یک رویکرد نظریه بازی برای قیمت‌گذاری رایانش ابری و تعیین سطح امنیت شرکت-های ارائه‌دهنده امنیت

مهدیه صادقیان [1]، مرتضی راستی برزکی [*2]، حسین خسروشاهی [3]

[1] دانشجوی کارشناسی ارشد، دانشکده مهندسی صنایع و سیستم ها، دانشگاه صنعتی اصفهان mahdie.sadeqian@in.iut.ac.ir

[2] استاد، دانشکده مهندسی صنایع و سیستم ها، دانشگاه صنعتی اصفهان rasti@cc.iut.ac.ir

[3] استادیار، دانشکده مهندسی صنایع و سیستم ها، دانشگاه صنعتی اصفهان khosroshahi@iut.ac.ir

چکیده

سخت‌افزارها ممکن است دچار خرابی‌های ناگهانی شوند و راه‌حل‌های نرم‌افزاری اغلب پرهزینه‌اند، بنابراین کاربران به محیطی نیاز دارند که بتوانند بدون نیاز به سخت‌افزار و نرم‌افزار گران‌قیمت، محاسبات و ذخیره‌سازی داده‌ها را انجام دهند. رایانش ابری این امکان را فراهم می‌کند، اما نگرانی‌هایی درباره امنیت داده‌ها در برابر حملات سایبری وجود دارد. شرکت‌های امنیتی با تعیین سطح امنیت و قیمت‌گذاری براساس ارزش اطلاعات و درصد بازیابی، می‌توانند از داده‌های کاربران محافظت کنند. آن‌ها می‌توانند استراتژی‌های متفاوتی مانند پیشگیری از حملات (ساختار رهبر) یا انتظار برای وقوع حمله و سپس مقابله (ساختار پیرو) را انتخاب کنند. در این مسئله این دو ساختار با حضور هکر کلاه سیاه بررسی شده است. نتایج نشان می‌دهد ساختار قدرت تأثیر زیادی بر مقدار قیمت ندارد اما سود را به‌شدت تحت تأثیر قرار می‌دهد. همچنین مشخص شد ارزش اطلاعات و کاهش اعتبار شرکت در اثر حمله موفق، به سود و میزان تقاضا تأثیر زیادی دارد.

کلمات کلیدی: قیمت‌گذاری، سرمایه‌گذاری، هکر کلاه سیاه، امنیت سایبری، نظریه بازی.

[*] نویسنده مسئول، ایران، اصفهان 84156-83111، دانشگاه صنعتی اصفهان، دانشکده مهندسی صنایع و سیستم‌ها

A Game-Theoretic Approach for Pricing Cloud Computing and Determining the Security Level of Security Provider Companies

Mahdie Sadeghian[1], Morteza Rasti-Barzoki[2], Hossein Khosroshahi[3]

[1] Master of science, Department of Industrial and Systems Engineering, Isfahan University of Technology, Isfahan 84156-83111, Iran

[2] Professor, Department of Industrial and Systems Engineering, Isfahan University of Technology, Isfahan 84156-83111, Iran

[3] Assistant Professor, Department of Industrial and Systems Engineering, Isfahan University of Technology, Isfahan 84156-83111, Iran

Abstract

Since hardware may experience sudden failure and software solutions are often costly, users need an environment to perform computational and data storage tasks without expensive hardware and software. Cloud computing can provide this capability, but the presence of cyber hackers and their attacks raise user concerns about their data security. As information is precious, losing it can result in significant costs for the information owner. To address this problem, companies have emerged to ensure the safety of cloud computing services, and cloud users can entrust their information security to them. This article aims to examine the competition between security provider companies and cyber hackers using game theory and determine the strategies of each player to determine the game structure. These structures are based on the leader's decision to determine the security level initially or after an attack has occurred. The company decides what price to offer the user based on the value of the information, the amount of effort needed to return the information after successful attack, the security level it needs to maintain and the power structure. Similarly, the hacker decides how much effort to put in based on the value of the information. The results show that the price decreases linearly based on the information value, when the company is the leader. In addition to the results obtained about the company's profit, it shows that in general, the company's profit, when it is a leader, is more than when it is a follower, and in particular, the company's profit based on the percentage of returned information in the leader's position is much higher than in the position of the follower. The level of security provided is also different according to the position of the company, and when the company is the leader, it is much higher than when the company is the follower, based on the hacker's credibility and the value of the returned information.

Keywords: Pricing, Investment, Black hat hacker, Cybersecurity, Game theory.

1- مقدمه

چاک رابینز[1]، مدیرعامل سیسکو، می‌گوید اگر جرایم سایبری به عنوان یک کشور در نظر گرفته شود، سومین اقتصاد بزرگ جهان را خواهد داشت[2]. با افزایش تهدیدات سایبری، انتظار می‌رود تا سال 2031 هر دو ثانیه یک حمله سایبری رخ دهد. بر اساس گزارش‌های ارائه شده، مهاجمان سایبری بیش از 4 میلیارد رکورد را در سال 2021 به سرقت بردند[2]. به همین علت، تمرکز شرکت‌ها به طور فزاینده‌ای بر روی توسعه اقدامات امنیت سایبری است [1]. در این راستا، سرمایه‌گذاری در امنیت سایبری با هدف به حداقل رساندن آسیب ناشی از حملات، انجام می‌گیرد [2]. ارائه‌دهندگان امنیت، مسئول ایجاد امنیت برای سایر شرکت‌ها هستند [3]. شرکت‌های ارائه‌دهنده امنیت، می توانند با تعیین سطح امنیت برای جلوگیری از حمله و سپس تعیین قیمت بر اساس ارزش اطلاعات و درصد قابل بازیابی اطلاعات، رهبری ساختار قدرت را در اختیار بگیرند. از طرف دیگر، این شرکت‌ها می‌توانند با انتظار برای وقوع یک حمله، موقعیت پیرو را بگیرند و سپس سطح امنیتی را بر اساس مهارت هکر و ارزش اطلاعات تعیین کنند. در این حالت، حمله در حال وقوع است و هکر برای دست‌یابی به اطلاعات تلاش می‌کند و شرکت در حال رسیدگی و ایجاد امنیت است. آمارهای اخیر نشان می‌دهد که تنها 0,05٪ از شرکت‌ها مایل به گرفتن موقعیت رهبری هستند[2].

در سال‌های اخیر، تحقیقات گسترده‌ای در مورد امنیت سایبری، استراتژی‌های شرکت‌ها و هکرها، مسائل سرمایه‌گذاری و قیمت‌گذاری در امنیت سایبری انجام شده است [4]. قیمت‌گذاری از مسائل مهمی است که نه تنها در حوزه امنیت سایبری بلکه در حوزه‌های مختلف دیگری از جمله حوزه زنجیره تامین چندکاله صورت می‌گیرد [5]. پژوهش [6] به قیمت‌گذاری زنجیره تامین چندکاله با استفاده از قرارداد تقسیم درآمد می‌پردازد. در حوزه امنیت سایبری نیز، بارتلوما[3] [7] مدل [8] را توسعه داد که در سه سطح گسترش می‌یافت. در این مدل، شرکت قیمت را در سطح اول ارائه نمود که براساس آن اندازه شبکه را تعیین می‌شود. [9] در زمینه قیمت‌گذاری، ابتدا مدلی را ارائه می‌کنند که قیمت بر اساس تقاضا و عرضه واقعی ابر تعیین می‌گردد.

