فصلنامه پژوهش‌های حفاظتی ـ امنیتی
دانشگاه جامع امام حسین(علیه‌السلام)
سال سیزدهم، شمارهٔ ۱ (بهار ۱۴۰۳) صص۹۵—۱۳۱

فرصت‌ها و تهدیدهای گمنامی فنی در فضای سایبر و راه‌کارهای مقابله با آن برای سازمان‌های اطلاعاتی ـ امنیتی

● احمد زوار تربتی[1] ●

استادیار دانشگاه علوم و فنون فارابی، تهران، ایران (نویسنده مسئول)

تاریخ دریافت: ۱۴۰۳/۰۱/۱۹ تاریخ پذیرش: ۱۴۰۳/۰۳/۱۷

چکیده

امنیت اطلاعات و ارتباطات یکی از مهم‌ترین تهدیدات استفاده از فضای سایبر است. عدم توجه به این تهدیدات به‌ویژه در سازمان‌های اطلاعاتی– امنیتی که نوع اطلاعات در اختیار آن‌ها محرمانه و حساس می‌باشد، بیش از سایر سازمان‌ها می‌تواند پیامدهای منفی و خطرآفرین به‌دنبال داشته باشد. در گذشته، بیشتر از علومی نظیر رمزنگاری برای بالا بردن امنیت اطلاعات استفاده می‌شده، اما اگر چه استفاده از این علوم، دسترسی به محتوای امن شده را مشکل یا غیرممکن می‌کند در بسیاری از موارد، منجر به هوشیاری و حساسیت افراد غیر مجاز خواهد شد و تلاش‌های کشف محتوا را در پیخواهد داشت. از این‌رو، استفاده از علم گمنام‌سازی، که با مخفی‌سازی همه اجزای ارتباط، مانع ایجاد حساسیت و هوشیاری نیز می‌گردد، اهمیت پیدا می‌کند. در استفاده از فناوری گمنامی در فضای سایبر، بسته به استفاده دشمن یا خودی از فناوری، دو وجه فرصت و تهدید مطرح است. این پژوهش به‌دنبال کشف فرصت‌ها، تهدیدات و راه‌کارهای مقابله‌ای با گمنامی نی در فضای سایبر است و با استفاده از روش تحلیل محتوای تفسیری با رویکرد استقرایی، از داده‌های به‌دست آمده از مصاحبه با ۲۰ نفر از خبرگان، مؤلفه‌های فرصت‌ها و تهدیدات گمنامی، در قالب مقوله‌های اصلی و فرعی (زیر مقوله‌ها) مشخص شدند و راه‌کارهای مقابله‌ای نیز در دو بخش فناورانه و مدیریتی دسته‌بندی گردیدند. روایی این پژوهش محتوایی– صوری است که توسط ده نفر از استادان مورد تأیید قرارگرفته است. برای پایایی نیز از فرمول هولستی استفاده شد که بر اساس فرمول محاسبه شده عدد ۸/۰ (بیش از ۷/۰) به‌دست آمده و بنابراین نتیجه حاصله از پایایی لازم برخوردار است.

کلید واژگان: گمنامی، فضای سایبر، سازمان‌های اطلاعاتی– امنیتی، تحلیل محتوا.

1.zavvarahmad@gmail.com

مقدمه

امروزه فضای سایبر که زاییده پیشرفت فناوری می‌باشد، تبدیل به بستری مناسب برای تعاملات در ابعاد مختلف گردیده که با ورود فناوری‌های جدید نظیر وب تاریک شکل تازه‌ای به‌خود گرفته و پیچیده‌تر شده است. مزایای فراوان فضای سایبر، همه را ناگزیر به استفاده از آن نموده؛ اما استفاده از این فضا، علاوه بر فرصت‌های فراوان، تهدیداتی را نیز در بر دارد. امنیت اطلاعات و ارتباطات یکی از مهم‌ترین تهدیدات استفاده از فضای سایبر است. وقتی که اطلاعات در بستری عمومی مبادله می‌گردد و افراد غیرمجاز نیز به اطلاعات دسترسی دارند، لزوم برقراری امنیت اطلاعات و ارتباطات ملموس‌تر می‌شود و مسایلی نظیر حفظ محرمانگی[1] و حریم خصوصی[2] کاربران اهمیت پیدا می‌کند. عدم توجه به این تهدیدات در سازمان‌ها، به‌ویژه در سازمان‌های اطلاعاتی- امنیتی که نوع اطلاعات در اختیار آن‌ها، محرمانه و حساس می‌باشد، بیش از سایر مؤسسات و سازمان‌ها می‌تواند پیامدهای منفی و خطرآفرین به‌دنبال داشته باشد. افشاگری‌های اخیر درباره برنامه‌های نظارت فراگیر در مقیاس جهانی نشان می‌دهند که حفظ حریم شخصی کاربران جهانی اینترنت در معرض خطر است. این افشاگری‌ها شامل مقادیر زیادی از داده‌های شخصی، فعالیت‌های مرور وب، اطلاعات مکانی و ارتباطات شخصی می‌باشد که به‌وسیله آژانس‌های امنیتی داخلی و خارجی به‌صورت انبوه برداشت شده‌اند. طراحی اینترنت که مستعد نظارت است، با کاهش هزینه ذخیره داده‌ها، از طریق جمع‌آوری و ذخیره داده‌ها، نظارت انبوه را فراهم می‌نماید (چااو و همکاران، ۲۰۲۴).

با رشد فوق‌العاده تعداد کاربران اینترنت و پیشرفت سریع فناوری‌های وابسته در سال‌های اخیر، بسیاری از مردم مایل هستند تا فعالیت‌های روزانهٔ خود را از طریق سیستم‌های شبکه‌های توزیع شده انجام دهند. از سویی نیز مردم این نگرانی بزرگ را دارند که جزئیات فعالیت‌های شخصی‌اشان از طرف شخص ثالث دنبال شود. به بیانی بهتر، حفظ حریم شخصی مبحث مهمی در وب است؛ چرا که آدرس IP کاربران، نام دامنه آن‌ها، سازمان، وبسایت‌های بازدید شده، اطلاعات درخواست شده و ... به‌راحتی در دسترس است. این اطلاعات از طریق کارپذیرهای نهایی، مدیریت سیستم محلی و حتی دیگر اشخاص در دسترس است. این امر تهدیدی جدی برای حفظ حریم شخصی است (وینکلر و باچمن، ۲۰۱۸).

1. Confidentiality
2. Privacy

برای محافظت از حریم خصوصی افراد می‌بایست محتوای خصوصی یک ارتباط و اطلاعات افراد درگیر در یک ارتباط محرمانهٔ اینترنتی، مخفی باقی بماند. از تکنیک‌های مختلف «رمزنگاری»[1]، «مبهم‌سازی»[2] و «جدول کد»[3]، به‌منظور «نامفهوم‌سازی»[4] محتوای خصوصی (اطلاعات پیام) برای موجودیت‌های غیرمجازی که ممکن است به اطلاعات و ارتباط دسترسی یافته باشند استفاده می‌شود. استفاده از این علوم، درست است که دسترسی به محتوای امن شده را مشکل یا غیرممکن می‌کند، اما در بسیاری از موارد، افراد غیر مجاز را هوشیار می‌کند که حتماً محتوا با روشی امن گردیده؛ بنابراین حساسیت ایجاد می‌گردد و تلاش‌های کشف محتوا را در پی‌خواهد داشت. از این‌رو، استفاده از تکنیک‌های مخفی‌سازی، که مانع ایجاد حساسیت و هوشیاری نیز می‌گردند، اهمیت پیدا می‌کند. برای موفقیت در امن‌سازی، بایستی ایمن‌سازی همه اجزای یک ارتباط (اطلاعات، فرستنده و گیرنده) مد نظر قرار گیرد و غیر از پیام، اطلاعات سایر اجزای ارتباط نظیر اطلاعات افراد درگیر در اتباط (طرفین ارتباط) نیز مهم است؛ به‌عنوان مثال اگر محرمانگی اطلاعات منتقل شده از طریق رمزنگاری تأمین شده باشد، پارامترهایی نظیر مبدأ و مقصد ارتباط قابل ردیابی است و شنودگر (یا هر موجودیت غیر مجاز دیگر) به سادگی می‌تواند کاربرِ در حال ارتباط، دفعات و مدت‌زمان ارتباط و طول پیام‌های ارسالی و دریافتی توسط وی را نیز شناسایی کند و از آن در جهت رسیدن به اهداف خود استفاده نماید (بنمزین و همکاران، ۲۰۱۱). تکنیک‌های «نهان‌نگاری»[5]، «نشانه‌گذاری حق کپی»[6]، «کانال پنهان (وششی، پوشیده یا مخفی)»[7]، «پوشش‌گذاری»[8] و «گمنامی»[9] با «مخفی‌سازی»[10] اطلاعات سایر اجزای ارتباط از دید و تشخیص موجودیت‌های غیر مجاز، به محافظت از حریم خصوصی در ارتباطات کمک می‌کنند. بر این اساس می‌توان دو سرشاخهٔ اصلی «نامفهوم‌سازی» و «مخفی‌سازی» را به‌عنوان روش‌های تأمین اینیت اطلاعات در نظر گرفت که نامفهوم‌سازی شامل سه زیر شاخه

1. Cryptography
2. Obfuscation
3. Code Table
4. Obscuring
5. Steganography
6. Copyright Marking
7. Covert Channel
8. Masking
9. Anonymity
10. Information Hiding

اصلی «رمزنگاری»، «مبهم‌سازی» و «جدول کد» است و مخفی‌سازی نیز شامل پنج زیرشاخهٔ اصلیِ نهان‌نگاری، نشانه‌گذاری حق کپی، انال پنهان، پوشش‌گذاری و گمنامی می‌باشد.

در این پژوهش به گمنامی در فضای سایبر پرداخته خواهد شد. موضوع امنیت شبکه درسال‌های گذشته در چهار محور محرمانگی، بی‌عیبی، در دسترس بودن و صحت دنبال می‌شود؛ اما مطالعات اخیر در بحث امنیت، گمنامی را نیز به‌عنوان یکی از مهم‌ترین شاخص‌های امنیت اطلاعات معرفی نموده است. در سازمان‌های بزرگ، اطلاعات حساسی وجود دارد که دشمنان می‌خواهند با نفوذ در آن‌ها در توسعه سازمان، اختلال ایجاد کنند. از این‌رو، این سازمان‌ها می‌خواهند ارتباطات مربوط به این اطلاعات را به‌صورت ناشناس انجام دهند. بنابراین برای حفظ حریم شخصی باید بتوان ارتباط را به‌صورت گمنام برقرار کرد (وینکلر و باچمن، ۲۰۱۸).

امروزه گستردگی شبکه‌های امن سازمانی به اندازه‌ای نیست که بتوان از هر نقطه‌ای (حتی در خارج از کشور) با سازمان مورد نظر ارتباط سریع برقرار کرد. این نیاز ارتباطی باعث می‌شود که برخی از کاربران به ناچار از بستر غیر امن اینترنت استفاده نمایند. در این بستر برای برخی از مأموریت‌ها که نیاز به مخفی ماندن «وجود ارتباط پنهانی» است علاوه بر روش‌های امن‌سازی اطلاعات، باید از روش‌های پوششی نیز استفاده کرد. همچنین برای برخی از کاربران خاص، نیاز است که «وجود هرگونه ارتباط مخفی یا غیرمخفی» نیز آشکار نگردد، پس باید با استفاده از روش‌هایی، گمنامی یک یا همهٔ عناصر دخیل در این ارتباط تأمین گردد.

عناوین مختلف پژوهشی به موضوع مواجهه شرکت‌ها، سازمان‌ها و دولت‌ها با فناوری‌ها و علوم نوظهور پرداخته‌اند و از جنبه‌های مختلف، پذیرش علوم و فناوری‌های نوظهور را بررسی نموده‌اند. مزایای استفاده از علوم و فناوری‌های نوظهور، فرصت‌هایی را ایجاد می‌کند که افراد، شرکت‌ها، سازمان‌ها و دولت‌ها را متقاعد می‌کند تا در کاربردهای مختلف از علوم و فناوری‌های نوظهور بهره گیرند هرچند استفاده از فناوری‌ها و علوم نوظهور، علاوه بر فرصت‌ها، تهدیداتی را نیز به‌وجود آورد است. بسیاری از تهدیدات حوزه گمنامی، ناشی از بهره‌گیری معاندین از بستر گمنامی در فضای سایبر است. در این پژوهش، سعی شده با بررسی فرصت‌ها و تهدیدات گمنامی فنی در فضای سایبر و راه‌کارهای مقابله با آن برای سازمان‌های اطلاعاتی– امنیتی، زمینه مواجهه آگاهانه با علم گمنامی فراهم شود.

طبق بررسی نگارندگان این مقاله، تاکنون موضوع این پژوهش در نشریات معتبر مورد بررسی

قرار نگرفته است. برخی از مواردی که بر اهمیت انجام این پژوهش دلالت می‌کند عبارت‌اند از:

۱- تعیین و تشریح ابعاد مختلف مزایا، معایب، فرصت‌ها و تهدیدات استفاده از بستر گمنامی در فضای سایبر و ضرورت مواجهٔ آگاهانهٔ سازمان‌های اطلاعاتی- امنیتی با آن.

۲- تعیین کاربردهای مختلف استفاده از بستر گمنامی در فضای سایبر.

۳- شناسایی و تعریف بهینه نیازمندی‌های پژوهشی در زمینه تأمین تجهیزات گمنام‌ساز

۴- تبیین ملاحظات طراحی و پیاده‌سازی یک شبکهٔ ارتباطی گمنام به‌منظور ایجاد بستری برای تبادل امن و پوششی پیام و اطلاعات در راستای اهداف سازمان‌های امنیتی - اطلاعاتی.

۵- برررسی و ارائه راهکارهای امنیتی باهدف به‌کارگیری سامانه‌های گمنام‌ساز در سازمان‌های اطلاعاتی- امنیتی.

