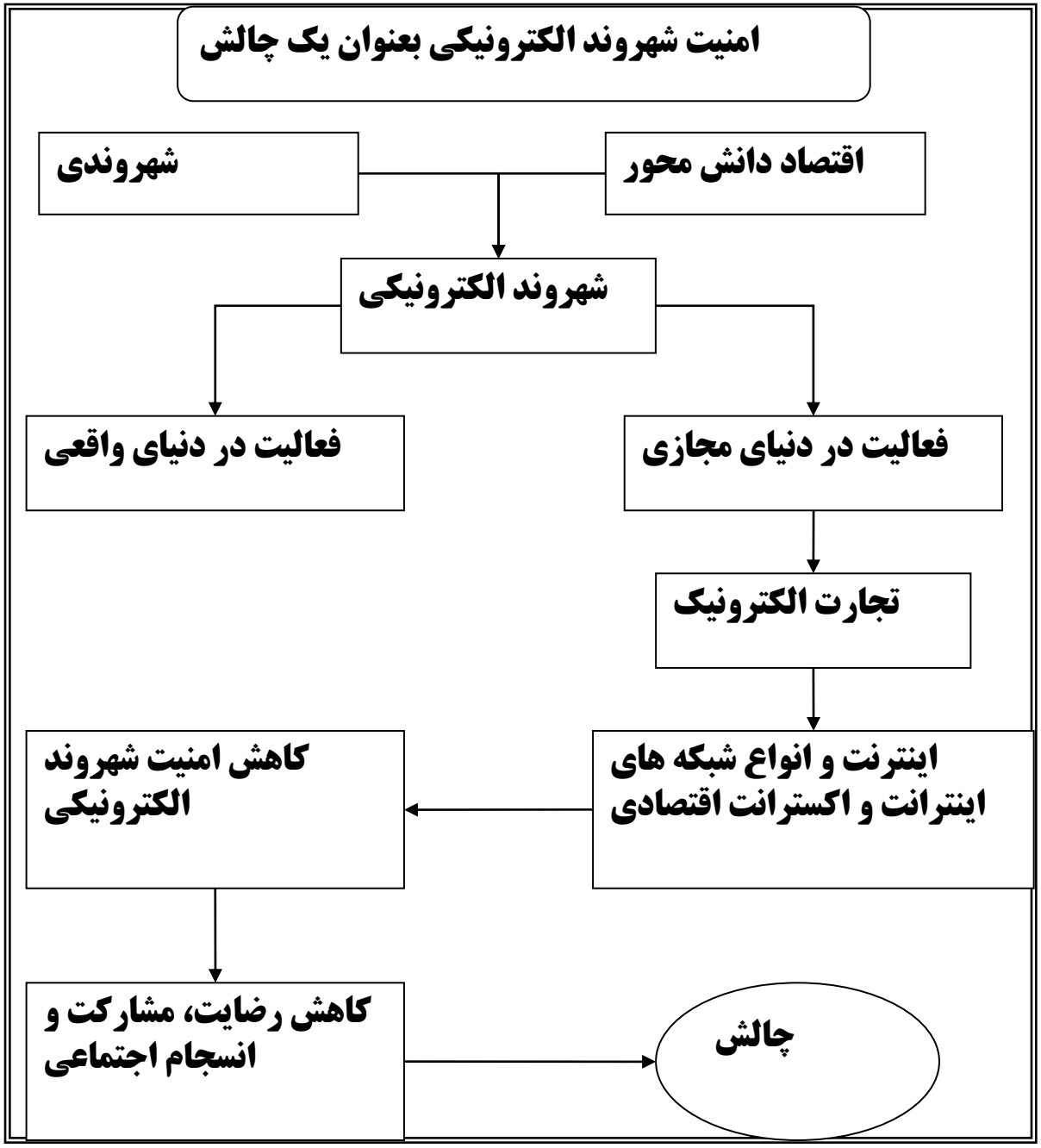
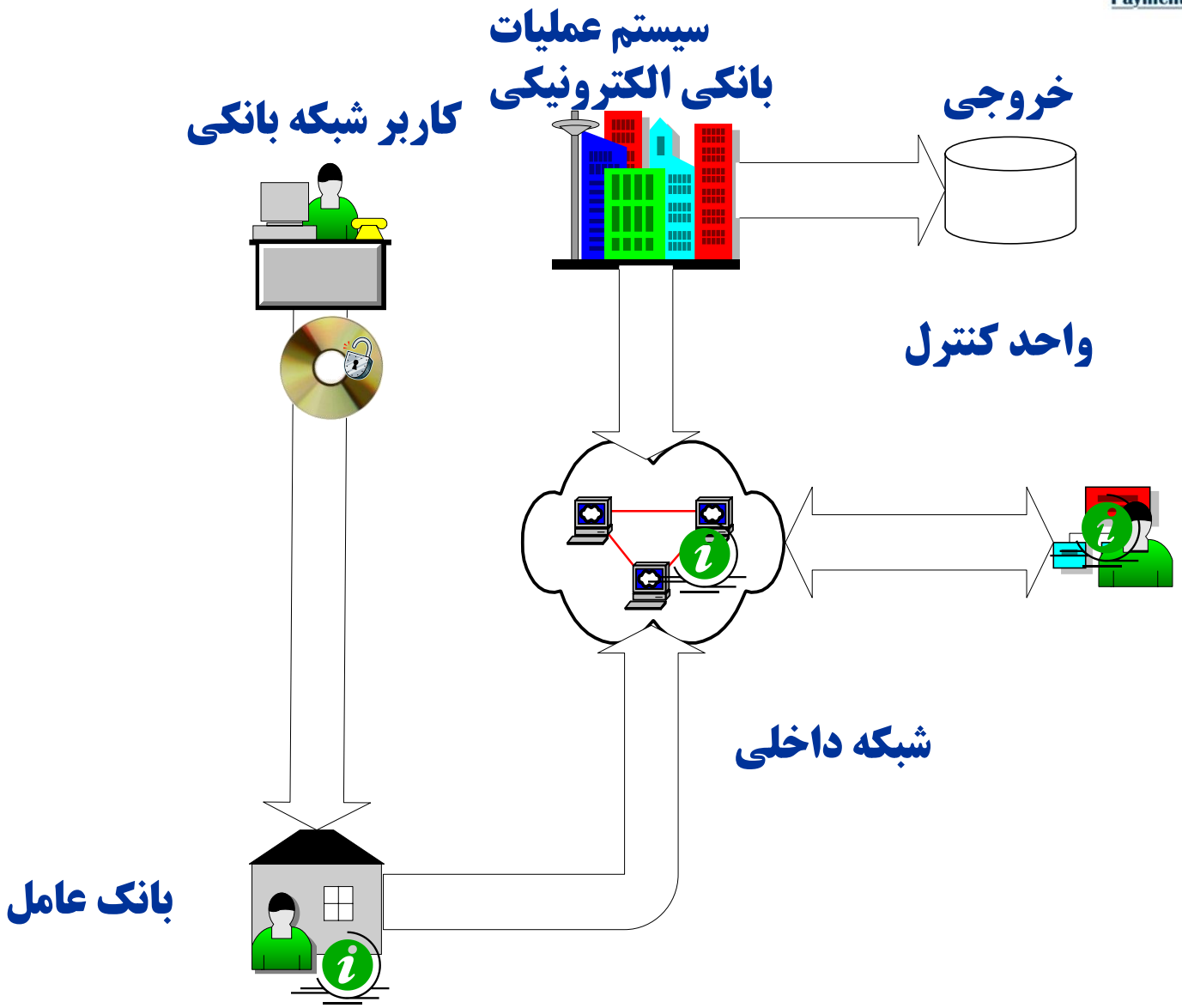
کاربرد مدل های تصادفی در برقراری امنیت اطلاعات بانکداری الکترونیک