ماهیت جرایم سایبری در مقایسه با گذشته به دلیل پیچیدگی روزافزون هکرها پیچیده‌تر شده است. چنگ و همکاران[4] [10] هکرها را به 13 نوع دسته‌بندی کرده و هفت انگیزه و استراتژی مرتبط با آن‌ها را بررسی می‌کند و از آن به عنوان چارچوبی برای کمک به تحلیل‌گران و مهندسان امنیتی استفاده می‌شود. طبقه‌بندی دیگر هکرها مربوط به سه دسته کلاه سفید، کلاه خاکستری و کلاه سیاه است. در سال 2011، [11] هکرهای اخلاقی یا کلاه سفید را مورد بحث قرار داد و آن‌ها را در برابر هکرهای کلاه سیاه دانست که به بهبود شرکت‌ها و افزایش امنیت با افزایش قابلیت‌های آن‌ها کمک می‌کنند. [12] همکاری و عدم همکاری هکرهای کلاه خاکستری را در مطالعه خود بررسی کرد. این مطالعه نشان می‌دهد هنگامی که یک هکر کلاه خاکستری تصمیم به همکاری با ارائه جزئیات آسیب‌پذیری به شرکت ارائه دهنده امنیت می‌کند، این شرکت نیز مایل است تا با هکر همکاری کند و آسیب‌پذیری خود را کاهش دهد.

---

[1] Chuck Robbins

[2] cybersecurityventures.com

[3] Bartholomae

[4] Chng al.

یکی از راه‌های بررسی سطوح امنیت و اشتراک‌گذاری اطلاعات، استفاده از رویکرد نظریه بازی است [13]. نظریه بازی پتانسیل بالایی برای ایجاد یک محیط تحلیلی در حوزه امنیتی دارد که با در نظر گرفتن حملات و دفاع، تعاملات بین هکر و شرکت را بررسی می‌کند [14]. همچنین، طبق یک نظرسنجی، نظریه بازی می‌تواند درک محققین از مسائل امنیتی و حریم خصوصی را تسهیل کند [15] و چارچوبی است که به مهندسان امنیتی کمک می‌کند تا استراتژی‌های بهینه را برای کاهش آسیب حملات سایبری به کار گیرند [16]. از جمله پژوهش‌های انجام شده در این حوزه، پژوهش‌های [8]، [17]، [7]، [18]، [12] و [19] است.

در پژوهش‌های گذشته، کاربر ابری به عنوان بازیکنی بوده است که بین دو استراتژی اشتراک و عدم اشتراک اطلاعات خود، تصمیم‌گیری نموده، در صورتی که ارزش اطلاعات آن دیده نشده است [19]. علاوه بر این، اگرچه بازی هکر و شرکت، در پژوهش [7] با رویکرد استکلبرگ حل شده است، اما تنها موقعیت رهبر برای شرکت بیان می‌شود. در صورتی که براساس گزارش‌های اعلام شده[2]، شرکت می‌تواند در جایگاه پیرو نیز باشد. همچنین در مقالات ارائه شده، نوع هکر نیز مطرح نبوده است.

نوآوری این تحقیق وجود کاربر ابری به عنوان بازیکن خارجی است که ارزش اطلاعات این بازیکن، در بدست آمدن مقدار تقاضا موثر است. علاوه بر این، این مقاله ارزش اطلاعات از دست رفته را در تعیین موقعیت یک شرکت بر اساس میزان تلاش هکر در نظر می‌گیرد. همچنین نوع هکر و میزان تلاش او برای دست‌یابی به اطلاعات، نیز مد نظر بوده است تا توابع سود، دقیق‌تر مدلسازی شود. وجود دو ساختار قدرت برای قیمت‌گذاری و تعیین سطح امنیت نیز از دیگر نوآوری‌های این پژوهش به حساب می‌آید. سوالات تحقیقی که مورد بررسی قرار می‌گیرد به شرح زیر است:

-قیمت تعادلی و سطح امنیت برای زمانی که شرکت تامین‌کننده امنیت رهبر باشد، چقدر است؟

-قیمت تعادلی و سطح امنیت برای زمانی که شرکت تامین‌کننده امنیت پیرو باشد، چقدر است؟

-درصد اطلاعات بازگشت شده پس از حمله موفق و ارزش اطلاعات کاربر ابری چه تاثیری بر سود شرکت دارد؟

در ادامه این مقاله، در بخش 2- مسئله مورد بررسی شرح داده شده و نمادها تعریف می‌شوند. در ادامه مدلسازی مربوط به هر بازیکن صورت گرفته و جواب‌های تعادلی ارائه شده است. در بخش 3- با استفاده از مثال عددی، به تجزیه و تحلیل مسئله پرداخته شده و نتیجه‌گیری صورت گرفته است. در نهایت در بخش 4- نتیجه‌گیری کلی و پیشنهادات آتی بیان می‌شود.

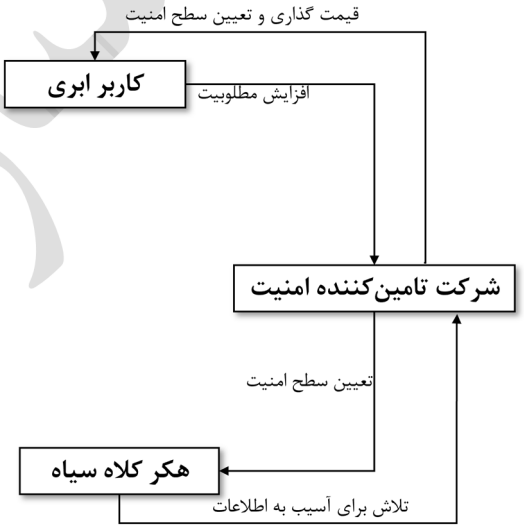
2- بیان مسئله و مدلسازی

ساختارهای قدرت بازی مورد مطالعه به گونه‌ای است که در ابتدا کاربر با افزایش مطلوبیت خود، اهمیت امنیت اطلاعات خود را مشخص می‌کند. در واقع، کاربر یک بازیکن خارجی[1] است. سپس زمانی که مطلوبیت کاربر مثبت شود، تقاضا به دست می‌آید که این مطلوبیت از توزیع یکنواخت پیروی می‌کند. متعاقباً، برای قیمت‌گذاری، هکر و شرکت تأمین‌کننده امنیت درگیر یک بازی استکلبرگ[2] می‌شوند که در آن شرکت تأمین‌کننده امنیت به عنوان رهبر عمل می‌کند

[1] exogenous player

[2] Stackelberg game

یا برعکس و این مسئله به روش استقرا به عقب[1] حل می‌شود. مسئله مورد بررسی شامل دو گروه بازیکن است، گروه اول شامل هکرهایی است که با حملات خود، امنیت سرویس ابری را مختل می‌کنند و به دنبال به دست آوردن اطلاعات کاربر هستند. گروه دوم شامل شرکت‌های ارائه دهنده امنیت است که قصد مبارزه با این حملات را دارند. هر چه شرکت‌ها در ایجاد امنیت سرمایه‌گذاری بیشتری کنند، سطح امنیت بیشتر می‌شود و تعداد کاربرانی که از خدمات آن‌ها استفاده می‌کنند، افزایش می‌یابد و باعث افزایش سود شرکت می‌شود. شکل 1 توپولوژی مسئله و فعالیت هر بازیکن را نشان می‌دهد. لازم به ذکر است در این مقاله تنها به بررسی هکرهای کلاه سیاه پرداخته می‌شود.