علاوه بر موارد بالا، مواردی نیز وجود دارند که انجام این پژوهش را ضروری می‌نمایند. مزایای علم گمنامی، خودی و غیر خودی را مجاب می‌کند از بستر گمنامی استفاده کنند، اما خالق علم گمنامی، بیگانان هستند و بایستی در مواجه با این علم آگاهانه عمل کرد و الزامات لازم برای مقابله با تهدیدات احتمالی را رعایت نمود. توجه نداشتن به این الزامات در حفظ گمنامی فنی در فضای سایبر، ممکن است تبعات جبران‌ناپذیری به افراد، سازمان‌ها و یا حتی کشورها وارد نماید. بنابراین ضروری است که ابعاد مختلف فرصت‌ها و تهدیدات استفاده از بستر گمنامی در فضای سایبر مشخص و راه‌کارهای مقابله‌ای پیشنهاد گردد. برخی از موارد دیگر که بر ضرورت انجام این پژوهش تأکید می‌کنند بدین شرح هستند:

۱- عدم آگاهی مدیران و کارشناسان مأموریتی از علم گمنامی و در نتیجه عدم استفاده از بستر گمنامی در ارتباطات مأموریتی در سازمان‌های اطلاعاتی- امنیتی و محروم شدن از مزایا و فرصت‌های استفاده از علوم نوظهور.

۲- عدم آشنایی با الزامات پدافند غیرعامل، استفاده از ابزارها و بستر گمنامی در فضای سایبر در ارتباطات حساس.

۳- عدم حمایت و پشتیبانی مدیران از اقدامات مرتبط با تهیه، تأمین، طراحی، پیاده‌سازی و استفاده از ابزارها و بستر گمنامی در فضای سایبر.

۴- عدم نظارت و کنترل تعاملات معاندین در بستر گمنامی فضای سایبر به علت عدم آشنایی مدیران و کارشناسان مأموریتی از علم گمنامی و راه‌کارهای نظارتی مربوطه.

طبق بررسی نگارندگان این مقاله، تاکنون موضوع این پژوهش در نشریات معتبر مورد بررسی قرار نگرفته است و از طرفی با توجه به ماهیت پیچیده اقدامات در سازمان‌های اطلاعاتی-امنیتی نمی‌توان از روش‌های کمی به شناخت کافی نسبت به موقعیت‌های معین دست یافت، از این‌رو استفاده از روش‌های کیفی ضرورت پیدا می‌نماید. پژوهش حاضر مطالعه‌ای نمی است و با استفاده از روش تحلیل تفسیری با رویکرد استقرایی و با روشی ساختارمند، از اجزای داده‌های به‌دست آماده از مصاحبه‌ها، به مؤلفه‌های فرصت‌ها، تهدیدات و راه‌کارهای مقابله‌ای گمنامی فنی در فضای سایبر پرداخته شده است. در این پژوهش، بعد از استخراج کدهای باز از مصاحبه‌های انجام شده با ۲۰ نفر از خبرگان حوزه پژوهش، زیر مقوله‌ها و سپس مقوله‌های محوری مشخص شده‌اند و در نهایت نیز نتایج دسته‌بندی شده ارائه گردیده‌اند. در بخش راهکارهای مقابله‌ای، نتایج در دو دسته راهکارهای فناورانه و مدیریتی ارائه شده‌اند.

مفاهیم و مبانی نظری

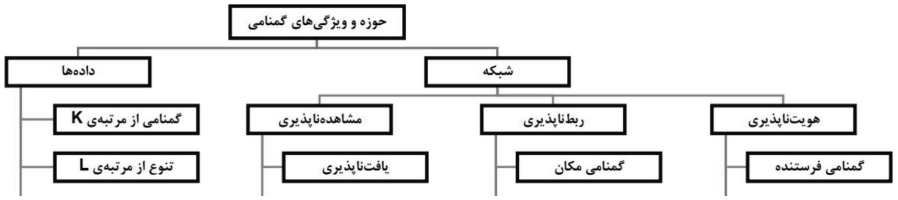
تعریف گمنامی

گمنامی به وضعیتی گفته می‌شود که در آن موجودیت مورد نظر در بین مجموعه‌ای از موجودیت‌های مشابه (مجموعهٔ گمنامی)، غیر قابل شناسایی باشد. «مجموعهٔ گمنامی» به مجموعه موجودیت‌هایی گفته می‌شود که ممکن است یک عمل مورد نظر (نظیر دریافت یا ارسال بسته‌های داده) را انجام داده باشند (نوس و همکاران، ۲۰۲۳). پس هرقدر مجموعهٔ گمنامی یک ابزار نظیر تعداد کاربران فعال آن و یا تعداد حالات ممکن برای وقوع یک رخداد، بزرگتر و بیشتر باشد، گمنامی بیشتری توسط آن ابزار یا روش تأمین خواهد گشت.

طبق تعریف مندرج در (فیتزمن و هانسن، ۲۰۰۸)،گمنامی از دید یک شنودگر، حالتی است که همه عامل‌های موجود می‌توانند فرستنده یا گیرنده یک پیام باشند. این تعاریف در حوزهٔ شبکه مطرح می‌باشد یعنی فرستنده، گیرنده، پیام و کانال در آن اهمیت دارد. اما گمنامی در حوزهٔ داده‌ها وصاً در هنگام ذخیره‌سازی و تجمیع آن‌ها در بانک‌های اطلاعاتی نیز مطرح است و اغلب بر روی حذف یا پوشاندن اطلاعات قابل شناسایی متمرکز شده‌اند (کرستین و همکاران، ۲۰۲۰). این روش‌ها در ادامه تشریح می‌گردد.

انواع گمنامی

بر اساس بررسی‌ها و جمع‌بندی انجام شده توسط نگارنده، با استفادهٔ ترکیبی از طبقه‌بندی‌های ارائه شده در (ادمن و ینر، ۲۰۰۹) و (شیرعلی و همکاران، ۲۰۲۳) و تکمیل آن می‌توان طبقه‌بندی زیر را بر اساس ویژگی‌های گمنامی به‌صورت شکل ۱ ارائه داد.



شکل ۱: ز رشاخه‌های گ نامی

گمنامی در حوزهٔ شبکه

هویت‌ناپذیری: هویت‌ناپذیری[1] یعنی دشمن قادر به تشخیص هویت عامل و یا گروه، اقدامات یا دیگر موارد مورد علاقه در میان مجموعهٔ مشابهی از عامل‌ها یا گروه نیست. هویت‌ناپذیری به چهار بخش زیر تجزیه می‌گردد (شیرعلی و همکاران، ۲۰۲۳):

گمنامی فرستنده (مبدأ) : گمنامی فرستنده[2] (SA) ، به معنای غیر قابل شناسایی بودن هویت مبدأ یک پیام، در مجموعه گمنامی فرستنده است. به‌عبارت‌دیگر، گمنامی فرستنده به معنای ربط‌ناپذیری یک پیام خاص با هویت هیچ فرستندهای و ربط‌ناپذیری هویت یک فرستنده با هیچ پیامی تعریف می‌شود (شیرعلی و همکاران، ۲۰۲۳) و (نوس و همکاران، ۲۰۲۳). به‌طور کلی مخفی ماندن هویت فرستنده از دید دشمنی که در سمت گیرنده قرار دارد هدف اصلی این نوع گمنامی است.

منامی گیرنده (مقصد): امی گیرنده (RA)[3] یعنی غیر قابل شناسایی بودن مقصد یک پیام، در مجموعه‌ی گمنامیِ گره‌های گیرنده. به عبارت دیگر، گمنامی گیرنده با ربط‌ناپذیری یک پیام خاص با هویت هیچ گیرنده‌ای و ربط‌ناپذیری هویت یک گیرنده چ پیامی تعریف

1. Unidentifiability
2. Sender Anonymity (SA)
3. Receiver Anonymity (RA)

می‌شود (شیرعلی و همکاران، ۲۰۲۳) و (نوس و همکاران، ۲۰۲۳) و مخفی ماندن هویت گیرنده از دید دشمنی که در سمت فرستنده قرار دارد هدف این نوع گمنامی است.

نامی متقابل (دوطرفه): نامی متقابل (MA)[1] ، نه تنها هویت فرستنده و گیرنده را از دشمن پنهان می‌دارد بلکه هویت فرستنده را از گیرنده و هویت گیرنده را از فرستنده پنهان می‌سازد (شیرعلی و همکاران، ۲۰۲۳).

گمنامی گروه: گمنامی گروه (GA)[2] ، مانع از ارتباط پیام خاص به یک گروه از عوامل (فرستندگان یا گیرندگان) می‌شود (کیان و همکاران، ۲۰۲۴).

ربطناپذیری: ربط‌ناپذیری[3] یعنی دشمن قادر به ارتباط دادن عامل‌ها، پیام‌ها، اقدامات و یا دیگر موارد مورد علاقه از طریق مشاهدهٔ سیستم نباشد و خود متشکل از سه حالت زیر است (شیرعلی و همکاران، ۲۰۲۳).

گمنامی محل (مکان): گمنامی مکان (LA)[4] ، یعنی یک پیام خاص را نتوان به محل فرستنده یا گیرنده، حرکت، مسیر و یا توپولوژی مرتبط نمود (شیرعلی و همکاران، ۲۰۲۳).

گمنامی ارتباطات (ارتباط): گمنامی ارتباطات (CA)[5] ، یعنی یک پیام خاص را نمی‌توان به هر جفت فرستنده-گیرنده مرتبط نمود و هیچ پیامی را نمی‌توان به یک جفت خاص فرستنده-گیرنده مرتبط نمود (شیرعلی و همکاران، ۲۰۲۳).

گمنامی ارتباطات گروه: گمنامی ارتباطات گروه (GCA)[6] ، یعنی پیام خاصی را نمی‌توان به هر جفت گروه فرستندگان- گیرندگان مرتبط نمود و هیچ پیامی قابل پیوند به جفت گروه فرستندگان- گیرندگان نمی‌باشد (شیرعلی و همکاران، ۲۰۲۳).

1. Mutual Anonymity (MA)
2. Group Anonymity (GA)
3. Unlinkability
4. Location Anonymity (LA)
5. Communication Anonymity (CA)
6. Group Communication Anonymity (GCA)

مشاهده‌ناپذیری: در بیشتر منابع، گمنامی به همان دو ویژگی پیش‌گفته یعنی هویت‌ناپذیری و ربط‌ناپذیری تعریف می‌شود و در برخی از منابع، افزودن ترافیک ساختگی[1] برای دستیابی به ویژگی سومی با عنوان مشاهده‌ناپذیری[2] مطرح شده است (نوس و همکاران، ۲۰۲۳). طبق این تعریف وقتی که دشمنان درحال مشاهدهٔ شبکه باشند، می‌توانند فرستنده‌ها و گیرنده‌های محلی را ببینند، اما نمی‌توانند تشخیص دهند که ارتباط بین چه کسانی برقرار است (شیرعلی و همکاران، ۲۰۲۳). در حالت کلی جهت دستیابی به مشخصه مشاهده‌ناپذیری، سیستم باید برای تأخیر دل‌خواه در ارسال پیام و تزریق ترافیک کاذب مجوز داشته باشد (وینکلر و باچمن، ۲۰۱۸). برخلاف گمنامی که در آن‌ها تن‌ها ارتباط موجودیت‌ها با شناسه‌ها یا دیگر موجودیت‌ها حفاظت می‌شود، در مشاهده‌ناپذیری، خود موجودیت‌ها نیز قابل تمیز از یکدیگر نیستند. در واقع موجودیت‌ها شبیه به نویز تصادفی هستند که هیچ تفاوتی با یکدیگر ندارند. همان‌طورکه در تعریف گمنامی، گمنامی در داخل مجموعهٔ گمنامی تعریف می‌شود، در اینجا نیز از مفهوم مجموعهٔ مشاهده‌ناپذیری استفاده می‌شود. منظور از مجموعهٔ مشاهده‌ناپذیری، مجموعه‌ای است که موجودیت در آن‌ها مشاهده‌ناپذیر می‌گردد (نوس و همکاران، ۲۰۲۳). البته در (فیتزمن و هانسن، ۲۰۰۸) این مفهوم با عنوان «یافت‌ناپذیری»[3] معرفی گردید و مشاهده‌ناپذیری، یافت‌ناپذیری موجودیت (به‌عنوان مثال ارسال پیام) از دید ناظران بیرونی به همراه گمنامی ناظران درونی (فرستنده و گیرندهٔ پیام) از دید یکدیگر، تعریف می‌گردد.

طبق تعریف ارائه شده در (شیرعلی و همکاران، ۲۰۲۳) مشاهده‌ناپذیری یعنی فرد بداندیش قادر به مشاهده موارد مورد علاقه بر خلاف هویت یا روابط عامل[4] نیست. مشاهده‌ناپذیری از دو طریق حاصل می‌شود. اول اینکه فرد بداندیش قادر به مشاهدهٔ هیچ‌گونه پیام یا موارد مورد علاقه از سوی عامل نباشد (خواه موارد مورد علاقه وجود داشته باشد یا نه). دوم اینکه، گمنامیِ عامل(های) دیگرِ مرتبط با موارد مورد علاقه، با سایر عامل‌ها یکسان باشد. به‌عنوان‌مثال، تمام عامل‌ها به‌طور همزمان پیام یکسانی را در سراسر شبکه ارسال نمایند. مشاهده‌ناپذیری بر گمنامی با غیر قابل تشخیص نگه

1. Dummy Traffic
2. Unobservability
3. Undetectable
4. agent

داشتن[1] پیام‌ها و همچنین گمنامی هویت‌ها[2] دلالت می‌نماید؛ بااین‌حال، تأمین همزمان هویت‌ناپذیری و ربط‌ناپذیری به مشاهده‌ناپذیری دلالتی ندارد (شیرعلی و همکاران، ۲۰۲۳).