افشین آشفته

بانک مرکزی جمهوری اسلامی ایران


امنیت شهروند الکترونیکی بعنوان یک چالش
شهروندی
اقتصاد دانش محور
شهروند الکترونیکی
فعالیت در دنیای واقعی
فعالیت در دنیای مجازی
تجارت الکترونیک
اینترنت و انواع شبکه های اینترانت و اکسترانت اقتصادی
کاهش امنیت شهروند الکترونیکی
کاهش رضایت، مشارکت و انسجام اجتماعی
چالش


سیستم عملیات بانکی الکترونیکی
کاربر شبکه بانکی
خروجی
واحد کنترل
شبکه داخلی
بانک عامل

امنیت اطلاعات در شبکه های اقتصادی

دو نوع اطلاعات در شبکه های رایانه ای موجود است:

- اطلاعات بازرسی رایانه Computer audit data (CAD) که مجموعه ای از رخدادهای حادث در ماشین میزبان را در برمی گیرد.
- اطلاعات ترافیکی شبکه که مربوط به بسته های اطلاعاتی در حال جابجایی در شبکه است و مربوط به ماشین میزبان می باشد.

- **روش شناخت امضا** (Signature recognition)
- **روش کشف عمل غیرمتعارف** (Anomaly detection)

مطالعات پایه ای روش کشف عمل غیر متعارف

۱۹۹۸: دبار و همکارانش، کاربردهای مولفه های شبکه عصبی

عدم کارایی کافی و به سرعت جایگزینی توسط روش های تلفیقی با روش های آماری

مطالعات پایه ای روش کشف عمل غیر متعارف

۱۹۹۸ و ۱۹۹۹ :در ابتدای بکارگیری
روشهای آماری، استفاده از تحلیل آماری
داده‌کاوی
توسط لی و استلفو

Data Mining

مطالعات پایه ای روش کشف عمل غیر متعارف

۲۰۰۱ : یی و همکاران، روش‌های یک‌متغیره ،
مانند آماره کای-مربع، حجم محاسباتی کم

روش های چند متغیره با حجم
محاسباتی بالا

روش های فرآیندهای تصادفی

مدل زنجیر مارکف

$$P(X_{n+1}=i_{n+1}|X_n=i_n,X_{n-1}=i_{n-1},\ldots,X_0=i_0)=P(X_{n+1}=i_{n+1}|X_n=i_n)$$

$$P(X_{n+1}=i_{n+1}|X_n=i_n)=P(X_{t+1}=j|X_t=i)=p_{ij}$$

$$P=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1s} \\ p_{21} & p_{22} & \cdots & p_{2s} \\ \vdots & \vdots & & \vdots \\ p_{s1} & p_{s2} & \cdots & p_{ss} \end{bmatrix}$$

$$Q=[q_1,q_2,\ldots,q_s] \qquad \sum_{j=1}^{s} p_{ij}=1$$

$$P(x_{n-T+1},\ldots,x_n) = q_{x_{n-T+1}} \prod_{t=1}^{T-1} p_{x_{n-t}x_{n-t+1}}$$

$$p_{ij} = \frac{N_{ij}}{N_i} \qquad q_i = \frac{N_i}{N}$$

مدل تصادفی مرتبه بالای جزیی

$$P(x_n, x_{n-1}, \ldots, x_0) = P(x_n | x_{n-1}, \ldots, x_0) P(x_{n-1} | x_{n-2}, \ldots, x_0) \ldots P(x_1 | x_0) P(x_0)$$

$$P(x_{n-T+1}, \ldots, x_{n-1}, x_n) = P(x_n | x_{n-1}, \ldots, x_{n-T+1}) \times$$

$$P(x_{n-1} | x_{n-2}, \ldots, x_{n-T+1}) \ldots P(x_{n-T+1})$$

مثال کاربردی

انتخاب زبان

پیت رمز

درخواست صورت حساب

درخواست وجه نقد

سیستم تحت نظارت ۱۰۰

درخواست

$$Q = [\, q_1, q_2, q_3, q_4 \,] = [1,0,0,0]$$

از ۱۰۰ نفر کاربری که در حال ثبت انتخاب زبان بوده-اند، ۳۰ نفر زبان مورد نظر خود را اشتباه انتخاب کرده و دوباره به مرحله انتخاب زبان برگشته اند و ۷۰ نفر به مرحله ثبت رمز وارد شده‌اند. بنابراین داریم