شکل 1 توپولوژی مسئله

2-1- نمادها

در ابتدا نمادهای به کار رفته در مسئله معرفی می‌گردد.

اندیس‌ها

C	اندیس کاربر ابری
F	اندیس شرکت تامین‌کننده امنیت
H	اندیس هکر کلاه سیاه

پارامترها

V	متغیر تصادفی مربوط به حداکثر ارزش اطلاعات کاربر که از یک توزیع یکنواخت پیروی می‌کند (واحد پولی)
δ	درصد آسیب وارد شده به اطلاعات بعد از حمله موفق (بدون واحد)
$d(p)$	تقاضای کاربر ابری
M	کل پولی که هکر برای هک کردن دریافت می‌کند (واحد پولی)
y	درصدی از پول که هکر قبل از حمله، دریافت می‌کند (بدون واحد)
O	اعتبار هکر با توجه به اطلاعاتی که در سایت تور[2] از آن هکر موجود است
λ	درصد افزایش اعتبار هکر بعد از یک حمله‌ی موفق که در بازه‌ی صفر و یک است (بدون واحد)
θ	درصد اطلاعاتی که شرکت بعد از حمله‌ی موفق می‌تواند بازیابی کند (بدون واحد)
N	تعداد کاربران ابری
k	ضریب تبدیل هزینه سطح امنیت در تابع سود شرکت
k_1	ضریب تبدیل هزینه تلاش هکر در تابع سود هکر
μ	ضریب تبدیل موفقیت حمله به واحد پولی

[1] backward induction

[2] The Onion Router

α ضریب کاهش اعتبار شرکت در صورت موفقیت حمله

γ ضریب تبدیل اعتبار هکر به واحد پولی

متغیرهای تصمیم

q سطح امنیت ایجاد شده که عددی بین صفر و یک است

p قیمتی که شرکت به کاربر ابری ارائه می‌دهد (واحد پولی)

e میزان افزایش تلاش هکر برای هک موفق که تابعی از زمان بوده و عددی بین صفر و یک است.

توابع وابسته

u_C تابع مطلوبیت کاربر ابری (واحد پولی)

u_F تابع سود شرکت تامین‌کننده امنیت (واحد پولی)

u_H تابع سود هکر (واحد پولی)

2-2- مفروضات مسئله

در مورد مدل مربوط به کاربران ابری، متغیر تصمیم‌گیری وجود ندارد و تنها مطلوبیت مثبت را تعیین می‌کند که باعث می‌شود امنیت خود را به شرکت ارائه دهنده امنیت بسپارند. تقاضا برای شرکت تامین کننده امنیت پس از تصمیم‌گیری در مورد این محدوده و در نظر گرفتن توزیع یکنواخت بدست می‌آید. در مدل هکر، از آنجایی که هکرهای کلاه سیاه مورد توجه قرار دارند، متغیر تصمیم، میزان تلاش مورد نیاز برای به دست آوردن اطلاعات بر اساس ارزش اطلاعات کاربر است. مدل نهایی مربوط به شرکت تامین کننده امنیت، دارای دو متغیر تصمیم است. متغیر تصمیم اول با قیمتی مرتبط است که کاربران ابری باید ارائه دهند تا امنیت خود را تضمین کنند و متغیر تصمیم دوم سطح امنیت ایجاد شده است. هکرها اعتبار دارند و به ازای هر هک موفق، اعتبار آنها افزایش می‌یابد و بالعکس.

2-3- تابع مطلوبیت و سود بازیکنان

معادله (1) تابع مطلوبیت کاربر ابری را نشان می‌دهد که به طور کلی شامل سطح امنیت ایجاد شده برای حفظ اطلاعات کاربر و هزینه‌ای که باید برای ایجاد آن بپردازد، است. در این تابع، V متغیر تصادفی است که حداکثر ارزش اطلاعات کاربر را نشان می‌دهد و از یک توزیع یکنواخت پیروی می‌کند [20] و p هزینه‌ای است که کاربر برای برقراری سطح امنیت به شرکت می‌پردازد. پارامتر q سطح امنیت ایجاد شده در یک شرایط عادی را نشان می‌دهد که براساس [18] عددی بین صفر و یک خواهد بود. پارامتر e نشان دهنده تلاش اضافی مورد نیاز یک هکر برای افزایش احتمال یک حمله موفق است. بخش اول و دوم این تابع حدکثر ارزش و پولی را که کاربر باید پرداخت نماید، نشان می‌دهد. بخش سوم مربوط به موفقیت حمله است که باعث آسیب به اطلاعات و کاهش رضایت مشتری و در نتیجه کاهش مطلوبیت می‌شود. کاهش مطلوبیت به علت حمله موفق زمانی اتفاق می‌افتد که مشتریان از حمله مطلع شوند و این درصورتی است که اطلاعاتشان آسیب ببیند یا از بین برود و بازیابی نشود. حمله در صورتی موفق است که هکر تلاش نماید و سطح امنیت شکسته شود یا به عبارتی برقرار نشود. برقراری سطح امنیت با متغیر تصمیم q نشان داده شده است و چون این متغیر عددی بین صفر و یک است، عدم برقراری آن به صورت $1-q$ خواهد بود. تلاش هکر نیز چون موثر است، به این احتمال اضافه می‌گردد. تمامی این بخش به صورت $1-q+e$ نوشته شده است. حال در صورت موفقیت حمله، شرکت تلاش می‌نماید تا اطلاعات آسیب دیده را بازیابی نماید. درصد اطلاعات بازیابی شده با پارامتر θ نشان داده شده است و در نتیجه عدم بازیابی اطلاعات $1-\theta$ خواهد بود. پس اگر حمله موفق باشد و اطلاعات بازیابی نشود، باتوجه به درصد آسیب اطلاعات که با δ نشان داده شده است، تقاضا کاهش میابد. این استدلال منجر به تشکیل بخش سوم تابع مطلوبیت

کاربر می‌شود. لازم به ذکر است این درصد در حداکثر ارزش کل ضرب می‌شود تا میزان آسیب اطلاعات بدست آید.

$$u_c = V - p - (1-q+e)(1-\theta)\delta V \quad (1)$$

کاربر زمانی امنیت اطلاعات خود را به شرکت تامین‌کننده امنیت می‌سپارد که مطلوبیت مثبتی داشته باشد. بنابراین لازم است تا $u_c \geq 0$ باشد و سپس V از این روش بدست آورده شود. کمترین حالتی که ممکن است کاربر امنیت خود را به شرکت تامین‌کننده امنیت بسپارد، در $u_C = 0$ است. در نتیجه، مطابق رابطه (2) تقاضا مشخص می‌گردد. معادله (4)میزان تقاضا برای شرکت تامین‌کننده امنیت را نشان می‌دهد. این معادله بر اساس روابط موجود در کتاب فیلیپس [21] نوشته شده است. در این کتاب برای بدست آوردن تابع تقاضا، از تمایل مشتری برای خرید استفاده می‌کند و برای سادگی فرض می‌کند تمایل مشتری به پرداخت، دقیقا برابر قیمت است که این مقدار، حد پایین انتگرال را خواهد داد و سپس با بدست آوردن تابع تجمعی مربوط به تابع چگالی احتمال یکنواخت، تقاضا بدست می‌آید.