گمنامی در حوزهٔ داده‌ها: گمنامی علاوه بر حوزه شبکه در حوزه داده‌ها نیز تعریف می‌شود که به معنای عدم امکان شناخت یک موجودیت از روی اطلاعاتی به غیر از شناسه است. این شاخه از گمنامی امروزه مخصوصاً در حوزهٔ پزشکی و حفظ حریم خصوصی بیماران و نگهداری سوابق پزشکی آنان کاربرد گسترده‌ای یافته است. به‌عنوان‌مثال در یک پایگاه داده ممکن است از روی اطلاعات تاریخ تولد و جنسیت بتوان افراد را بدون دانستن شناسه افراد (کد ملی) شناسایی نمود. به‌منظور جلوگیری از این نوع حملات در حوزهٔ حریم خصوصی از اصطلاحاتی در حوزه گمنامی داده استفاده می‌شود که در ادامه تشریح شده‌اند.

گمنامی از مرتبه K: برای گمنامی از مرتبه K^3 نیاز است تا با کمک اجماع‌گیری و کلی‌سازی اطلاعات غیر حساس، هر مجموعه از اطلاعات غیر حساس دارای حداقل K نمونه باشند. به‌عنوان‌مثال می‌توان داده غیر مهم سن را به‌صورت بازهای تعریف نمود. همچنین تنها چند رقم اول کد پستی را ذخیره نمود. به این ترتیب درصورتی‌که مجموعه‌ای از اطلاعات غیر مهم در کنار هم در اختیار مهاجم قرار گیرند، مهاجم نمی‌تواند موجودیت مورد نظر را شناسایی نماید (لین، ۲۰۲۴).

تنوع از مرتبه L: معیار تنوع از مرتبه L^4 ، برای رفع نواقص گمنامی از مرتبه K ارائه شد. حالتی را در نظر بگیرید که با یک مجموعه از اطلاعات غیر حساس، به K موجودیت برسیم که همگی دارای اطلاعات حساس یکسانی باشند. به‌عنوان‌مثال تمامی این K موجودیت دارای یک بیماری باشند. دراین‌صورت، مهاجم به خواسته خود که دانستن بیماری سوژه مورد نظر است دست می‌یابد. تنوع از مرتبه L اطمینان حاصل می‌کند که در هر مجموعهٔ K گمنامی، حداقل L تنوع در داده‌های حساس وجود داشته باشد (کیان و همکاران، ۲۰۲۴).

1. indistinguishable
2. identities anonymous
3 K-anonymity.
4. L-diversity

نزدیکی از مرتبه T: معیار نزدیکی از مرتبه T[1] نیز برای بهبود معیار تنوع از مرتبه L پیشنهاد شد. هدف از این معیار یکسان‌سازی پراکندگی داده‌های حساس در هر گروه گمنامی از مرتبه K با پراکندگی داده‌ها در کل جدول است. به این منظور تفاوت این دو پراکندگی نباید بیشتر از T باشد. در غیر این صورت مهاجم می‌تواند محدودهٔ داده حساس در گروه گمنامی از مرتبه K را استخراج کند و تا حدودی به اطلاعات مورد نظر خود دست یابد (دی ویمرکتی و همکاران، ۲۰۲۳).

جمع‌بندی

برای تأمین گمنامی کامل در حوزهٔ شبکه نیاز به تأمین هم‌زمان سه ویژگیِ «هویت‌ناپذیری»، «ربط‌ناپذیری» و «مشاهده‌ناپذیری» و برای تأمین گمنامی کامل در حوزهٔ داده نیاز به رعایت هم‌زمان سه ویژگی «گمنامی از مرتبهٔ k»، «تنوع از مرتبهٔ L» و «نزدیکی از مرتبهٔ T» است. هدف از گمنامی در این دو حوزه، ناتوان‌سازی دشمن از شناسایی فرستنده / گیرنده / ارتباط و پیام مبادله شده بین آن‌ها و کمینه‌سازی میزان بهره‌برداری او از محتوای اطلاعات (در صورت دسترسی) تا حد ممکن است. پیش از تهیه و استفاده از ابزارهای گمنام‌ساز، می‌بایست پاسخ پنج پرسش کلیدی زیر را برای هر هدف مشخص نمود تا بتوان راه‌کار مناسب برای تأمین گمنامی را برگزید:

۱- چه چیزی/ شخصی باید گمنام شود؟ (بررسی ملزومات گمنامی فرستنده، گیرنده، پیام، دو طرفه، گروه و...).

۲- از دید چه شخصی باید مخفی شود؟ (بررسی توانایی و موقعیت دشمن، حملات و ...)

۳- برای چه کاربردی باید مخفی شود؟ (بررسی کاربردهای ارتباط کم‌تأخیر و پرتأخیر بی‌سیم، باسیم و ترکیبی)

۴- فرستنده و گیرنده در چه بستری هستند؟ (بررسی اندازه جمعیت گمنامی، گروه‌های جمعیتی، میزان ترافیک پایدار شبکه و..)

۵- چگونه باید مخفی شود؟ (بررسی شبکه‌ها، روش‌ها و ابزارهای تأمین گمنامی)

به‌عنوان نمونه اگر امکان تأمین جمعیت گمنامی برای یک ابزار تولید شده برای ارتباط گمنام وجود نداشته باشد، استفاده از آن ابزار به‌عنوان گمنام‌ساز به مصلحت نیست؛ چرا که نه تنها باعث ایجاد گمنامی نمی‌شود بلکه با اندکی بررسی و به علت تعداد کاربران بسیار کم و محدود آن شبکه

1. T-closeness

یا ابزار، استفاده ننمودن از تکنیک‌های فریب و نبود ترافیک پوششی برای آن ارتباط، کل شبکه ارتباطی (فرستندگان و گیرندگان) قابل کشف خواهد بود. بنابراین با توجه به کاربرد و سطح امنیتی مورد نیاز، می‌بایست اقدامات امنیتی مورد نیاز در هر لایه را انتخاب و به نحو مطلوب اجرا نمود.

در هر ارتباط سه بخش فرستنده، گیرنده و کانال ارتباطی وجود دارد که امر تولید و ارسال، انتقال و دریافت پیام را برعهده دارند. بسته به وضعیت این اجزا، چهار روش ارتباطی زیر قابل تعریف و استفاده‌اند:

۱- ارتباط آشکار: در این نوع ارتباط، فرستنده، گیرنده، پیام و کانال ارتباطی معلوم است.

۲- ارتباط امن: هدف از این نوع ارتباط، نامفهوم بودن پیام برای دشمن است و اغلب با استفاده از رمزنگاری پیام یا کانال ا صاصی رمزشده انجام می‌شود. این روش ارتباطی ممکن است باعث حساس شدن دشمن شود زیرا وجود یک ارتباط محرمانه برای او محرز است و فرستنده و گیرنده آن یز قابل شناسای ند. همچنین ممکن است اطلاعاتی در مورد مرورگر، سیستم عامل، زمان، مدت و تعداد دفعات ارتباط و... نیز برای دشمن مشخص شود. به‌طورکلی هنگام فعالیت در فضای سایبر، اطلاعات گوناگونی از کاربر در این فضا منتشر می‌گردد. به‌عنوان‌مثال زمانی که فردی از طریق یک مرورگر اقدام به جست‌وجوی مطلبی می‌کند و یا یک صفحهٔ وب را باز می‌کند، در حال ارسال اطلاعاتی می‌باشد که حتی در صورت استفاده از ارتباط رمزشده (امن) نیز این اطلاعات به‌صورت خودکار و بدون دخالت کاربر منتشر می‌گردد. برخی از این موارد عبارت‌اند از: ۱- آدرس اینترنتی[1] مبدأ ۲-آدرس اینترنتی مقصد ۳-آدرس MAC مبدأ ۴- موقعیت جغرافیاییِ مبدأ و مقصد به‌صورت تقریبی (و شاید دقیق با استفاده از اطلاعات جانبی وابسته به سیستم مورد استفاده در صورت وجود و فعال بودن نظیر GPS، موقعیت آنتن BTS و...) ۵- نوع سیستم عامل ۶- ۀ سیستم عامل ۷- نوع مرورگر و شماره نسخهٔ آن ۸- رمز یا کشف بودن ارتباط ۹- پروتکل‌های ارتباطی ۱۰- تعداد دفعات ارتباط ۱۱- تاریخ ارتباط ۱۲- طول زمان ارتباط ۱۳- طول پیام‌های ار الی و دریافتی ۱۴- اندازه صفحه نمایش (ابعاد مانیتور). همچنین ممکن است به علت اشتباهات آگاهانه یا ناآگاهانه کاربران، اطلاعات دیگری هم آشکار گردد. پس احتمال دارد دشمن برای شنود، رمزشکنی، تداخل، جعل یا قطع ارتباط، و... اقدام نماید.

1. IP: Internet Protocol

ارتباط پوششی: مخفی ماندن وجود پیام محرمانه برای دشمن، هدف اصلی این نوع ارتباط است و برای عادی نشان دادن ارتباط از یک پوشش مناسب نظیر روش‌های سنتی جوهرهای نامرئی‌نویسی یا روش‌های نهان‌نگاری در متن[۱] ، صوت[۲] ، تصویر[۳] ، ویدئو[۴] ، پروتکل‌های شبکه[۵] ، قالب فایل‌ها[۶] ، فضاهای بلااستفاده[۷] و یا روش‌های ابتکاری[۸] دیگر استفاده می‌شود. به علت مخفی نبودن وجود ارتباط بین گیرنده و فرستنده، احتمال شک‌برا یز بودن آن برای دشمن و در نتیجه تلاش برای قطع ارتباط، نهان‌کاوی و . . . وجود دارد.

ارتباط گمنام: مخفی ماندن وجود هرگونه ارتباط بین فرستنده و گیرنده هدف اصلی این نوع ارتباط است که بسته به کاربرد ممکن است گمنامی فرستنده، گیرنده ویا ارتباط میان آن‌ها با استفاده از روش‌هایِ تأمین گردد که در ادامه به‌طور کامل تشریح می‌گردد.

از دید یک کاربر اینترنت، «گمنامی»[۹] به معنای مخفی بودن شناسهٔ کاربر از دید مهاجم، در حین استفاده از خدمات اینترنت است. «شناسه» به زیرمجموعه‌ای از خصیصه‌های[۱۰] یک موجودیت گفته می‌شود، که آن موجودیت را از دیگر موجودیت‌های موجود متمایز می‌کند. در شبکه‌های رایانه‌ای،

1. Text steganography (Format-based methods, Random and statistical generation methods, and Linguistic methods)
2. Audio steganography (Speech and Music Steganography)
3. Image steganography (Photo, Paint, Graphics Interchange, and 3D Image Steganography)
4. Video steganography (Format-based methods, Technique-based method, and other methods)
5. Network Protocols steganography (Steganography in Intra-protocols and Inter-protocols)
6. Steganography in File-Format (PDF format, Portable Executable File, attaching or binding in a file, and etc)
7. Steganography in Unused Spaces (such as: Latent Data, Unallocated Space, slack space, HPA (Host Protected Area), and Reserved areas (Header and Footer))
8. Contraption Steganography (such as: Captcha, Barcode, QR-Code, Sudoku Table, Online Games, Circuitry, Human genomic DNA, and etc)
9. Anonymity
10. Attribute

شناسه می‌تواند از آدرس کنترل دسترسی رسانه (MAC)[1]، آدرس پروتکل اینترنت (IP)[2]، مکان جغرافیایی، یا آدرس پست الکترونیکی تشکیل شده باشد.

هدف از گمنامی، مخفی کردن و حذف اطلاعات مربوط به شناسهٔ کاربر است. با این وجود، در صورت نیاز می‌توان از طریق کانال گمنامی ایجاد شده بین فرستنده و گیرنده، اطلاعات مربوط به شناسه را به مقصد منتقل نمود. به‌منظور داشتن گمنامی، نیاز به مجموعه‌ای از موجودیت‌های مشابه با خاصیت‌های یکسان ا ت که به آن «مجموعه‌ی گمنامی»[3] گفته می‌شود.

بنابر تعریفی که در (نوس و همکاران، ۲۰۲۳) آمده، «گمنامی به وضعیتی گفته می‌شود که در آن موجودیت مورد نظر در بین مجموعه‌ای از موجودیت‌های مشابه (مجموعهٔ گمنامی)، غیر قابل شناسایی باشد». «مجموعهٔ گمنامی به مجموعه موجودیت‌هایی گفته می‌شود که ممکن است عمل مورد نظر را انجام داده باشند (به‌عنوان‌مثال این عمل می‌تواند دریافت یا ارسال بسته باشد)». به‌عبارت‌دیگر (نوس و همکاران، ۲۰۲۳) « منامی حالتی است که (از دید یک شنودگر) همه عامل‌های ممکن می‌توانند فرستنده یا گیرنده یک پیام باشند».

تزمان[4] و هانسن[5] در راستای استانداردسازی واژه‌های مورد استفاده در ادبیات سیستم‌های ارتباط گمنام، قاله‌ای نوشتند و اصطلاحات خود را ارائه کردند. طبق تعریف آن‌ها گمنامی عبارت است از «ناشناخته ماندن هویت در یک مجموعه». به‌عبارت‌دیگر گمنامی حالتی است که (از دید یک شنودگر) همه عامل‌های ممکن می‌توانند فرستنده یا گیرنده یک پیام باشند (آدوم و همکاران، ۲۰۲۳). به‌طورکلی یک سیستم گمنامی تلاش می‌کند تا بین پیام ارسال شده و گیرندهٔ واقعی (امی گیرنده) و بین پیام دریافت شده و ارسال‌کنندهٔ واقعی (گمنامی فرستنده)، «ربط‌ناپذیری»[6] به‌وجود آید (ادمن و ینر، ۲۰۰۹) ناشناسی پیوند بدین معنی است که در بین فرستنده‌ها و گیرنده‌ها، دشمن نتواند تشخیص دهد که چه کسی با چه کسی در ارتباط است (فیتزمن و هانسن، ۲۰۰۸).