$$p_{11} = 0.3, p_{12} = 0.7, p_{13} = 0, p_{14} = 0$$

از ۱۰۰ نفری که در مرحله ورود رمز بوده‌اند در مرحله بعدی ۳۰ نفر رمز را اشتباه وارد کرده و دوباره سعی کرده، ۵۰ نفر درخواست صورت حساب داشته و ۲۰ نفر نیز درخواست وجه نقد را کرده‌اند

$$p_{21}=0, p_{22}=0.3, p_{23}=0.5, p_{14}=0.2$$

بعد از واقعه سوم یعنی درخواست صورت حساب، از ۱۰۰ نفر کاربر ۲۰ نفر مجدداً درخواست صورت حساب و ۸۰ نفر درخواست وجه نقد داشته‌اند

$$p_{31}=0, p_{32}=0, p_{33}=0.2, p_{34}=0.8$$

و بالاخره از ۱۰۰ نفری که درخواست وجه نقد را داشته‌اند در مرحله بعدی ۴۰ نفر درخواست صورت حساب و ۶۰ نفر درخواست وجه نقد را مجدداً ارسال داشته‌اند

$$p_{41}=0, p_{42}=0, p_{43}=0.4, p_{44}=0.6$$

$$P=\begin{bmatrix} 0.3 & 0.7^{@*} & 0 & 0 \\ 0 & 0.3 & 0.5 & 0.2 \\ 0 & 0 & 0.2 & 0.8 \\ 0 & 0 & 0.4 & 0.6 \end{bmatrix} \qquad P^{(2)}=P^{2}=\begin{bmatrix} 0.09 & 0.42 & 0.35 & 0.14 \\ 0.00 & 0.09^{*} & 0.33^{@} & 0.58 \\ 0.00 & 0.00 & 0.36 & 0.64 \\ 0.00 & 0.00 & 0.32 & 0.68 \end{bmatrix}$$

$$P^{(3)}=P^{3}=\begin{bmatrix} 0.027 & 0.189 & 0.336 & 0.448 \\ 0.000 & 0.027^{*} & 0.343 & 0.63 \\ 0.000 & 0.000 & 0.328 & 0.672^{@} \\ 0.000 & 0.000 & 0.336 & 0.664 \end{bmatrix}$$

$$P^{(4)}=P^{4}=\begin{bmatrix} 0.0081 & 0.0756 & 0.3409 & 0.5754 \\ 0.000 & 0.0081^{*} & 0.3341 & 0.6578 \\ 0.000 & 0.000 & 0.3344 & 0.6656 \\ 0.000 & 0.000 & 0.3328 & 0.6672^{@} \end{bmatrix}$$

$$P^{(5)}=P^{5}=\begin{bmatrix} 0.00243 & 0.02835 & 0.33614 & 0.63308 \\ 0.0000 & 0.00243^{*} & 0.33399 & 0.66358 \\ 0.0000 & 0.0000 & 0.33312 & 0.66688 \\ 0.0000 & 0.0000 & 0.33344^{@} & 0.66656 \end{bmatrix}$$

بنابراین طبق رفتار صحیح کاربران در زمان کنترل، احتمال اینکه یک کاربر، ابتدا یک بار انتخاب زبان و سپس پنج بار رمز را فراموش کرده باشد، برابر است با:

$$P(x_0, x_1, x_2, x_3, x_4, x_5) = q_{x_0} \prod_{t=1}^{5} p_{x_{5-t} x_{6-t}}$$