$$u_c = 0$$
$$V = \frac{p}{1-\delta-e\delta+q\delta+2\delta\theta+2e\delta\theta-2q\delta\theta} \quad (2)$$

$$V \sim U(0,1) \quad (3)$$

$$d(p) = N\int_{V\to\frac{p}{1-\delta-e\delta+q\delta+2\delta\theta+2e\delta\theta-2q\delta\theta}}^{1} dx = 1-\frac{p}{1+(1+e-q)\delta(-1+2\theta)} \quad (4)$$

در ادامه براساس این رابطه، تابع سود شرکت مطابق معادله (5) نوشته خواهد شد. برای سهولت حل، در ادامه تعداد کاربران ابری نرمال و N، 1 درنظر گرفته شده است. معادله (6) تابع سود هکر با توجه به موفقیت و عدم موفقیت حمله را نشان می‌دهد. برای تبدیل توابع سود به واحد پولی، نیاز به ضرایب تبدیل می‌باشد. بدین منظور ضرایب تبدیل برای هر عبارت به توابع اضافه شده است که در بخش نمادها نیز معرفی گردید.

$$u_F = d(p) * p - \frac{(kq^2)}{2} - (1-q+e)\alpha\mu \quad (5)$$

$$u_H = My + (1-q+e)(1-y)M + (1-q+e)\lambda O\gamma - (q-e)(1-\lambda)O\gamma - \frac{(k_1 e^2)}{2} \quad (6)$$

حال باید با توجه به ساختارهای مختلف، مسئله را حل نمود. در ابتدا فرض بر این است که تامین‌کننده امنیت تصمیم‌گیر اول و رهبر است و در مورد سطح امنیت مورد نیاز تصمیم و قیمت را به کاربر اعلام می‌کند. مقادیر تعادلی براساس اثبات‌های صورت گرفته در پیوست1 و با روش استقرا به عقب بدست آمد. روابط (7) و (8) و (9) مقادیر تعادلی را نشان می‌دهد.

$$p^* = \frac{1}{8}\left(4 + \frac{\delta(-1+2\theta)(4k-\delta+2\delta\theta-4\alpha\mu)}{k} - \frac{4\delta(-1+2\theta)(M(-1+y)-O\gamma\lambda)}{k_1}\right) \quad (7)$$

$$q^* = \frac{\delta - 2\delta\theta + 4\alpha\mu}{4k} \quad (8)$$

$$e^* = \frac{M - My + O\gamma\lambda}{k_1} \quad (9)$$

برای بررسی ساختار قدرت دیگر بازی، باید هکر در ابتدا تصمیم‌گیرنده باشد و شرکت تامین‌کننده امنیت به عنوان پیرو عمل نماید.

مقادیر تعادلی براساس اثبات‌های صورت گرفته در پیوست2 و با روش استقرا به عقب بدست آمد. روابط (10) و (11) و (12) مقادیر تعادلی در این ساختار قدرت را نشان می‌دهند.

$$p^* = \frac{1}{8}\left(\begin{array}{l} 4 + \dfrac{\delta(-1+2\theta)(4k+\delta(-1+2\theta)+4\alpha(-1+\theta)\mu)}{k} - \\ \dfrac{4\delta(-1+2\theta)(M(-1+y)+O\gamma(-1+\lambda))}{k_1} \end{array}\right) \quad (10)$$

$$q^* = \frac{\delta - 2\delta\theta + 4\alpha\mu - 4\alpha\theta\mu}{4k} \quad (11)$$

$$e^* = \frac{M - My + O\gamma - O\gamma\lambda}{k_1} \quad (12)$$

3- مثال عددی و تحلیل حساسیت

در ادامه با استفاده از مثال عددی سعی می‌شود تا مسئله مورد تحلیل قرار گیرد. لازم به ذکر است علاوه بر این مثال عددی، 19 مثال عددی دیگر بررسی شد تا صحت نتایج حاصله بررسی گردد. برای بررسی میزان تفاوت مقادیر سود در نمونه‌های مختلف، از آزمون آماری فریدمن استفاده گردید. براساس نتیجه آزمون فریدمن و مقایسه با مقدار p-value که برابر 0/00955 بود، فرض تفاوت بین نتایج، رد شد و در نتیجه بین مقادیر سود تفاوت چشم‌گیری براساس نمونه‌های ایجاد شده وجود نداشت. محاسبات مربوط به این آزمون در پیوست3 قابل مشاهده است.

3-1- مثال عددی

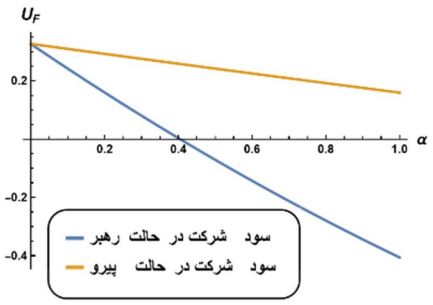
جهت فهم بهتر مسئله یک مثال عددی از مسئله ارائه می‌گردد و سپس به تحلیل حساسیت توابع سود نسبت به پارامترهای مختلف پرداخته و نکات مهم آن بیان می‌شود. جدول 1 مقادیر مورد استفاده برای پارامترها را نشان می‌دهد. لازم به ذکر است برای اینکه تمام مقادیر یک واحد شوند، با توجه به منابع هریک، نرمال شده‌اند.

جدول 1: مقادیر درنظر گرفته شده برای پارامترها در مثال‌ها و تحلیل حساسیت‌ها

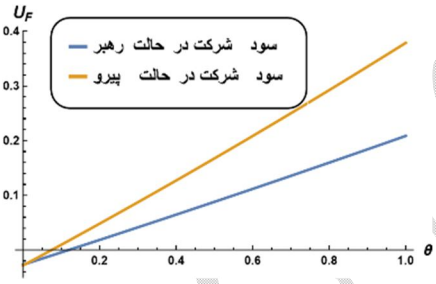
پارامتر	مقدار دهی	منابع
k	1	[22]
α	3	مصاحبه با مهندسین امنیت
k_1	3	[22]
O	0,4	[22]
γ	0,2	[22]
δ	0,3	[22]
λ	0,2	مصاحبه با مهندسین امنیت
μ	1,5	مصاحبه با مهندسین امنیت
M	4	[16]
y	0,5	مصاحبه با مهندسین امنیت

با حل مسئله حاصل از پارامترهایی که مقادیر آن در جدول 1 ارائه گردیده است، نتایج زیر حاصل می‌گردد. شکل 2 سود شرکت را در دو سناریو براساس پارامتر ضریب کاهش اعتبار شرکت نشان می‌دهد. همانطور که مشخص است، براساس این پارامتر، سود شرکت در حالت پیرو بودن بیشتر است. شکل 3 سود شرکت را براساس درصد بازگشت اطلاعات نشان می‌دهد. در این حالت نیز سود شرکت در جایگاه پیرو بیشتر بوده و هرچه درصد بازگشت اطلاعات بیشتر باشد، سود افزایش می‌یابد. شکل 4 مقایسه قیمت را در دو ساختار قدرت نشان می‌دهد. همانطور که مشخص است، قیمت‌ها در این دوحالت، تقریبا یکسان تعیین می‌شود.