در اکثر منابع، ویژگی گمنامی بر حسب موقعیت دشمن و برای فرستنده، گیرنده و ارتباط تعریف

1. Media Access Control
2. Internet Protocol
3. Anonymity set
4. Pfitzmann
5. Hansen
6. Unlinkability

می‌شود. طبیعی است که گمنامی کامل در صورتی روی می‌دهد که هر سه نوع گمنامی (گمنامی گیرنده، گمنامی فرستنده و گمنامی ارتباط) به‌صورت هم‌زمان تأمین شود.

طبقه‌بندی پروتکل‌های گمنامی

تاکنون برای مقایسه و طبقه‌بندی پروتکل‌های گمنامی، دسته‌بندی‌های مختلفی ارائه شده است نظیر GSS[1] (والاسیچ و همکاران، ۱۹۹۲)، CPG[2] (ساکنا و همکاران، ۲۰۲۳)، CAT[3] (تیلویک و اولویر، ۲۰۰۵). سامپیگِثایا[4] و پووِندران[5] (گارسیا و تورگلوسی، ۲۰۲۴) پروتکل‌های گمنامی را به دو دسته نظیر به نظیر و شبکه‌های بتنی بر میکسنت‌ها تقسیم کرده و سپس رِن[6] و وُو[7] (کرامر و همکاران، ۲۰۲۳) پنج دستهٔ سامانه‌های میکسنت مبنا[8]، دیسینت مبنا[9]، مسیریِ ی مبنا[10]، نظیر به نظیر[11] و سایر را پیشنهاد نمودند. به تدریج با افزایش تعداد پروتکل‌ها و روش‌های أمین گمنامی، این مرزبندی‌ها نیز د تر شدند. اِدْمان[12] و یِنِر[13] (ادمن و ینر، ۲۰۰۹) از منظری دیگر، پروتکل‌های گمنامی را به دو نوع پرتأخیر[14] و کم‌تأخیر[15] طبقه‌بندی کردند. جامع‌ترین طبقه‌بندی پیشنهادی تا کنون، طبقه‌بندی «مکعبی» یا CT[16] است که توسط کِلی[17] و همکارانش در سال ۲۰۱۲ ارائه شد (شیرعلی و همکاران، ۲۰۲۳). با استفاده از این طبقه‌بندی سه بعدی میتوان بر اساس سه مؤلفهٔ ویژگی

1. A Group Support System (GSS) taxonomy
2. A lower-level Collaborative Peer Group (CPG) taxonomy
3. Connection Anonymity Taxonomy
4. Sampigethaya
5. Poovendran
6. Ren
7. Wu
8. Mixnet-based schemes
9. DC-net systems
10. Network routing-based techniques
11. Peer-to-Peer networks
12. Edman
13. Yener
14. HIGH-LATENCY ANONYMITY SYSTEMS
15. LOW-LATENCY ANONYMITY SYSTEMS
16. Cubic Taxonomy (CT)
17. Kelly

گمنامی (AP[1])، سطح تهدیدات (AC[2]) و نوع شبکه (NT[3])، به دسته‌بندی و مقایسهٔ پروتکل‌های تأمین گمنامی پرداخت. یک رویکرد دیگر که همواره به موازات طبقه‌بندی پروتکل‌های گمنامی مورد توجه بود، ارزیابی میزان گمنامیِ حاصل شده با استفاده از روش‌ها یا پروتکل‌های گمنامی ادعایی نظیر (میکائیل و همکاران، ۱۹۹۸)، (جانگ و همکاران، ۲۰۲۳)) و (پاتیل و هورالی، ۲۰۲۳) ا ت که درجات نزولی یا صعودی را برای میزان گمنامی پیشنهاد نموده‌اند. بررسی‌های نگارنده مقاله منجر به جمع‌بندی و ارائه طبقه‌بندی پارامترهای مختلف شبکه‌ها، پروتکل‌ها و روش‌های تأمین منامی بدین شرح شده است که به علت محدودیت مقاله، دسته‌بندی‌های مرتبط با هریک از این پارامترها و جزئیات تشریح نشده است (شیرعلی و همکاران، ۲۰۲۳): ۱-روش دست‌یابی به گمنامی ۲- کاربرد ۳- فاکتورهای امنیتی سیستم ۴- ارزیابی کمی و کیفی میزان گمنامی ۵- قابلیت دشمنی (تهدید) ۶- پیچیدگی کد ۷- وضعیت موجود (فعلی) پروتکل‌ها و ابزارها ۸- نوع شبکه (باسیم، بی‌سیم و ترکیبی) ۹- میزان تأخیر پروتکل‌ها ۱۰- حوزه (شبکه یا داده) ۱۱- ویژگی‌های گمنامی (هویت‌ناپذیری[4]، ربط‌ناپذیری[5] و مشاهده‌ناپذیری[6]).

پیشینه پژوهش

مرور ادبیات در بیشتر رویکردهای پژوهشی انجام می‌شود و هدف شناخت بیشتر مسئله مورد نظر و ابعاد مسئله است. مرور پیشینه نه گویای مفاهیم عمده و نه ارائه دهندهٔ فرضیه‌هاست بلکه مرور آن، نشانگر وجود شکاف یا نوعی سوگیری در دانش موجود است و در نتیجه اندک‌مایه‌ای برای مطالعه فراهم می‌آورد. این کار سطح نظری را ارتقا داده و ساخت تعاریف را بهبود می‌دهد. بر این اساس در این قسمت به نگاهی مختصر به ادبیات و برخی از پژوهش‌های داخلی و خارجی اکتفا می‌کنیم. موضوع این پژوهش با توجه به نیاز واقعی و خلأ موجود، مطرح شده است و به‌طور مستقیم در زمینهٔ این پژوهش کاری انجام نشده است اما برخی پژوهشات مرتبط با موضوع این پژوهش که در دسترس بوده‌اند و آن‌ها را می‌توان مبنا یا مؤید مباحث مطرح شده در این پژوهش قرار داد در ادامه آورده شده است.

1. Anonymity Property
2. Adversary Capability
3. Network Type
4. Unidentifiability
5. Unlinkability
6. Unobservability

برخی پژوهش‌ها به بررسی و اثبات نقاط قوت و ضعف ابزارها، پروتکل‌ها، روش‌ها و شبکه‌های گمنام‌ساز پرداخته‌اند. به‌عنوان‌مثال علیزاده و باقری در پژوهشی برای پرداختن به برخی ضعف‌های یک پروتکل گمنامی، امنیت پروتکل احراز اصالت و توافق کلید سبک وزن، جانبابائی و همکاران را مورد مطالعه و بررسی قرار داده و نشان داده‌اند که در برابر برخی حملات ناامن است. در نهایت نیز پیشنهادی برای بهبود پروتکل ارائه داده‌اند (علیزاده و باقری، ۱۴۰۱). همایون وهمکارانش در کار خود، با استفاده از یادگیری ماشین، غیر قابل تفکیک بودن و غیر قابل شناسایی بودن ترافیک شبکه گمنام‌ساز پارس از ترافیک عادی را بررسی کردند (همایون و همکاران، ۱۴۰۰). سلماسی‌زاده و همکارانش در پژوهشی حمل‌های جدید به شبکه مخلوط مرکب جیکوبسون ارائه داده‌اند که ویژگی صحت این شبکه مخلوط را نقض می‌کند. آن‌ها نشان داده‌اند که با استفاده از این حمله درصورت تبانی یکی از فرستنده‌ها با اولین سرور مخلوط‌کننده، این سرور قادر خواهد بود که پیام تمامی فرستنده‌ها را با پیام‌های دل‌خواه خود جایگزین کند (سلماسیزاده و همکاران، ۱۳۹۸). فراهانی و ماهان در مقاله‌ای پس از معرفی ایده NESA در زمینه گمنامی کوانتومی و مسئله شام رمزنگاران، گمنامی در رمزنگاری کوانتومی را تعریف نموده‌اند و سپس پروتکل‌های گمنامی گیرنده- شناس و فرستنده- ناشناس ارائه شده توسط Shi شرح داده شده و ایراداتی را که بر این دو پروتکل وارد هستند بیان نموده‌اند (فراهانی و ماهان، ۱۳۹۴).

در برخی از پژوهش‌ها، طراحی و پیاده‌سازی ابزارها، پروتکل‌ها، روش‌ها و شبکه‌های گمنام‌ساز پیشنهاد شده‌اند. به‌عنوان‌مثال مجاهد و همکارانش در پژوهشی یک پروتکل کامل برای احراز هویت، توافق کلید، و تبادل پیام ارائه داده‌اند که نسبت به حملات کوانتومی مقاوم است، از زنجیره قالب‌ها و قراردادهای هوشمند برای احراز هویت استفاده می‌کند و با استفاده از الگوریتم چرخ‌دنده دوتایی و رمزنگاری انتها- به- انتها از امنیت بالایی در تبادل پیام برخوردار است (مجاهد و همکاران، ۱۴۰۲). هاتفی و همکارانش در مقالهٔ خود، یک طرح پرداخت الکترونیک مبتنی بر زنجیره قالب را ارئه داده‌اند که علاوه بر قابلیت حفظ گمنامی و حریم خصوصی کاربران صادق، درصورت لزوم قادر به ردیابی و تنبیه کاربران مخرب بدون نیاز به استفاده از شخص سوم قابل اعتماد، نیز می‌باشد. آن‌ها از یک امضای کور عادلانه و یک طرح تسهیم راز استفاده کرده‌اند و برای حفظ گمنامی کاربران از نام‌های مستعار استفاده کرده‌اند (هاتفی و همکاران، ۱۴۰۰). حسنی کرباسی و همکارانش در کار خود معماری مبتنی بر Lattice و سیستم رمزنگار NTRU و امضای دیجیتال NSS پیشنهاد داده‌اند که منجر به اصلاح ساختار معماری شبکه‌های گمنام کلاسیک شده است و در مقابل حملات کوانتومی مقاوم است (حسنی کرباسی و همکارانش، ۱۳۹۳). امیری در پژوهشی

یـک چارچـوب گمنامی بـرای پیشـگیری از حملـهٔ دانـش پیش‌زمینـه، افشـای هویـت، و ویژگـی مالـکان طراحـی نموده است کـه سـودمندی داده‌های گمنـام را بیشـینه کنـد (امیری، ۱۳۹۹). رضازاده و همکارانش در پژوهش خود، روشی را برای پیاده‌سازی شبکه اقتضایی خودرویی با استفاده از زنجیره بلوکی پیشنهاد داده‌اند که اقدام به تأیید و ارسال تراکنش‌های حاوی اطلاعات می‌کند، به‌گونه‌ای که افزون بر توانایی رهگیری داده‌های تاریخچه‌ای، دارای امتیاز کلیدی دسترس‌پذیری بیشینه است و چالش همبندی را حل می‌کند. در روش پیشنهادی، چالش‌های سربار و تأخیر اولیه راه‌اندازی و گمنامی مسیر خودروهای ارسال‌کننده تراکنش حل شده و با به‌کارگیری رمزنگاری نامتقارن، گمنامی هویت تأمین گردیده است. چالش تحمل تأخیر زمان تولید و انتشار تعداد زیادی تراکنش جهت تکمیل یک بلوک بزرگ نیز مرتفع شده و امنیت تراکنش‌هایی که هنوز تحویل فرآیند زنجیره بلوک نشده‌اند مدیریت شده است (رضازاده و همکارانش، ۱۳۹۹). احمدی و نیکوقدم در مقاله خود، اثبات کرده‌اند که روش‌هایی که تا قبل از این مقاله، در شبکه‌های سیار سراسری پیشنهاد شده است نه تنها در مقابل برخی از حملات از جمله حمله تکرار، حمله داخلی، حمله جعل هویت کاربر، اپراتور مرجع و اپراتور کمکی و حمله منع سرویس آسیب‌پذیرند، بلکه برخی ویژگی‌های امنیتی از جمله گمنامی و عدم ردیابی کاربر، احراز هویت متقابل، محرمانگی کامل رو به جلو و امنیت کلید نشست را فراهم نمی‌آورند. آن‌ها در مقاله خود، یک طرح احراز هویت مبتنی بر کارت هوشمند برای شبکه‌های سیار سراسری ارائه داده‌اند که نه‌تنها ضعف‌های امنیتی موجود در طرح‌های پیشین را برطرف می‌سازد، بلکه احراز هویت متقابل میان هر سه موجودیت (کاربر، اپراتور مرجع و اپراتور کمکی) را به‌همراه حفظ گمنامی کاربر نیز فراهم می‌کند. در نهایت، نیز با مقایسه امنیت و کارایی طرح پیشنهادی با طرح‌های پیشین نشان داده‌اند که طرح پیشنهادی از امنیت و کارایی قابل قبولی برخوردار است (احمدی و نیکوقدم، ۱۳۹۸). جانبابائی و همکارانش در پژوهشی، پروتکل‌های احراز اصالت در حوزه اینترنت اشیا را بررسی و محدودیت‌ها و آسیب‌پذیری‌های امنیتی آن‌ها را تحلیل کرده‌اند و در نهایت نیز پروتکل احراز اصالت جدیدی پیشنهاد داده‌اند که گمنامی به‌عنوان یک پارامتر مهم در آن لحاظ شده است (جانبابائی و همکارانش، ۱۳۹۷). احمدی و همکارانش در پژوهشی، با پیاده‌سازی و ارزیابی روش نشان‌گذاری مبتنی بر فاصله، به‌عنوان یکی از روش‌های ردیابی نفوذ، نشان دادند که این روش دارای نقطه ضعف نقاط مرزی است و راهکاری برای بهبود روش مبتنی بر فاصله ارائه داده‌اند (احمدی و همکارانش، ۱۳۹۶). مهرجو و ستاری نائینی در کار خود، روشی برای حفظ حریم خصوصی شبکه‌های هوشمند برق از طریق الگوریتم گمنامی مرتبه k و رمزنگاری داده‌ها ارائه داده‌اند (مهرجو و ستاری نائینی، ۱۳۹۶). پورنقی و همکارانش، در کار خود طرح ارائه شده توسط لی و لای برای احراز

اصالت در شبکه‌های اقتضایی بین خودرویی مورد تجزیه و تحلیل قرار داده‌اند و سه سناریوی حمله به این طرح را، که امکان جعل امضای کاربر را به مهاجم می‌دهند، معرفی نموده‌اند و در ادامه نیز یک طرح بهبودیافته از طرح لی و لای را پیشنهاد داده‌اند (پورنقی و همکارانش، ۱۳۹۴).