$$= 1 \times 0.7 \times 0.09 \times 0.027 \times 0.0081 \times 0.00243$$

$$= 0.000000$$

حال یک رفتار عادی را در نظر میگیریم. فرض کنیم کاربری ابتدا انتخاب زبان و سپس رمز را وارد کرده، صورت حساب را درخواست میکند. در مرحله چهارم و پنجم در خواست وجه نقد و در مرحله آخر درخواست صورت حساب را مینماید. بنابراین داریم:

$$P(x_0, x_1, x_2, x_3, x_4, x_5) = q_{x_0} \prod_{t=1}^{5} p_{x_{5-t} x_{6-t}}$$

$$= 1 \times 0.7 \times 0.33 \times 0.672 \times 0.6672 \times 0.33344$$

$$= 0.0345346$$

جمع بندی و نتیجه گیری

با توجه به مباحث فوق مشخص است که مدلهای تصادفی آماری به خوبی در بحث برقراری هوشمند امنیت شبکه های اقتصادی کارایی دارند و بطور گسترده مورد استفاده قرار می گیرند. در روشهای کشف نفوذهای خرابکارانه آماری، نیازی به وجود بانک اطلاعاتی حاوی شکلهای نفوذ شناخته شده مانند آنچه آنتی ویروس ها ،بر اساس روش شناخت امضاء، عمل می کنند نیست و این نوع سیستم های کشف عمل غیر متعارف، قابلیت آن را دارند که حملات کاملاً جدید را با مقایسه با رفتار عادی کاربران شناسایی و از نفوذ خرابکارانه جلوگیری کنند. البته در شبکه های کنونی از هر دو روش کشف عمل غیر متعارف و روش شناخت امضاء به عنوان مکمل یکدیگر استفاده می کنند و این کار علاوه بر بالا بردن اطمینان باعث می شود وقت سیستم امنیتی را جهت نفوذهای شناخته شده تلف نکنیم.

Debar H, Becker M, Siboni D. *A neural network component for an intrusion detection system.* Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, May 1992. IEEE Computer Society Press: Anaheim, CA, 1992; 240–250.

W. Lee, and S. J. Stolfo, *Data mining approaches for intrusion detection,* in Proc. 7th USENIX Security Symp. San Antonio, TX. Jan. 1998.

W. Lee, and S. J. Stolfo, and K. W. Mok, *A data mining framework for building intrusion detection models*, in Proc. Symp. Security Privacy, May 1999.

W. DuMouchel and M. Schonlau, *A comparison of test statistics for computer intrusion detection based on principal components regression of transition probabilities*, in Proc. 30th Symp. Interface: Comput. Sci. Stat.

Wespi A, Debar H, Dacier M, Nassehi M. *Fixed- vs. variable length patterns for detecting suspicious process behavior.* Journal of Computer Security 2000; 8: 159–181.

N. Ye, *A Markov chain model of temporal behavior for anomaly detection.* In Proc. IEEE SMC Inform. Assurance Security Workshop, West Point, NY, June 2000, pp. 166-169.

Ye N, Li X, Chen Q, Emran SM, Xu M. *Probabilistic techniques for intrusion detection based on computer audit data*. IEEE Transactions on Systems, Man, and Cybernetics 2001; 31(4):266-274.

Ye N, Chen Q. *An anomaly detection technique based on a chi-square statistics for detecting intrusions into information systems.* Quality and Reliability Engineering International 2001; 17(2):105-112.

Ju WH. Vardi Y. *A hybrid high-order Markov chain model for computer intrusion detection.* Technical Report No. 92, National Institute of Statistical Sciences. http://www.niss.org/downloadabletechreports.html.

S. L. Scott. *Detecting network intrusion using a Markov modulated nonhomogeneous poisson process*. [Online]. Available: http://www-rcf.use.edu/~sls/fraud.ps.

Ashofteh Afshin, *A new Nonparametric Reliability Measure for Computer Intrusion Detection,* International Conference on the Future of Statistical Theory, Practice and Education. (Indian School of Business, Hyderabad, ANDHRA PRADESH, India, December 29 - January 1, 2005)

Toffler, Alvin & Heidi, *Revolutionary Wealth*, 2005.

با آرزوی شادکامی برای کلیه حضار گرامی