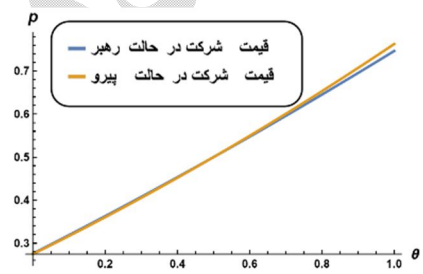
در ادامه شکل 5 قیمت، براساس ضریب کاهش اعتبار شرکت رسم گردید. این شکل نشان می‌دهد براساس این پارامتر، قیمت تعیین شده در وضعیتی که شرکت رهبر است، کمتر از حالتی است که شرکت پیرو باشد. شکل 6 متغیر تصمیم سطح امنیت ایجاد شده را براساس ضریب کاهش شرکت نشان می‌دهد. بدیهی است که هرچقدر این ضریب بیشتر باشد، لازم است تا سطح امنیت بالاتری تعیین گردد تا اعتبار شرکت کمتر آسیب ببیند.



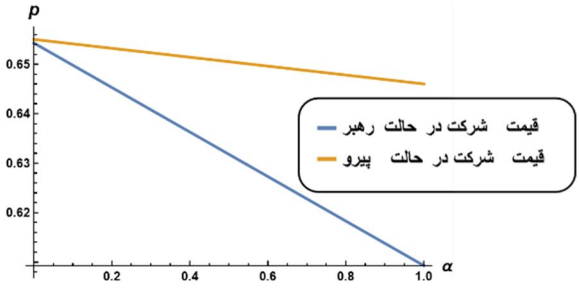
شکل 2 مقایسه سود شرکت براساس کاهش اعتبار شرکت در حمله موفق



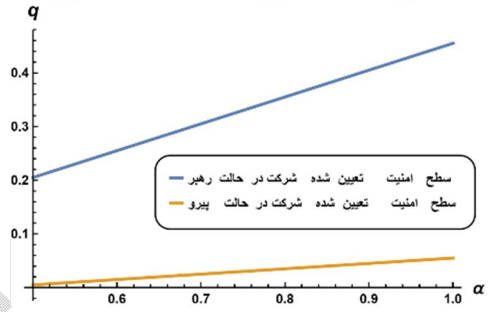
شکل 3 مقایسه سود شرکت براساس درصد اطلاعات بازگشتی



شکل 4 قیمت شرکت براساس درصد اطلاعات بازگشتی



شکل 5 قیمت تعیین شده توسط شرکت براساس کاهش اعتبار شرکت هنگام حمله موفق



شکل 6 سطح امنیت تعیین شده براساس کاهش اعتبار شرکت هنگام حمله موفق

براساس نمودارهای فوق و همچنین تحلیل‌های صورت گرفته نتایجی حاصل گردید که در ادامه بیان می‌شود:

نتیجه 1 با توجه به نمونه‌های مختلف شبیه سازی شده و مقادیر بدست آمده و همچنین نمونه‌ی ارائه شده در این پژوهش، دو پارامتر درصد بازیابی اطلاعات و ضریب کاهش اعتبار شرکت، دو پارامتر اساسی در مقدار سود هستند. شرکت‌های تامین‌کننده امنیت، با توجه به این دو پارامتر و اهمیت هریک، می‌توانند ساختار قدرت و قیمت خود را تعیین نمایند.

نتیجه 2 شکل 4 نشان می‌دهند زمانی که تصمیم بر اساس درصد اطلاعات بازیابی شده باشد، قیمت تعیین شده توسط شرکت، در درصد بازیابی پایین، در دو ساختار، تفاوتی ندارند. هرچه درصد بازیابی افزایش یابد، قیمت تعیین شده در حالت پیرو، بیشتر خواهد بود؛ اما این تغییر زیاد نبوده و می‌توان گفت قیمت در دو ساختار تقریبا یکسان تعیین می‌شود. با این وجود، مطابق شکل 3، سود شرکت براساس این پارامتر، در ساختار رهبر بودن شرکت، تفاوت زیادی با سود در حالت پیرو دارد. این تغییر با وجود یکسان بودن تقریبی قیمت‌ها، ناشی از تفاوت سطح امنیت ایجاد شده و تلاش هکر در دو ساختار است. تفاوت سطح امنیت ایجاد شده در سود شرکت مطابق با نتایج مطالعه [7] نیز می‌باشد.

نتیجه 3 شکل 5 قیمت تعیین شده را براساس پارامتر ضریب کاهش اعتبار شرکت در صورت موفقیت حمله نشان می‌دهد. براساس این شکل مشخص است که هرچه میزان کاهش اعتبار بیشتر باشد، قیمت کاهش می‌یابد. دلیل این امر این است که با توجه به کاهش اعتبار، شرکت محبوبیت کمتری در بین مشتریان خود خواهد داشت، بنابراین لازم است تا برای جذب مشتری، قیمت خود را کاهش دهد و از این طریق، زیان وارده را جبران نماید. همچنین در این شکل مشاهده می‌شود که قیمت در حالت رهبر بودن، بسیار کمتر تعیین می‌شود. شکل 2 تفاوت سود براساس این پارامتر را در دو ساختار نشان می‌دهد. همانطور که مشخص است، سود در حالت رهبر بودن نیز کاهش بسیاری نسبت به حالت پیرو بودن دارد.

نتیجه 4 سطح امنیت تعیین شده براساس پارامتر ضریب کاهش اعتبار شرکت، زمانی که شرکت پیرو باشد، بسیار کمتر است از زمانی که شرکت رهبر باشد. این امر به وضوح در شکل 6 مشخص است. این نتیجه، یکی دیگر از دلایلی است که باعث می‌شود سود در

حالت رهبر بودن کمتر از حالت پیرو بودن باشد؛ زیرا سطح امنیت در حالت رهبر بودن شرکت، بالاتر بوده و درنتیجه هزینه‌ای که شرکت برای تامین سطح امنیت متحمل می‌شود، بسیار بیشتر بوده و باعث کاهش سود می‌شود.

نتیجه 5 بالاتر بودن سطح امنیت ایجاد شده در حالت رهبر بودن شرکت، به این علت است که شرکت باید قبل از حمله و بدون اطلاع از وضعیت حمله و مهارت هکر، سطح امنیت را ایجاد کرده و قیمت را ارائه دهد [7]. بنابراین لازم است تا در حد امکان با توجه به ارزش اطلاعات، امنیت ایجاد شود و در نتیجه ممکن است سطح امنیت بسیار بالاتر از حد مورد نیاز تعیین شود و این می‌تواند دلیل دیگری باشد که تنها 0,05 درصد از شرکت‌ها این ساختار را انتخاب می‌نمایند[2].