برخی از منابع، به جنبه‌هایی از مزایا و تهدیدات گمنامی در فضای سایبر و عوامل مؤثر بر آن پرداخته‌اند به‌عنوان‌مثال کنعانی و همکارانش در پژوهشی توصیف و تبیینی از را ۀ گمنامی در صحنه مجازی با ویژگی‌های فردی و محیطی در آن صحنه با استفاده از نظریه نمایشی گافمن و ترکل سخن گفته‌اند. بر اساس یافته‌های این پژوهش، متغیرهای پایگاه تحصیلی و محدودیت‌های سنتی ۴۱/۵ درصد از تغییرات متغیر گمنامی در روابط اینترنتی را تبیین می‌کنند و کاربران اینترنت برای کاستن از بار محدودیت‌های سنتیِ مرتبط با ایجاد روابط در صحنه واقعی، از طریق گمنامی در صحنه مجازی، به‌عنوان کنشگری فعال ایفای نقش می‌کنند (کنعانی و همکارانش، ۱۳۹۷). مشایخ و همکارش در مقاله خود به شناسایی فرصت‌ها و تهدیدهای فضای مجازی و راه‌کارهایی برای کم شدن آسیب‌ها پرداخته‌اند (مشایخ و همکاران، ۱۴۰۲). معمار و همکارانش در پژوهشی به شبکه‌های اجتماعی مجازی و بحران هویت پرداخته‌اند و بحران‌های ناشی از گمنامی در شبکه‌های اجتماعی مجازی را به دو دسته تقسیم کرده‌اند: یک دسته بحران‌های کلی ناشی از مواجهه انسان با فضای مجازی، که از آن به اضطراب دیجیتالی یاد می‌کنند و دوم، بحران‌های ناشی از هویت‌های مجازی. پژوهش آن‌ها نشان داد که شبکه‌های اجتماعی مجازی، باعث تغییرات اساسی در نهادهای هویت‌ساز شده‌اند و عوامل معناساز هویتی را دست‌خوش تغییر نموده‌اند (معمار و همکاران، ۱۳۹۱). کنگاوری و همکاران در مقاله‌ای، با استناد به اینکه یکی از ویژگی‌های فضای مجازی گمنامی افراد است و نوجوانان و جوانان امروز بیشتر وقت خود را صرف حضور در این فضا کرده‌اند، با روش مروری و با استناد از منابع کتابخانه‌ای به روشن‌سازی نحوۀ تاثیرات فضای مجازی بر تغییر هویت نوجوانان پرداخته‌اند (کنگاوری و همکاران، ۱۴۰۲). عبداللهیان و همکاران در کار خود بـه مطالعـه و مقایسۀ ساختار، کنش‌های متقابل، گمنـامی و شـیوۀ بازتـاب «خـود» در چهار شبکۀ اجتماعی مجازی؛ ۱. چـتروم‌ها در یـاهو ۲.گروه‌های مجازی در یاهو ۳. شبکۀ قرارملاقـات اکیوپیـد و ۴. شـبکۀ اجتمـاعی فیسبوک پرداخته‌اند. نتـایج پژوهش آن‌ها نشان می‌دهد شیوۀ بازتاب «خود» تحت تأثیر ویژگی‌های ساختاری، گمنـامی یـا هنجارها در دنیای مجازی شکل می‌گیرد (عبداللهیان و همکاران، ۱۳۹۲). ترابیان نیز در مقاله‌ای با هدف آشنا کردن جوانان، نوجوانان و والدین آن‌ها آثار مثبت و منفی فضای مجازی را بررسی نموده است.

روش‌شناسی پژوهش

پژوهش حاضر در زمره پژوهشات کیفی جای می‌گیرد زیرا با استفاده از روش تحلیل تفسیری و با رویکرد استقرایی از اجزای داده‌های به‌دست‌آمده از مصاحبه‌ها با روشی ساختارمند به مفهوم و مؤلفه‌های فرصت‌ها، تهدیدها و راه‌کارهای مقابله‌ای ممانی فنی در فضای سایبر پرداخته است. این پژوهش را از نظر هدف، به‌واسطه پرداختن به موضوع مفهوم و یا مؤلفه‌های گمنامی فنی در فضای سایبر می‌توان در زمره پژوهشات توسعه‌ای قرار داد، زیرا به تبیین و بسط مفهوم گمنامی فنی می‌پردازد.

پژوهشات از نظر اعتبار علمی، به دو دسته ذهنی[1] و عینی[2] تقسیم می‌گردند. در پژوهشات ذهنی، پدیده‌ها و روابط بین آن‌ها از طریق تحلیل‌های ذهنی و بدون استعانت از واقعیات تجربی کشف و تعریف می‌شوند. در پژوهشات عینی، ماهیت و روابط پدیده‌ها با کمک تجربه و آزمایش در محیط خارج از ذهن و در دنیای ملموس و محسوس شناخته می‌شوند (پرهیزکار و آقاجانی،۱۳۹۰: ۲۹۱)، این پژوهش از نظر اعتبار علمی در دسته‌بندی پژوهش‌های عینی به‌شمار می‌آید.

نمونه‌های این پژوهش را ۲۰ نفر از خبرگان تشکیل داده است شامل؛ ۱- اعضای هیئت علمی دانشگاه که با مأموریت سازمان‌های اطلاعاتی- امنیتی مرتبط و آشنا بودند. ۲. کارشناسان خبره عملیاتی (که به‌عنوان کاربران نهایی ابزارهای گمنامی مطرح‌اند) و ۳- پژوهشگران فنی (که درواقع تولیدکنندگان ابزار ممانی هستند) که دارای حداقل ۲۰ سال سابقهٔ کار تخصصی و همچنین از تحصیلات کارشناسی ارشد و بالاتر برخوردار بوده و در پست‌های مدیریتی مشغول انجام وظیفه می‌باشند.

جدول ۱: مشخصات نمونه پژوهشی

مشخصات نمونه	کارشناس ارشد عملیاتی	پژوهشگر ارشد فنی	اعضای هیئت علمی (دکتری)
تعداد	۹	۷	۴
تعداد کل مصاحبه شونده‌ها	۲۰ نفر		

با عنایت به نوع پژوهش (کیفی) روش نمونه‌گیری در این پژوهش نمونه‌گیری غیراحتمالی از

1. Subjective
2. Objective

نوع هدفمند است. در روش‌های کیفی (برخلاف روش‌های کمی) مرحله گردآوری داده و تجزیه وتحلیل آن‌ها به‌صورت توأم انجام می‌شود. این یکی از ویژگی‌های گردآوری داده‌های کیفی است که به آن نمونه‌برداری جهت‌دار (در مقابل نمونه‌برداری تصادفی) و یا نمونه‌برداری نظری گفته می‌شود. در این رویکرد، زمینه هر نمونه پژوهش بر اساس نتایج تجزیه و تحلیل نمونه قبلی مشخص می‌شود و بدین لحاظ فرآیند پژوهش کیفی تا اندازه زیادی غیرساختاریافته و وابسته به زمینه و موضوع پژوهش است. این ویژگی‌ها روش‌های کیفی را متعدد و منعطف ساخته است (علی احمدی و غفاریان، ۱۳۸۲: ۲۵۰). حجم نمونه نیز تمام شمار در نظر گرفته شده است. روایی و سنجش روایی محتوایی[1] این پژوهش با توجه به نوع آن، که از گونهٔ کیفی است، از نوع محتوایی- صوری است و توسط ده نفر از استادان مورد تأیید قرارگرفته است. با توجه به نوع پژوهش (کیفی)، برای پایایی این پژوهش از فرمول هولستی استفاده شاده است که فرمول آن به شرح زیر است:

معادله ۱

$$PAO= 2A/ (nA+nB)$$

در این فرمول PAO به معنی درصد توافق مشاهده شده، A تعداد توافق‌های بین دو کدگذار و nA و nB به ترتیب تعداد واحدهای کدگذاری شده از سوی کدگذاران A و B است. این رقم از صفر (هیچ توافق) تا یک (توافق کامل) متغیر است (محمدی‌مهر، ۱۳۸۷: ۱۵۵).

پایایی از طریق فرمول هولستی برحسب درود توافق محاسبه شد.

A = تعداد کدهای مورد تأیید دو خبره

nA =تعداد کدهای مورد تأیید خبره اول

nB = تعداد کدهای مورد تأیید خبره دوم

معادله ۲

$$PAO=2*6 / (8+7) = 0/8$$

نظر به اینکه براساس فرمول محاسبه شده عدد ۸/۰ به‌دست آمده است و عدد مذکور بیش از ۷/۰ است، بنابراین نتیجه حاصله از پایایی لازم برخوردار است.

۱. روایی محتوایی (Content Value) این اطمی‌نان را به‌وجود می‌آورد که مقیاس (در نظر گرفته شده برای پژوهش) شامل یکسری موارد کافی و نمونه برای استفاده از مفهوم است (خاکی، ۲۸۹:۱۳۷۸).

روش تجزیه و تحلیل داده‌ها

تحلیل محتوا نوعی بررسی اسناد و مدارک می‌باشد که ممکن است شخص پژوهشگر یا افراد دیگـر به جمع‌آوری آن پرداختـه باشنـد ولی تحلیـل و وارسی آن توسط شخص محقق انجـام می‌گیرد که کلمات، عبارات، اسامی، بندها، تصاویر، موضوع‌ها یا هر جلوهٔ ویژهای که مورد نظر پژوهشگر است در برگه ثبت می‌گردد. با وجود تنوع اسناد و مدارک، از روش علمی برای تحلیل آن استفاده می‌شود. فرآیند کلی عملیات تحلیل محتوا عبارت است از:

۱) موضوع مورد مطالعه از قبل تعیین می‌گردد که می‌تواند لغات، جملات، عناوین اصلی مقالات و موارد مشابه آن باشد. به‌عنوان نمونه، پژوهش برای به‌دست آوردن بار ارزشی به‌کاررفته در یک مقاله انجام می‌گیرد.

۲) بیـان یک چارچوب که تئـوری پژوهش بر آن مبتنی است. با توجـه به تئوری موجود، فرضیه‌ها و متغیرهای مرتبط با مفاهیم مشخص می‌گردد و با استفاده از روش مناسب برای متغیرهای مورد نظر و با اهدافی که بر آن مترتب می‌باشد، به تحلیل داده‌ها پرداخته می‌شود.

۳) در نظر گرفتن وسیل‌های برای اندازه‌گیری متغیرها. به‌عنوان‌مثال، تهیه فهرستی از واژگان کلیدی به قصد شمارش آن و به‌دست آوردن معانی که در آن واژگان قصد گردیده است.

۴) تهیه و تنظیم ابزارِ جمع‌آوری اطلاعات با توجه به موضوعی که قرار است پژوهش در آن انجام گیرد.

۵) جمع‌آوری اطلاعات مربوط به طرح پژوهش. با در نظر گرفتن زمان مشخص و مکانی که قرار است عملیات در آن انجام گیرد. در ضمن لازم است به جمع‌آوری متن‌ها یا واژه‌هایی پرداخته شود که به‌طور عموم در مسئلهٔ مورد پژوهش کاربرد داشته باشد. پس از انجام مراحل فوق، داده‌های جمع‌آوری شده به دسته‌های مختلف طبقه‌بندی می‌گردند.

۶) پژوهشگر پس از جمع آوری اطلاعات، به تجزیه و تحلیل آن دسته از داده‌هایی می‌پردازد که با فرضیهٔ پژوهش مرتبط می‌باشد تا بتواند نتایج مورد نظر را به‌دست آورد.

مراحل کدگذاری در تحلیل محتوای کیفی با رویکرد استقرایی

در جدول ۲، مراحل کدگذاری در تحلیل محتوای کیفی با رویکرد استقرایی نشان داده شده است. این جدول برای هر یک از اهداف این پژوهش به ۲ جدول کدگذاری باز و کدگذاری مقوله‌ای، به شرح جداول ۳ تا ۸، توسعه داده شده است که به‌عنوان نمونه، سطر اول جداول ۳ و ۶ تکمیل شده‌اند.

جدول ۲: مراحل کدگذاری در تحلیل محتوای کیفی با رویکرد استقرایی

ردیف	جملات کلیدی متون(مصاحبه‌ها، مشاهده‌ها، اسناد)	برچسب‌ها / کدها	زیر مقوله‌ها/ زیر طبقه‌ها	مقوله‌ها/ طبقه‌ها

جدول ۳: کدگذاری باز مصاحبه‌های مرتبط با سؤال اول پژوهش (فرصت‌های استفاده از گمنامی فنی در فضای سایبر برای سازمان‌های اطلاعاتی – امنیتی چیست؟)

ردیف	سمت	واحد معنی	کد
۱	مصاحبه شونده ۰۱	بالابردن امنیت محتواهای دیجیتالی در فضای سایبر، استفاده دسترسی به شبکه‌های اجتماعی خارجی فیلتر شده، استفاده از رمزارزها برای تبادلات مالی، انتشار گزارشات خبری سرّی به‌صورت گمنام، رأی‌گیری گمنام، دسترسی و خرید فناوری‌ها و علوم با تکنولوژی بالا غیر قابل دسترس در وب آشکار، نشر نویسندگی گمنام، ایمیل و به‌اشتراک‌گذاری و ارسال فایل گمنام.	محافظت از دارایی‌های دیجیتال (فایل‌ها و پیام‌های) اشتراک‌گذاری یا تبادل شده (کد۱) استفاده از بستر گمنامی برای استفاده از نرم‌افزارهای شبکه‌های اجتماعی خارجی (کد۲) استفاده از بستر گمنامی برای تبادلات مالی، گزارشات مردمی به پلیس یا نیروهای امنیتی از فعالیت‌های غیرقانونی بدون ترس از مجازات و یا کیفرخواست (کد۳) رأی‌گیری گمنام (کد۴) استفاده‌ازبستر گمنامی برای جست‌وجوی فناوری‌ها و علوم با تکنولوژی بالا (کد۵) استفاده از بستر گمنامی در حوزهٔ نشریات برای چاپ آثار پژوهشی (کتاب، مقاله و ...) نویسنده‌های گمنام (کد۶) استفاده از بستر گمنامی برای ارتباطات با تأخیر و آفلاین (ایمیل، به‌اشتراک‌گذاری و ارسال فایل و ...) (کد ۷).
.....	.....	.....	.....
۲۰	مصاحبه شونده ۲۰	.....	.....

جدول ۴: کدگذاری باز مصاحبه‌های مرتبط با سؤال دوم پژوهش (دیدات استفاده از گ نامی فنی در فضای سایبر برای سازمان‌های اطلاعاتی – امنیتی چیست؟)

ردیف	سمت	واحد معنی	کد
۱	مصاحبه شونده ۰۱	.....	.....
	مصاحبه شونده ۰۲	.....	.....

جدول ۵ :کدگذاری باز مصاحبه‌های مرتبط با سؤال سوم پژوهش (راه‌کارهای مقابله با تهدیدات استفاده از گ نامی فنی در فضای سایبر برای سازمان‌های اطلاعاتی – امنیتی چیست؟)

ردیف	سمت	واحد معنی	کد
۱	مصاحبه شونده ۰۱	.....	.....
	مصاحبه شونده ۰۲	.....	.....

جدول ۶: مقوله‌بندی کدهای باز مرتبط با سؤال اول پژوهش (فرصت‌های استفاده از گمنامی فنی در فضای سایبر برای سازمان‌های اطلاعاتی – امنیتی چیست؟)

ردیف	مقوله اصلی	مقوله فرعی	شماره کدها
۱	**استفاده از بستر گمنامی برای حفظ حریم خصوصی افراد**	۱- محافظت از دارایی‌های دیجیتال ذخیره شده (نظیر اطلاعات شخصی افراد مانند اعتقادات مذهبی، مسایل فرهنگی، بیماری‌های شخصی، و شناسه (هویت) دوستان آنها)، سابقه فعالیت در فضای سایبر، اطلاعات مکانی و ... ۲- محافظت از دارایی‌های دیجیتال (فایل‌ها و پیام‌های) اشتراک‌گذاری یا تبادل شده ۳- وب‌گردی شهروندان به‌صورت آزادانه (بخواهند بدون آنکه سابقه جست‌وجو و عادات شخصی آنها توسط سازمان‌های تبلیغاتی آمارگیری شود) ۴- محافظت از سیستم‌ها و شبکه‌ها در برابر مجموعه‌ای منظم از حملات سایبری به منظور جلوگیری از نفوذ به شبکه‌ها	۲۳-۶۸-۸۲-۴۵ ۱۴-۵۷-۷۳-۸۰-۵۱-۶۶ ۴-۶-۷-۱۹-۲۴-۲۵-۵۰- ۵۸-۶۱-۶۰-۶-۱۷-۱۲-۱۸- ۱۳-۱۶ ۶۴-۶۵-۶۶-۶۷
...	....	....	.....

جدول ۷: مقوله‌بندی کدهای باز مرتبط با سؤال دوم پژوهش (تهدیدات استفاده از گ نامی فنی در فضای سایبر برای سازمان‌های اطلاعاتی – امنیتی چیست؟)

ردیف	مقوله اصلی	مقوله فرعی	شماره کدها
۱	....	....	.....
...	....	....	.....

جدول ۸: مقوله‌بندی کدهای باز مرتبط با سؤال سوم پژوهش (راه‌کارهای له با تهدیدات استفاده از گمنامی فنی در فضای سایبر برای سازمان‌های اطلاعاتی – امنیتی چیست؟)

ردیف	مقوله اصلی	مقوله فرعی	شماره کدها
۱	....	....	.....
...	....	....	.....

یافته‌های پژوهش

فرصت‌ها: بر اساس تجزیه و تحلیل صورت‌گرفته طی دو مرحله کدگذاری باز و کدگذاری مقوله‌ای از ۲۰ مصاحبه انجام‌شده، ۹۲ کد مستخرج گردید که تحلیل کدها، منجر به شناسایی ۲۶ مقوله فرعی شد و در نهایت از دسته‌بندی مقوله‌های فرعی، ۶ مقوله اصلی استخراج گردید. مقوله‌های اصلی و فرعی در جدول ۹، نشان داده شده است.

جدول ۹: فرصت‌های استفاده از گ نامی فنی در فضای سایبر

ردیف	مقوله‌های اصلی	مقوله‌های فرعی
۱	استفاده از بستر گمنامی برای حفظ حریم خصوصی افراد	۱- جلوگیری از رصد سابقه فعالیت در فضای سایبر، اطلاعات مکانی، دارایی‌های دیجیتال ذخیره شده (نظیر اطلاعات شخصی افراد مانند اعتقادات مذهبی، مسایل فرهنگی، بیماری‌های شخصی، و شناسه (هویت) دوستان آن‌ها) و... ۲- محافظت از دارایی‌های دیجیتال (فایل‌ها و پیام‌های) اشتراک‌گذاری یا تبادل شده ۳- آزادی در وب‌گردی شهروندان (بدون آنکه سابقه جست‌وجو و عادات شخصی آن‌ها توسط سازمان‌های تبلیغاتی آمارگیری شود) ۴- جلوگیری از نفوذ به سیستم‌ها و شبکه‌ها در برابر مجموعه‌ای منظم و هدفمند از حملات سایبری
۲	استفاده از بستر گمنامی برای فعالیت‌های عمومی و پرکاربرد	۵-استفاده از بستر گمنامی برای استفاده از نرم‌افزارهای شبکه‌های اجتماعی خارجی. ۶-استفاده از بستر گمنامی برای مزایده گمنام و سایر معاملات ۷-استفاده از بستر گمنامی برای تبادلات مالی
۳	استفاده از بستری گمنام برای آزادی بیان	۸-گزارش اخبار سرّی و دارای طبقه‌بندی توسط خبرنگاران، خبرچینان، مخالفان حکومت‌ها، سازمان‌های اطلاعاتی، شاهدها و ... ۹-بیان انتقادها و پیشنهادها ۱۰-گزارش‌های مردمی به پلیس یـ نیروهای ا نیتی از فعالیت‌های غیرقانونی بدون ترس از مجازات و یا کیفرخواست. ۱۱-رأی‌گیری گمنام

۴	استفاده از بستر گمنامی برای انجام پژوهش‌ها	۱۲-استفاد از بستر گمنامی به منظور جلوگیری از فاش شدن فهرست، کمیت و حتی محتوای پروژه‌های دارای طبقه‌بندی ۱۳-استفاده از بستر گمنامی برای جست‌وجوی فناوری‌ها و علوم با تکنولوژی بالا ۱۴-استفاده از بستر گمنامی در حوزهٔ نشریات برای چاپ آثار پژوهشی (کتاب، مقاله و ...) نویسنده‌های گمنام. ۱۵-استفاده از بستر گمنامی در پژوهش‌ها به منظور جمع‌آوری نظرات گمنام افراد در محیط‌های دانشگاهی و پژوهشاتی. ۱۶-استفاده از گمنامی برای دستیابی به سرویس‌های اینترنتی و سایت‌های بلوکه شده برای کشورهای خاص (به‌وسیله ISP)
۵	استفاده سازمان‌های امنیتی و سرویس‌های اطلاعاتی برای ارتباطات دارای حیطه‌بندی به منظور مخفی ماندن وجود هر نوع ارتباط (فریبکارانه، امن و پوششی)	۱۷-استفاده از بستر گمنامی دوطرفه به منظور پنهان ماندن شناسهٔ فرستنده و گیرنده از دید مهاجم و نیز از دید طرفین ارتباط. ۱۸-استفاده از بستر گمنامی برای ارتباطات با تأخیر و آفلاین (ایمیل، به‌اشتراک‌گذاری، ارسال فایل و...) ۱۹-استفاد از بستر گمنامی برای ارتباطات بلادرنگ (چت، تلفن اینترنتی و...) و امکان برقراری ارتباط حساس اجتماعی همانند اتاق‌های گفت‌وگو و فروم‌های وب ۲۰-استفاد از بستر گمنامی برای سازماندهی و شخصی‌سازی اطلاعات مشترک بر روی شبکه‌های عمومی، بدون هیچ‌گونه خطر در حریم خصوصی ۲۱-استفاده از بستر گمنامی برای ایجاد امکان جلوگیری از شنود اطلاعات کاربران و عدم توانایی ثبت اطلاعاتِ ردوبدل شده و تحلیل ترافیک آن توسط کاربران دیگر (مهاجمان)
۶	استفاده از بستر گمنامی برای عملیات سایبری سازمان‌های امنیتی	۲۲-استفاده از گمنامی در اقدامات آفندی نظیر هک و نفوذ ۲۳-استفاده از گمنامی در شناسایی: جمع‌آوری گمنام اطلاعات ولو آشکار محیطی در مورد هدف نظیر زمان‌ها و مکان‌های حضور، فعالیت، عضویت و ... همچنین تجهیزات مورد استفاده هدف. ۲۴-نگه‌داشتن دسترسی به‌صورت گمنام: استفاده از ترفندها نظیر درج درب‌های پشتی و ... به‌منظور حفظ دسترسی و استفاده در ورودهای بعدی. ۲۵-استفاده از گمنامی در پویش و اسکن: جمع‌آوری گمنام اطلاعات سیستمی در مورد هدف نظیر آسیب‌پذیری‌های نرم‌افزارها و برنامه‌های کاربردی، سخت‌افزارها، سیستم‌عامل، شبکه، وبگاه و ... هدف به‌منظور اثبات نفوذپذیری (در تست نفوذ) ۲۶-رصد فعالیت استفاده‌کنندگان از ابزارهای گمنامی نظیر VPN به منظور سرنخ‌یابی امنیتی یا جرایم سایبری و ...

تهدیدها و راه‌کارهای مقابله‌ای

بر اساس تجزیه و تحلیل صورت گرفته طی دو مرحله کدگذاری باز و کدگذاری مقوله‌ای از ۲۰ مصاحبه صورت گرفته در این پژوهش، برای تهدیدات، ۶۳ کد باز به‌دست آمد که تحلیل کدها، منجر به شناسایی ۱۶ مقوله فرعی گردید. از دسته‌بندی مقوله‌های فرعی، ۹ مقوله اصلی استخراج شد. مقوله‌های اصلی و فرعی در جدول ۱۰، نشان داده شده است.

در مورد راه‌کارهای مقابله، با توجه به این نکته که «راه‌کارهای مقابله با تهدیدات مختلف، در بسیاری از موارد با هم اشتراک دارند»، ازاین‌رو ترجیح داده شد که فقط مقوله‌های فرعی ارائه شوند و با تحلیل ۸۴ کد باز به‌دست آمده از مصاحبه‌ها، ۲۲ مقوله فرعی به‌عنوان راه‌کارهای مدیریتی و ۲۰ مقوله فرعی به‌عنوان راه‌کار فناورانه استخراج گردید که نتایج در جداول ۱۱ و ۱۲ آورده شده است

جدول ۱۰: نتایج تجمیعی تهدیدات گ نامی فنی در فضای سایبر

ردیـ	مقوله اصلی	مقوله فرعی
۱	عدم پرداختن به فناوری گمنامی در فضای سایبر برای سازمان‌های اطلاعاتی	۱- برتری سرویس‌های امنیتی حریف از گمنامی در فضای سایبر در برابر ناتوانی و عقب‌ماندگی سرویس‌های خودی در این فضا. ۲- عقب‌ماندگی از سازمان‌های اطلاعاتی رقیب داخلی و عدم بهره‌برداری از فرصت‌ها و مزیت‌های رقابتی ناشی از فناوری گمنامی در فضای سایبر نظیر ایمن‌سازی ارتباطات با منابع.
	موارد ناشی از سوءاستفاده از فناوری گمنامی در فضای سایبر	
۲	دشواری مأموریت سازمان‌های اطلاعاتی - امنیتی در احاطه و رصد فعالیت‌ها و ارتباطات غیرامنیتی گروه‌های تروریستی، جواسیس و سرویس‌های امنیتی غیر	۲- عدم احاطه بر فعالیت گروه‌های تروریستی، جواسیس و سرویس‌های امنیتی غیر (ارتباطات با اعضا، جذب عضو، تبلیغات، مبادلات مالی، آموزش و ...) که از بستر گمنامی فضای سایبر استفاده می‌کنند.
۳	کاهش احتمال موفقیت در فارنزیک دیجیتال (جرم‌یابی دیجیتال)	۳-ضعف دانشی و عدم احاطه به موضوع پیچیدگی ابزارهای گمنامی
۴	انتشار اخبار یا بانک‌های اطلاعاتی محرمانه	۴- استفاده خبرنگاران و دلالان اطلاعات در بستر گمنامی فضای سایبر (انتشار اخبار محرمانه داخلی تحت عناوینی نظیر فعالان حقوق مدنی با حق آزادی سخن، یا حقوق روزنامه‌نگاران با حق محافظت از منابع خبری).