نتیجه 6 تحلیل پارامتریک متغیر تصمیم مربوط به سطح امنیت ایجاد شده نشان می‌دهد اگر، تمامی پارامترهای موجود در این متغیر تصمیم مثبت باشد، همواره سطح امنیت ایجاد شده در حالت رهبر بودن شرکت، بیشتر از حالت پیرو بودن آن است.

نتیجه 7 تحلیل پارامتریک متغیر تصمیم تلاش هکر نشان می‌دهد اگر، $\lambda > \frac{1}{2}$ و بقیه پارامترها مثبت باشد، تلاش هکر زمانی که شرکت رهبر باشد، بیشتر از زمانی است که شرکت پیرو باشد.

4- نتیجه‌گیری و پیشنهادات آتی

این مقاله به بررسی رابطه بین هکرها و یک شرکت ارائه-دهنده امنیت می‌پردازد تا قیمت و سطح امنیتی مورد نیاز شرکت را بسته به ساختار قدرت تعیین کند. پس از مدل‌سازی و بررسی ساختارهای مختلف قدرت و با استفاده از داده‌های موجود در ادبیات و مصاحبه با کارشناسان امنیت سایبری، قیمت‌ها و سود در موقعیت‌های مختلف شرکت مقایسه شد. نتایج نشان می‌دهد جایگاه شرکت در ساختار قدرت، تاثیر زیادی بر قیمت ارائه شده براساس درصد بازیابی اطلاعات ندارد. با این وجود، سود در حالت پیرو بودن براساس همین پارامتر و همچنین پارامتر ضریب کاهش اعتبار شرکت، همواره بالاتر از جایگاه رهبر است.

از محدودیت‌های این پژوهش، درنظر گرفتن تنها یک نوع هکر و یک شرکت است. همچنین نوع تابع تقاضا در نظر گرفته شده، خطی است و تنها از تعدادی از پارامترهای تاثیرگذار طبعیت می‌کند. برای مطالعات آینده، علاوه بر پوشش دادن محدودیت‌های این مسئله، می‌توان بودجه کاربر ابری برای سرمایه‌گذاری امنیت سایبری را درنظر گرفت و آن را به عنوان محدودیت وارد مسئله نمود. همچنین درنظر گرفتن انواع دیگر هکر، برای نوشتن توابع سود، می‌تواند نتایج متفاوتی را ارائه دهد. به عنوان مثال هکرهای کلاه خاکستری را درنظر گرفت که می‌توانند استراتژی‌های افشا یا همکاری با شرکت را دارند. در نهایت در این مسئله می‌توان به جای درنظر گرفتن درصد بازگشت اطلاعات، از بیمه ابری استفاده نمود که در صورت حمله و آسیب به اطلاعات کاربر، شرکت مبلغی را به عنوان بیمه به کاربر پرداخت نماید. این مورد نیز در توابع سود مربوط به شرکت و کاربر تاثیر خواهد داشت.

پیوست

پیوست1. در ادامه اثبات مربوط به حل مسئله بر اساس ساختار قدرت اول یعنی رهبر بودن شرکت تامین‌کننده امنیت، بیان شده است.

در ابتدا لازم است تا مشخص شود تابع مقعر است. در صورت منفی بودن مشتق دوم تابع، می‌توان با استفاده از مشتق اول، نقاط تعادلی را بدست آورد. با توجه به

اینکه از روش استقرا به عقب برای حل مسئله استفاده شده است، لازم است تا ابتدا تابع مربوط به پیرو حل شده و سپس با قرار دادن مقادیر بدست آمده در تابع رهبر، مسئله‌ی مربوط به رهبر حل گردد.

$$\frac{\partial^2 u_H}{\partial e^2} = -k \tag{13}$$

$$\frac{\partial u_H}{\partial e} = M\left(1-y\right) + O\gamma\lambda - ek_1 \tag{14}$$

$$M\left(1-y\right) + O\gamma\lambda - ek_1 = 0 \tag{15}$$

$$e^* = \frac{M - My + O\gamma\lambda}{k_1} \tag{16}$$

با قرار دادن این مقدار در تابع رهبر، تابع رهبر جدید ساخته می‌شود. سپس با در نظر گرفتن ماتریس هسین مربوط به این تابع، می‌توان راجع به مقعر بودن آن نظر داد. با فرض $2\theta > 1$، مینور اول ماتریس هسین منفی خواهد بود. با محاسبه مینور دوم ماتریس هسین عبارت (21) بدست خواهد آمد. با توجه به مثبت بودن قسمت‌های مختلف این رابطه و همچنین مثبت بودن مخرج کسر، می‌توان با ساده‌سازی آن را به عبارت (22) تبدیل کرد. با علم به آنکه تمامی پارامترهای موجود در این رابطه مثبت است، با فرض $k\left(Y\right)^3 > 3S + J\left(U\right)$، مینور دوم ماتریس هسین منفی شده و در نتیجه تابع مقعر است. لازم به ذکر است در مقداردهی پارامترهای مسئله، این مورد درنظر گرفته شده است. در ادامه با توجه به مقعر بودن توابع سود، با استفاده از مشتق اول مقادیر تعادلی بدست می‌آید.

$$u_F = p\left(1 - \frac{p}{1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)}\right) - \alpha\mu\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right) - \frac{kq^2}{2} \tag{17}$$

$$\frac{\partial^2 u_F}{\partial p^2} = -\frac{2}{1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)} \tag{18}$$

$$\frac{\partial^2 u_F}{\partial q^2} = -k - \frac{2p^2\delta^2\left(-1+2\theta\right)^2}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\frac{M-My+O\gamma\lambda}{k_1}\right)\right)^3} \tag{19}$$

(20)

$$\begin{pmatrix} -\dfrac{2}{1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)} & -\dfrac{2p\delta\left(-1+2\theta\right)}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)\right)^2} \\ -\dfrac{2p\delta\left(-1+2\theta\right)}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)\right)^2} & -k-\dfrac{2p^2\delta^2\left(-1+2\theta\right)^2}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)\right)^3} \end{pmatrix}$$

(21)

$$\det = \frac{2\left(\begin{array}{l} -3p^2\delta^2\left(1-2\theta\right)^2+k\left(1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)\right)^3- \\ p^2\delta^3\left(-1+2\theta\right)^3\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right) \end{array}\right)}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)\right)^4}$$

$$\det = 2\left(-3S+k\left(Y\right)^3-J\left(U\right)\right) \tag{22}$$

$$\frac{\partial u_F}{\partial p} = 1-\frac{2p}{1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)} \tag{23}$$

$$\frac{\partial u_F}{\partial q} = -kq+\alpha\mu-\frac{p^2\delta\left(-1+2\theta\right)}{\left(1+\delta\left(-1+2\theta\right)\left(1-q+\dfrac{M-My+O\gamma\lambda}{k_1}\right)\right)^2} \tag{24}$$

$$p^* = \frac{1}{8}\left(4+\frac{\delta\left(-1+2\theta\right)\left(4k-\delta+2\delta\theta-4\alpha\mu\right)}{k}-\frac{4\delta\left(-1+2\theta\right)\left(M\left(-1+y\right)-O\gamma\lambda\right)}{k_1}\right) \tag{25}$$

$$q^* = \frac{\delta-2\delta\theta+4\alpha\mu}{4k} \tag{26}$$

با قرار دادن مقادیر تعادلی در معادله (16) مقدار تعادلی متغیر تصمیم هکر نیز بدست خواهد آمد.

$$e^* = \frac{M-My+O\gamma\lambda}{k_1}.\square \tag{27}$$

پیوست2. در ادامه اثبات مربوط به حل مسئله بر اساس ساختار قدرت دوم یعنی پیرو بودن شرکت تامین‌کننده امنیت، بیان شده است.