۵	ناتوانی در رصد فعالیت‌های مجرمانه در بستر گمنامی فضای سایبر	۵- استفاده مجرمان از ابزارهای بستر گمنامی فضای سایبر (قاچاق، کلاهبرداری، خرید و فروش اسلحه و اعضای بدن، خرید و فروش بانک‌های اطلاعاتی و ...)
۶		۶- عدم نظارت به ایجاد و ارائه سرویس‌های فضای مجازی توسط افراد خودی نظیر وب‌سایت‌های مختلف در بستر گمنامی بدون نیاز به آشکارسازی مکان سایت
۷	خنثی‌شدن اقدامات حکومتی (سانسور) به‌منظور ممانعت از دسترسی به برخی از بخش‌های فضای مجازی نظیر شبکه‌های اجتماعی خارجی یا سایت‌های اینترنتی معاند	۷- دسترسی به برخی از بخش‌های فضای مجازی نظیر شبکه‌های اجتماعی خارجی یا سایت‌های اینترنتی معاند با استفاده از ابزارهای گمنامی در فضای سایبر
موارد ناشی از سوءاستفاده از فناوری گمنامی در فضای سایبر		
۸	استفاده از ابزارهای گمنامی غیر بومی ملی نبودن اینترنت و زیرساخت‌های آن، پروتکل‌های شبکه، الگوریتم‌های گمنام‌سازی، ابزار نرم‌افزاری (مرورگر و ...)	۸- ایجاد حساسیت خالق ابزار گمنامی به کاربران و رصد فعالیت و اطلاعات آن‌ها که منجر به شناسایی مأموران امنیتی، افشای هویت منابع اطلاعاتی، رصد فعالیت سازمان‌های امنیتی (نظیر ارتباط با منابع) و لو رفتن روش‌های عملیات اطلاعاتی می‌گردد. ۹- شناسایی و رصد فعالیت‌های عمومی در فضای گمنامی (نظیر افشای هویت محققان علمی، آگاهی از فعالیت‌های علمی گمنام و ...) ۱۰- تسلط خالقان فناوری بر بستر گمنامی و امکان دست‌کاری و سرقت اطلاعات، عدم دسترسی‌پذیری و ناپایداری سامانه‌ها در مواقع لزوم.
۹	خنثی‌شدن گمنامی و عدم موفقیت در مأموریت و عملیات اطلاعاتی - امنیتی	۱۱-عدم رعایت ملزومات کاربری استفاده از ابزارهای گمنامی نظیر استفاده هم زمان از مرورگر گمنام و مرورگر غیر گمنام
		۱۲-عدم رعایت ملزومات تعامل با ارائه‌دهندگان سرویس‌های گمنامی نظیر در اختیار قرار دادن اطلاعات هویتی نزد ارائه‌دهندگان سرویس‌های گمنامی به‌عنوان شخص ثالث
		۱۳-استفاده از ابزارهای قدیمی که منجر به عقب‌ماندگی از به‌روزرسانی‌های فناوری و در نتیجه ناکارآمدی فناوری می‌شود (عدم آگاهی از پیشرفت‌های به‌روز و در نتیجه متناسب با نیازها و پیشرفت‌های فناوری، تأمین ابزارها، به‌کارگیری و پشتیبانی از سامانه‌ها در مأموریت‌ها، انجام نمی‌شود) و در تقابل با دشمن در این حوزه شکست می‌خوریم.
		۱۴-ضعف‌ها و محدودیت‌های بومی فناوری (ضعف روش‌ها، الگوریتم‌ها و پروتکل‌های بومی و...) در مقابله با روش‌های کشف گمنامی
		۱۵-عدم رعایت ملزومات عملیاتی در طراحی و پیاده‌سازی سامانه‌های بومی ه منجر به تفاوت ابزارهای گمنامی بومی با غیر بومی و در نتیجه افشای ابزارهای گمنامی بومی می‌شود (نظیر ترافیک و جمعیت کم کاربران و ...).

جدول ۱۱: نتایج تجمیعی راه‌کارهای مدیریتی مقابله با تهدیدات گمنامی در فضای ایبر

ردیف	شرح راه‌کار
۱	انجام حمایت‌های مؤثر سازمانی به‌ویژه از سوی مسئولان و مدیران ارشد سازمان و تأمین اعتبارات کافی و لازم در راستای انجام دادن پژوهش و توسعه هدفمند و تولید منابع بومی در به‌کارگیری شبکه گمنامی بومی در سازمان‌های اطلاعاتی و امنیتی.
۲	تشکیل کمیته تخصصی تصمیم‌گیری در استفاده از بستر گمنامی فضای سایبر.
۳	استفاده از افراد متخصص و توانمند برای فعالیت و کار با ابزارهای گمنامی.
۴	تشکیل تیم‌های کاری طراحی، اجرا، پشتیبانی و رفع اشکال، رصد، پایش و واکنش به تهدیدات احصا شده.
۵	مهاجرت از سامانه‌های گمنامی فعلی به سامانه‌های به‌روز و پیشرفته.
۶	برنامه‌ریزی صحیح و اصولی و تعامل با ارگان‌های موازی و سازمان‌های پیشرو در حوزه گمنامی (بررسی تجارب و اقدامات اعضای جامعه اطلاعاتی و نیروهای مسلح در به‌کارگیری فناوری گمنامی فضای مجازی و هم‌افزایی تخصصی فی‌مابین اعضای جامعه اطلاعاتی نظیر تعامل مؤثر با وزارت ارتباطات و فناوری اطلاعات در خصوص ملاحظات به‌کارگیری ابزارهای گمنامی مثل مرورگر TOR)
۷	انجام دادن اقدامات صیانت امنیتی در شبکه گمنامی بومی از قبیل کنترل، نظارت، آموزش، استقرار استانداردهای بومی، رعایت اصول طبقه‌بندی و حیطه‌بندی، با استفاده از نیروی انسانی متعهد، متخصص و جهادی در راستای تداوم و استمرار امنیت فناوری مذکور مورد تأکید قرار گیرد.
۸	ایجاد ساختار و جذب نیروی انسانی متخصص برای راه‌اندازی، توسعه، پشتیبانی، امنیت و کنترل امنیت فناوری گمنامی فضای سایبر در سازمان‌های امنیتی.
۹	استفاده از نخبگان دانشگاهی و بهره‌برداری از شرکت‌های دانش‌بنیان مطمئن و فعال جهت طراحی زیرساخت‌ها و ابزارهای گمنامی.
۱۰	نهادینه‌سازی اصول، الزامات و ملاحظات پدافند غیرعامل و پدافند سایبری هوشمند در طرح‌های توسعه‌ای سامانه بومی گمنامی.
۱۱	افزایش سطح دانش و آگاهی و تقویت بنیه علمی کارکنان، تصمیم‌سازان و تصمیم‌گیران در خصوص مزایا و چالش‌های به‌کارگیری فناوری گمنامی فضای سایبر در سازمان‌های امنیتی.
۱۲	اتخاذ تدابیر لازم برای فرهنگ‌سازی استفاده از فناوری گمنامی در فضای سایبر در سازمان‌های امنیتی.
۱۳	اعزام کارشناسان فنی به دوره‌های مرتبط با آموزش گمنامی و استفاده از ابزارهای گمنامی.
۱۴	اطلاع‌رسانی مستمر پیرامون ملاحظات و سیاست‌هایی که بایستی توسط کاربران برای حضور در بستر گمنامی فضای سایبر مراعات گردد و برخورد قانونی با تخلفات و شکست‌های احتمالی.
۱۵	تهیه دستورالعمل مقابله با سطوح مختلف گمنامی در فضای سایبر
۱۶	تدوین آیین‌نامه‌ها، شیوه‌نامه‌ها، الگوهای امنیت و کنترل امنیت مربوط به پیاده‌سازی فناوری گمنامی فضای سایبر در سازمان‌های امنیتی.

۱۷	تشکیل تیم‌های پژوهش و توسعه و تدوین نقشه راه (اتخاذ راهبرد، تعیین خط‌مشی، هدف‌گذاری، برنامه‌ریزی، اولویت‌بندی، زمان‌بندی) در حوزه گمنامی فضای سایبر
۱۸	تأمین اعتبارات و هزینه‌های لازم برای پژوهشات و تولید ابزارهای گمنامی
۱۹	تعامل سازمان‌های اطلاعاتی با جامعه علمی در حوزهٔ گمنامی فضای سایبر.
۲۰	ایجاد تیم‌های رصد مستمر و مداوم تهدیدات و آسیب‌های ابزارهای گمنامی در فضای سایبر به‌منظور واکنش به‌موقع، آگاهی از پیشرفت فناوری و ...
۲۱	بررسی رویکرد سازمان‌های اطلاعاتی - امنیتی حریف در حوزه به‌کارگیری فناوری گمنامی فضای سایبر.
۲۲	طراحی ساختار سازمانی برای تیم‌های رصد و پایش مستمر و مداوم فعالیت‌های بستر گمنامی فضای سایبر.

جدول ۱۲: نتایج تجمیعی راهکارهای فناورانه مقابله با تهدیدات گمنامی در فضای سایبر

ردیف	شرح راه‌کار
۱	استفاده موازی از دیگر فناوری‌های مخفی‌ساز (ایمن‌ساز) نظیر رمزنگاری، نهان‌نگاری، بلاکچین و ... برای بالابردن امنیت
۲	استفادهٔ ترکیبی از ابزارها و سناریوهای گمنامی برای تحقق سطوح مختلف گمنامی و بالابردن ضریب گمنامی
۳	تلفیق ابزارهای گمنامی بومی با ابزارهای گمنامی غیر بومی.
۴	سفارشی‌سازی خدمات گمنامی در جهت تسلط بیشتر بر بستر گمنامی مورد استفاده.
۵	شناسایی و به‌کارگیری روش‌های رصد فعالیت کاربران ابزارها و بسترهای گمنامی غیر بومی (نظیر دسترسی به سرورهای لایه اول مرورگر TOR) و بومی مختلف با روش‌های مستقیم و غیر مستقیم و کنترل مستقیم یا غیر مستقیم نظیر آلوده‌سازی
۶	بررسی و به‌کارگیری ابزارهای نوین فارنزیک دیـ یتال (جرم‌یابی دیجیتال) در بستر گمنامی فضای سایبر
۷	رعایت ملزومات عملیاتی ابزارهای گمنامی نظیر ترافیک و جمعیت بالای کاربران و ... در طراحی، پیاده‌سازی و کاربری سامانه‌های بومی.
۸	تأمین، به‌کارگیری و پشتیبانی از ابزارهای گمنامی بر اساس پیشرفت‌های بهروز فناوری و متناسب با سطوح مختلف گمنامی.
۹	طراحی و عمومی‌سازی ابزارهای گمنامی در فضای سایبر در جهت احاطه به تعاملات در آن حوزه
۱۰	تولید و به‌کارگیری ابزارهای گمنامی بومی (زیرساخت‌ها، مرورگر، الگوریتم‌ها، پروتکل‌ها و ...)
۱۱	تولید ابزارهای کنترل و مانیتورینگ بر روی بسترهای ارتباطی گمنامی بومی.
۱۲	جایگزینی ماشین به‌جای انسان و استفاده از ابزارهای گمنامی رباتیک بدون دخالت انسان برای کاهش خطا و حفظ گمنامی.

۱۳	بررسی و شناسایی دقیق نقاط ضعف و قوت ابزارهای گمنامی غیر بومی و بومی و تشخیص صحیح فرصت‌ها و تهدیدها
۱۴	رعایت ملزومات کاربری استفاده از ابزارهای گمنامی نظیر عدم استفاده هم‌زمان از مرورگر گمنام و مرورگر غیر گمنام
۱۵	رعایت ملزومات تعامل با ارائه‌دهندگان سرویس‌های گمنامی نظیر عدم در اختیار قرار دادن اطلاعات هویتی نزد ارائه‌دهندگان سرویس‌های گمنامی به‌عنوان شخص ثالث
۱۶	لحاظ نمودن اقدامات پیش‌زمینه برای استفاده از ابزارهای گمنامی و حضور در بستر گمنامی (نظیر تشکیل هویت مجازی جعلی با استفاده از ابزار و یا سایت‌های خدمات‌دهندهٔ هویت جعلی، تهیه نسخه پشتیبان امن از اطلاعات و ...)
۱۷	توسعه و به‌کارگیری مستمر روش‌های به‌روز ارزیابی زیرساخت‌ها، شبکه‌ها و ابزارهای کاربردی گمنامی در فضای سایبر.
۱۸	طراحی و به‌کارگیری سناریوهای فریب به‌منظور اهداف امنیتی - اطلاعاتی
۱۹	ایجاد آزمایشگاه‌های مرجع در سطح سازمان‌های اطلاعاتی و امنیتی در راستای بررسی تخصصی فرصت‌ها، تهدیدها و راه‌کارهای برون‌رفت از چالش‌های این فناوری و ارزیابی ایمنی و امنیتی سامانه‌های سخت‌افزاری و نرم‌افزاری ایجاد و توسعه داده شود.
۲۰	باتوجه‌به ماهیت شبکه گمنامی بومی، برای پایداری شبکه و سامانه‌های کاربردی در شرایط بحرانی، مرکز داده به‌منظور پشتیبانی از اطلاعات و زیرساخت جایگزین طراحی و عملیاتی گردد

نتیجه‌گیری

مزایای استفاده از علوم و فناوری‌های نوین، فرصت‌هایی را ایجاد می‌کنند که افراد، شرکت‌ها، سازمان‌ها و دولت‌ها را متقاعد می‌کند تا در کاربردهای مختلف از علوم و فناوری‌های نوظهور بهره‌گیرند. بسیاری از فرصت‌های ایجاد شده ناشی از استفادهٔ گمنامی فنی در فضای سایبر، به امکاناتی که ابزار گمنامی ایجاد می‌کند بستگی دارد و برخی دیگر به نوع کاربرد آن‌ها بر می‌گردد. این پژوهش، منجر گردید به اینکه فرصت‌های گمنامی فنی در فضای سایبر برای سازمان‌های اطلاعاتی- امنیتی در ۶ مقوله اصلی و ۲۶ مقوله فرعی دسته‌بندی شوند که به‌علت محدودیت مقاله، از ذکر موارد در نتیجه‌گیری خودداری می‌شود.