در ابتدا لازم است تا مشخص شود تابع مقعر است. برای این منظور از ماتریس هسین استفاده می‌شود. برای منفی بودن مینور اول همان فرض پیوست 1 برای منفی بودن مینور اول درنظر گرفته شد. با محاسبه مینور دوم ماتریس هسین عبارت (31) بدست خواهد آمد. با توجه به مثبت بودن قسمت‌های مختلف این رابطه و همچنین مثبت بودن مخرج کسر، می‌توان با ساده‌سازی آن را به عبارت (33) تبدیل کرد. با علم به آنکه تمامی پارامترهای موجود در این رابطه مثبت است، با فرض $2(kA)^3 > B(C)$، مینور دوم ماتریس هسین منفی شده و در نتیجه تابع مقعر است. لازم به ذکر است در مقداردهی پارامترهای مسئله، این مورد درنظر گرفته شده است. با توجه به اینکه از روش استقرا به عقب برای حل مسئله استفاده شده است، لازم است تا ابتدا تابع مربوط به پیرو حل شده و سپس با قرار دادن مقادیر بدست آمده در تابع رهبر، مسئله‌ی مربوط به رهبر حل گردد.

$$\frac{\partial^2 u_F}{\partial p^2} = -\frac{2}{1+(1+e-q)\delta(-1+2\theta)} \tag{28}$$

$$\frac{\partial^2 u_F}{\partial q^2} = -k - \frac{2p^2\delta^2(-1+2\theta)^2}{\left(1+(1+e-q)\delta(-1+2\theta)\right)^3} \tag{29}$$

$$\begin{pmatrix} -\frac{2}{1+(1+e-q)\delta(-1+2\theta)} & -\frac{2p\delta(-1+2\theta)}{\left(1+(1+e-q)\delta(-1+2\theta)\right)^2} \\ -\frac{2p\delta(-1+2\theta)}{\left(1+(1+e-q)\delta(-1+2\theta)\right)^2} & -k-\frac{2p^2\delta^2(-1+2\theta)^2}{\left(1+(1+e-q)\delta(-1+2\theta)\right)^3} \end{pmatrix} \tag{30}$$

$$\det = \frac{2\left(k\left(1+(1+e-q)\delta(-1+2\theta)\right)^3 - p^2\delta^2(1-2\theta)^2\left(3+(1+e-q)\delta(-1+2\theta)\right)\right)}{\left(1+(1+e-q)\delta(-1+2\theta)\right)^4} \tag{31}$$

$$\det = 2(kA)^3 - B(C) \tag{32}$$

$$\frac{\partial u_F}{\partial p} = 1 - \frac{2p}{1+(1+e-q)\delta(-1+2\theta)} \tag{33}$$

$$\frac{\partial u_F}{\partial q} = -kq - \frac{p^2\delta(-1+2\theta)}{\left(1+(1+e-q)\delta(-1+2\theta)\right)^2} + \alpha(1-\theta)\mu \tag{34}$$

$$p = \frac{k\left(4+4(1+e)\delta(-1+2\theta)\right)+\delta(-1+2\theta)\left(\delta(-1+2\theta)+4\alpha(-1+\theta)\mu\right)}{8k} \tag{35}$$

$$q = \frac{\delta - 2\delta\theta - 4\alpha\left(-1+\theta\right)\mu}{4k} \tag{36}$$

با قرار دادن روابط (35) و (36) در تابع هدف هکر(رابطه (6)) تابع هدف هکر بدست خواهد آمد.

سپس با جای‌گذاری رابطه (42) در روابط(35) و (36) مقادیر تعادلی شرکت بدست می‌آید.

$$p^* = \frac{1}{8}\left(\begin{array}{l} 4 + \dfrac{\delta\left(-1+2\theta\right)\left(4k + \delta\left(-1+2\theta\right) + 4\alpha\left(-1+\theta\right)\mu\right)}{k} - \\ \dfrac{4\delta\left(-1+2\theta\right)\left(M\left(-1+y\right) + O\gamma\left(-1+\lambda\right)\right)}{k_1} \end{array}\right) \tag{37}$$

$$q^* = \frac{\delta - 2\delta\theta + 4\alpha\mu - 4\alpha\theta\mu}{4k} \tag{38}$$

$$u_H = My - \frac{O\gamma\lambda\left(\delta - 2\delta\theta + 4\alpha\mu - 4\alpha\theta\mu\right)}{4k} + M\left(1-y\right)\left(1 + e - \frac{\delta - 2\delta\theta + 4\alpha\mu - 4\alpha\theta\mu}{4k}\right) + \tag{39}$$

$$O\gamma\left(1-\lambda\right)\left(1 + e - \frac{\delta - 2\delta\theta + 4\alpha\mu - 4\alpha\theta\mu}{4k}\right) - \frac{e^2 k_1}{2}$$

$$\frac{\partial^2 u_H}{\partial e^2} = -k_1 \tag{40}$$

$$\frac{\partial u_H}{\partial e} = M\left(1-y\right) + O\gamma\left(1-\lambda\right) - ek_1 \tag{41}$$

$$e^* = \frac{M - My + O\gamma - O\gamma\lambda}{k_1}.\square \tag{42}$$

پیوست3. آزمون فریدمن

در این پژوهش، 19 نمونه‌ی دیگر با توجه به محدودیت‌های هر پارامتر که در پیوست1 و پیوست2 بیان گردید، ایجاد شد و براساس آن مقادیر تابع هدف را بدست آمد. سپس با استفاده از آزمون فریدمن نتایج ارزیابی شد. آزمون فریدمن یک آزمون آماری ناپارامتریک است که توسط میلتون فریدمن توسعه یافته است. این روش هر سطر را رتبه‌بندی می‌کند و سپس رتبه‌بندی در ستون‌ها را در نظر می‌گیرد. در ادامه روند انجام آزمون فریدمن ارائه شده است.

فرض صفر، تفاوت بین نتایج درنظر گرفته شد. برای انجام آزمون فریدمن و رد یا تایید فرض صفر، 19 نمونه در نظر گرفته شد. این نمونه‌ها با تغییر هر یک از پارامترها ایجاد

شده است. به عنوان مثال نمونه اول، درصد آسیب اطلاعات در حمله موفق، کم، در نمونه دوم این پارامتر متوسط و در نمونه سوم این پارامتر در حد بالا، مقداردهی شده است. بقیه نمونه‌ها نیز با تغییر مقدار پارامترها به کم، متوسط و زیاد ایجاد شده و مقادیر تابع سود در دو سناریو بدست آمده است. مقادیر سود در جدول 2، نشان داده شده است. سپس براساس روند انجام آزمون فریدمن، این مقادیر سود، رتبه‌بندی شده و رتبه‌ها در هر ستون با یکدیگر جمع شدند. میانگین رتبه‌ها بدست آمده و براساس آماره آزمون فریدمن که در رابطه (43) نشان داده شده است، مقدار این آماره بدست آمد. در این رابطه n تعداد نمونه‌ها و k تعداد سناریوهای بررسی شده است. پس از بدست آوردن این آماره، مقدار p-value محاسبه گردید و برابر 0,00955 شد که این، مقدار کمی برای p-value بوده و درنتیجه فرض صفر رد شد.

$$Q = \frac{12n}{k(k+1)} \sum_{j=1}^{k} (\overline{r}_j - \frac{(k+1)}{2})^2 \qquad (43)$$

جدول 2: مقادیر سود با نمونه‌های مختلف

	شرکت در حالت پیرو	شرکت در حالت رهبر
نمونه 1	0.090479	0.066986
نمونه 2	0.184317	0.121533
نمونه 3	0.278779	0.189106
نمونه 4	0.288779	0.167106
نمونه 5	0.692112	-0.720228
نمونه 6	0.296279	0.150606
نمونه 7	0.300215	0.256686
نمونه 8	0.267487	0.103126
نمونه 9	0.283679	0.177886
نمونه 10	0.283729	0.177996
نمونه 11	0.388867	0.276893
نمونه 12	0.325139	0.216946
نمونه 13	0.284713	0.177592
نمونه 14	0.284312	0.177812
نمونه 15	0.284179	0.177886
نمونه 16	0.283979	0.177996
نمونه 17	0.203759	-0.160794

جدول 3: رتبه‌بندی مقادیر سود و محاسبه میانگین

	شرکت در حالت پیرو	شرکت در حالت رهبر	جمع رتبه ها	میانگین
نمونه 1	1	4	5	0.454545455
نمونه 2	2	6	8	0.727272727
نمونه 3	6	14	20	1.818181818
نمونه 4	14	8	22	2
نمونه 5	19	1	20	1.818181818
نمونه 6	15	7	22	2
نمونه 7	16	16	32	2.909090909
نمونه 8	5	5	10	0.909090909
نمونه 9	7	12	19	1.727272727
نمونه 10	8	13	21	1.909090909
نمونه 11	18	17	35	3.181818182
نمونه 12	17	15	32	2.909090909
نمونه 13	12	10	22	2
نمونه 14	12	11	23	2.090909091
نمونه 15	11	12	23	2.090909091
نمونه 16	10	13	23	2.090909091
نمونه 17	3	2	5	0.454545455
نمونه 18	4	3	7	0.636363636
نمونه 19	9	9	18	1.636363636

5- مراجع

1. O'Connor, S., et al., *SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security.* Information Sciences, 2021: p. DOI: https://doi.org/10.1016/j.ins.2021.08.098
2. Chronopoulos, M., E. Panaousis, and J. Grossklags, *An options approach to cybersecurity investment.* IEEE Access, 2017. **6**: p. DOI:10.1109/ACCESS.2017.2773366.
3. Whaiduzzaman, M. and A. Gani. *Measuring security for cloud service provider: A Third Party approach.* in *2013 International Conference on Electrical Information and Communication Technology (EICT).* 2014. IEEE, DOI: 10.1109/EICT.2014.6777855.
4. Che, J., et al., *Study on the security models and strategies of cloud computing.* Procedia Engineering, 2011. **23**: p. 586-593, https://doi.org/10.1016/j.proeng.2011.11.2551.
5. Hsieh, C.-C., Y.-L. Chang, and C.-H. Wu, *Competitive pricing and ordering decisions in a multiple-channel supply chain.* International Journal of

Production Economics, 2014. **154**: p. 156-165, https://doi.org/10.1016/j.ijpe.2014.04.024.
6. Chen, Z.-S., et al., *Optimal pricing decision in a multi-channel supply chain with a revenue-sharing contract.* Annals of Operations Research, 2022. **318**(1): p. 67-102, https://doi.org/10.1007/s10479-022-04748-7.
7. Bartholomae, F., *Cybercrime and cloud computing. A game theoretic network model.* Managerial and Decision Economics, 2018. **39**(3): p. 297-305,DOI:https://doi.org/10.1002/mde.2904.
8. Shy, O., *The economics of network industries.* 2001: Cambridge university press,DOI:https://doi.org/10.1146/annurev-economics-081023-024638.
9. Cong, P., et al., *Profit-driven dynamic cloud pricing for multiserver systems considering user perceived value.* IEEE Trans. Parallel Distrib. Syst, 2018. **29**(12): p. 2742-2756, DOI: 10.1109/TPDS.2018.2843343
10. Chng, S., et al., *Hacker types, motivations and strategies: A comprehensive framework.* Computers in Human Behavior Reports, 2022: p. 100167, DOI: https://doi.org/10.1016/j.chbr.2022.100167.
11. Caldwell, T., *Ethical hackers: putting on the white hat.* Network Security, 2011. **2011**(7):p.10-13,DOI: https://doi.org/10.1016/S1353-4858(11)70075-7.
12. Cohen, D., A. Elalouf, and R. Zeev, *Collaboration or separation maximizing the partnership between a "Gray hat" hacker and an organization in a two-stage cybersecurity game.* International Journal of Information Management Data Insights, 2022. **2**(1): p. pages 100073, DOI:https://doi.org/10.1016/j.jjimei.2022.100073.
13. Rachamalla, S. and S.H. Fatima, *GAME THEORY AND CYBER SECURITY.* 2020: p. DOI: 10.1145/1852666.1852704
14. Shiva, S., S. Roy, and D. Dasgupta. *Game theory for cyber security.* in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*.2010,10.1145/1852666.1852704.
15. Do, C.T., et al., *Game theory for cyber security and privacy.* ACM Computing Surveys (CSUR), 2017. **50**(2): p. 1-37, DOI: https://doi.org/10.1145/3057268.
16. Hyder, B. and M. Govindarasu. *Optimization of cybersecurity investment strategies in the smart grid using game-theory*. in *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. 2020. IEEE,DOI:10.1109/ISGT45199.2020.9087634.
17. Xiao, P. and Z. Tang, *Game theory–based resource pricing model in cloud platforms.* International Journal of Communication Networks and Distributed Systems, 2015. **14**(3): p. 256-271,https://doi.org/10.1504/IJCNDS.2015.068666.
18. Feng, S., et al., *Joint pricing and security investment in cloud security service market with user interdependency.* IEEE Transactions on Services Computing, 2020. **15**(3): p. 1461-1472, DOI: 10.1109/TSC.2020.2996382.
19. Ge, H., et al., *A game theory based optimal allocation strategy for defense resources of smart grid under cyber-attack.* Information Sciences, 2024: p. https://doi.org/10.1016/j.ins.2023.119759.
20. Huang, J., M. Leng, and M. Parlar, *Demand functions in decision modeling: A comprehensive survey and research directions.* Decision Sciences, 2013. **44**(3): p. 557-609.
21. Phillips, R.L., *Pricing and revenue optimization*. 2021: Stanford university press.
22. Gao, X., et al., *Information security investment with budget constraint and security information sharing in resource-sharing environments.* Journal of the Operational Research Society, 2023. **74**(6): p. 1520-1535, DOI: 10.1080/01605682.2022.2096506