استفاده از فناوری‌ها و علوم نوظهور، علاوه بر فرصت‌ها، تهدیداتی را نیز به‌وجود می‌آورد. پذیرش فناوری‌ها و علوم نوظهور، همواره موضوع پژوهش‌های کاربردی بوده است. بسیاری از تهدیدات حوزه گمنامی، ناشی از بهره‌گیری معاندان از بستر گمنامی در فضای سایبر است؛ چرا که قدرت سازمان‌های اطلاعاتی- امنیتی خودی در کنترل، نظارت و رصد تعاملات گروه‌های معاند، ناکافی بوده و در بسیاری

از موارد، ناتوان می‌باشد. در خیلی از مواقع برای گمنامی در فضای سایبر، از ابزارهای غیر بومی استفاده می‌شود؛ که بایستی یک سری اقدامات عملی، نظیر گمنامی نزد فروشنده نرم‌افزار/ابزار گمنامی، رعایت شود تا گمنامی کامل رعایت شود. برای عملیاتی کردن ابزارهای گمنامی بومی نیز لازم است که علاوه بر رعایت ملاحظات فنی در طراحی ابزار گمنامی، اقدامات مدیریتی نظیر اتخاذ تدابیری برای پرکاربر کردن نرم‌افزار تولیدشده، انجام شود تا بتوان به هدف گمنامی مناسب رسید؛ چرا که عوامل غیر فنی نظیر بررسی اندازه جمعیت گمنامی و گروه‌های جمعیتی در موفقیت سامانه‌های گمنام‌ساز تأثیر دارند. نتایج این پژوهش منجر به ارائه تهدیدات گمنامی فنی در فضای سایبر برای سازمان‌های اطلاعاتی- امنیتی در سه دسته کلی شد: الف - موارد ناشی از عدم پرداختن به فناوری گمنامی در فضای سایبر برای سازمان‌های اطلاعاتی. ب- موارد ناشی از سوءاستفاده از فناوری گمنامی در فضای سایبر. ج- موارد ناشی از استفاده از فناوری گمنامی در فضای سایبر. بررسی نتایج به‌دست‌آمده نشان می‌دهد که: ۱- بین برخی تهدیدات احصا شده رابطه علی و معلولی وجود دارد که بسته به موضوع، در برخی موارد، علت یا معلول بیشتر از یک مورد است. ۲- برخی از تهدیدات ذکر شده، درواقع تهدیداتی (مقوله‌های اصلی) هستند که در نتیجهٔ سوء استفاده از بستر گمنامی فضای سایبر ایجاد گردیده‌اند و با تهدیدات متناظر (زیر مقوله‌ها) رابطه علی و معلولی دارند.

تجزیه و تحلیل راه‌کارهای مقابله‌ای با تهدیدات گمنامی فنی در فضای سایبر برای سازمان‌های اطلاعاتی- امنیتی، منجر به ارائه نتایج در دو دستهٔ راه‌کارهای مدیریتی و راه‌کارهای فناورانه گردید و با لحاظ این نکته که «راه‌کارهای مقابله با تهدیدات مختلف، در بسیاری از موارد با هم اشتراک دارند»، فقط ۲۲ مقوله فرعی به‌عنوان راه‌کارهای مدیریتی و ۲۰ مقوله فرعی به‌عنوان راه‌کار فناورانه آورده شده است.

منابع و مأخذ

الف) منابع فارسی

۱. احمدی، احمد، دهقانی، مهدی، و صالح اصف‌هانی، محمود. (۱۳۹۶). **ارائه روش حل مساله نقاط مرزی در نشان گذاری مبتنی بر فاصله در جریان شبکه گمنامی**. پدافند الکترونیک و سایبری، ۵(۲ (پیاپی ۱۸))، ۱۹-۳۵.

۲. علی احمدی، علیرضا، غفاریان، وفا، (۱۳۸۲)، **اصول شناخت و روش پژوهش**، فصلنامه علمی پژوهشی علوم انسانی، دانشگاه الزهرا، شماره ۴۶ و ۴۷.

۳. احمدی، فهیمه، و نیکوقدم، مرتضی. (۱۳۹۸). **یک روش احراز هویت و توافق کلید نشست امن در شبکه های سیار سراسری با حفظ گمنامی کاربر**. مهندسی برق (دانشکده فنی دانشگاه تبریز)، ۴۹(۳ (پیاپی ۸۹))، ۹۶۵-۹۸۴.

۴. امیری، فاطمه. (۱۳۹۹). **حفظ حریم خصوصی در برون سپاری داده‌های سامانه‌های اطلاعاتی با تکیه بر سودمندی داده**. پردازش و مدیریت اطلاعات (علوم و فناوری اطلاعات)، ۳۶(۱ (پیاپی ۱۰۳))، ۲۱۱-۲۴۲.

۵. پرهیزکار، محمدمهدی، آقاجانی افروزی، علی‌اکبر، (۱۳۹۰)، **روش‌شناسی پژوهش پیشرفته در مدیریت با رویکرد کاربردی**، تهران، انتشارات دانشگاه پیام نور.

۶. پورنقی، سیدمرتضی، برمشوری، مصطفی، و گردشی، محمود. (۱۳۹۴). **طرح بهبود یافته احراز اصالت, با حفظ گمنامی مشروط در شبکه‌های اقتضایی بین خودرویی**. پدافند الکترونیک و سایبری، ۳(۲ (پیاپی ۱۰))، ۱-۱۲.

۷. ترابیان، مرضیه، ۱۴۰۲، **تاثیرات مثبت و منفی فضای مجازی**، پژوهش‌های مطالعات اسلامی معاصر، سال اول، شماره دوم.

۸. جانبابائی، شادی، قرائی، حسین، و محمدزاده، ناصر. (۱۳۹۷). **ارائه طرح احراز اصالت سبک با قابلیت گمنامی و اعتماد در اینترنت اشیا**. پردازش علایم و داده ها، ۱۵(۴ (پیاپی ۳۸))، ۱۱۱-۱۲۲.

۹. حسنی کرباسی، امیر، علیدوست‌نیا، مهران، و ابراهیمی آتانی، رضا. (۱۳۹۳). **طراحی یک سامانه ارتباطات گمنام با استفاده از رمزنگاری مبتنی بر مشبکه‌ها. پدافند الکترونیک و سایبری**، ۲(۳ (پیاپی۷))، ۱۳-۲۲.

۱۰.رضازاده، فرید، آقاصرام، مهدی، میزانیان، کیارش، و مصطفوی، سیداکبر. (۱۳۹۹). **گمنامی توزیع شده بر پایه زنجیره بلوک تجمعی در شبکه ا تضایی خودرویی**. پدافند الکترونیک و سایبری، ۸(۴ (پیاپی ۳۲))، ۴۱-۵۲.

۱۱. سلماسیزاده، محمود، مرتضوی، سیدامیر، و مهاجری، جواد. (۱۳۹۸). **حمله‌ای جدید به شبکه مخلوط مرکب جیکوبسون. پدافند الکترونیک و سایبری**، ۷(۳)، ۱۱۳-۱۱۹.

۱۲. عبدالهیان، حمید، زاهدی، محمدجواد، و شیخ انصاری، مهین. (۱۳۹۲). **ارزیابی ساختار, کنش های متقابل, گمنامی و بازنمایی خود در چهار شبکه اجتماعی مجازی**. مطالعات بین رشته‌ای در رسانه و فرهنگ (رسانه و فرهنگ)، ۳(۲).

۱۳. علیزاده، جواد؛ باقری، نصور. (۱۴۰۱). **مشاهداتی روی یک طرح احراز اصالت سبک وزن با قابلیت گمنامی و اعتماد در اینترنت اشیا**، فصلنامه پردازش علایم و داده‌ها، شماره ۳، ۵۳.

۱۴.فراهانی، هادی، و ماهان، حسین. (۱۳۹۴). **گمنامی کوانتومی بر پ ه مساله شام رمزنگاران**. کنفرانس ریاضی ایران، چهل و ششمین کنفرانس ریاضی ایران، دانشگاه یزد، ص ۱-۴.

۱۵. کنعانی، محمد امین، و محمدزاده، حمیده. (۱۳۹۷). **مطالعه گمنامی در روابط اینترنتی و عوامل جامعه شناختی موثر بر آن. جامعه شناسی کاربردی** (مجله پژوهشی علوم انسانی دانشگاه اصفهان)، ۲۹(۲ (پیاپی ۷۰))، ۱۷-۳۸.

۱۶. کنگاوری، سوسن و کنگاوری، کوثر، ۱۴۰۲، **بررسی تاثیر فضای مجازی تغییر هویت در نوجوانان**، اولین کنفرانس بین المللی روانشناسی، علوم اجتماعی، علوم تربیتی و فلسفه، بابل

۱۷. مجاهد، محمد مهدی و دیگران (۱۴۰۲)، **پروتکلی برای ارتباطات گمنام احراز اصالت شده با رمزنگاری پساکوانتومی و قراردادهای هوشمند**، مجله مهندسی برق دانشگاه تبریز، جلد ۵۳، شماره ۱.

۱۸. مشایخ، فرحناز، حاجی زاده، هانیه، ۱۴۰۲، **فرصت‌ها و آسیب‌های فضای مجازی**، فصلنامه انگاره‌های نو در پژوهشات آموزشی، سال دوم، شماره ۲، صص ۱.

۱۹. معمار، ثریا؛ عدلی پور، صمد؛ خاکسار، فائزه. (۱۳۹۱). **شبکه‌های اجتماعی مجازی و بحران هویت (با تأکید بر بحران هویتی ایران)**، فصلنامه علمی – پژوهشی مطالعات و تحقیقات ا ماعی در ایران، دوره اول، شماره۴، ص۱۷۱-۱۱۱.

۲۰. مهرجو، اهدا، و ستاری نائینی، وحید. (۱۳۹۶). **روشی نوین برای حفظ حریم خصوصی**

شبکه های هوشمند برق از طریق الگوریتم گمنامی مرتبه k و رمزنگاری داده ها. کنفرانس ملی فناوری‌های نوین در مهندسی برق و کامپیوتر.

۲۱. هاتفی، زهرا؛ بیات، مجید؛ حامیان، نگین.(۱۴۰۰). **طراحی یک پروتکل پرداخت الکترونیکی مبتنی بر زنجیره قالب با حفظ گمنامی کاربران**، شریه علمی"پدافند الکترونیکی و سایبری"، سال نهم، شماره۲، ص۱۰۰-۸۵.

۲۲. همایون، حامد، دهقانی، مهدی، و اکبری، حمید. (۱۴۰۰). **مروری تحلیل ترافیک شبکه گمنام ساز پارس با استفاده از یادگیری ماشین**. پدافند غیر عامل، ۱۲(۲ (پیاپی ۴۶))، ۱-۱۷.

ب) منابع لاتین

23.Chao, D., Xu, D., Gao, F., Zhang, C., Zhang, W., & Zhu, L. (2024). **A Systematic Survey On Security in Anonymity Networks: Vulnerabilities, Attacks, Defenses, and Formalization**. IEEE Communications Surveys & Tutorials.

24.di Vimercati,S.D.C.,Foresti,S.,Livraga,G.,&Samarati, P. (2023). **k-Anonymity: From Theory to Applications**. Trans. Data Priv.,16(1), 25-49.

25. H. Tillwick and M. Olivier, "**Towards a Framework for Connection Anonymity**," in SAICSIT, pp. 113-122, 2005.

26. J. S. Valacich, A. R. Dennis, L. M. Jessup, and J. F. Nunamaker, Jr., "**A Conceptual Framework of Anonymity in Group Support Systems**," in 25th Hawaii International Conference on System Sciences Kauai HI, USA, pp. 101-112 vol. 4, 1992.

27. Jung, S., Park, S., Son, S. B., Lee, H., & Kim, J. (2023). **Network Security and Trustworthiness**. In Fundamentals of 6G Communications and Networking (pp. 747-762). Cham: Springer International Publishing.

28. Kerstin N. Vokinger, Daniel J. Stekhoven, and Michael Krauthammer, "**Lost in Anonymization – A Data Anonymization Reference Classifivation Merging Legal and Technical Considerations,**" Publlished in the SAGE Journals, The Journal of Law, Medicine & Ethics, pp 228-231, Aprill 28, 2020.

29. Kocaoğullar, C., Hugenroth, D., Kleppmann, M., & Beresford, A. R. (2023). **Pudding: Private User Discovery in Anonymity Networks**. arXiv preprint arXiv:2311.10825.

30. Kramer, A., Rezabek, F., & von Seck, R. (2023). **Recent Advancements in Privacy Preserving Network Layer Approaches**. Network, 19.

31. Lin, Y. (2024). **Moving beyond anonymity: Embracing a collective approach to location privacy in data-intensive geospatial analytics**. Environment and Planning F, 26349825231224029.

32. López-García, D. A., Pérez Torreglosa, J., Vera, D., & Sánchez-Raya, M. (2024). **Binary-Tree-Fed Mixnet: An Efficient Symmetric Encryption Solution**. Applied Sciences, 14(3), 966.

33. M. Edman and B. Yener, "**On anonymity in an electronic society: A survey of anonymous communication systems," ACM Computing Surveys (CSUR), vol. 41, no. 1**, pp. 1-35, 2009.

34. Meng, X., & Liang, M. (2023). **Port-Based Anonymous Communication Network: An Efficient and Secure Anonymous Communication Network**. Sensors, 23(21), 8810.

35. Michael K. Reiter and Aviel D. Rubin, "**Crowds: Anonymity for web transactions," ACM Trans**. Information and System Security, pp. 66-92, November 1998.

36. Neves, F., Souza, R., Sousa, J., Bonfim, M., & Garcia, V. (2023). **Data privacy in the Internet of Things based on anonymization: A review**. Journal of Computer Security, (Preprint), 1-31.

37. **NSA targets the privacy-conscious**. http://daserste.ndr.de/panorama/aktuell/NSA-targets-the-privacy-onscious,nsa230.html. Retrieved on 2015.05.13.

38. Odoom, J., Huang, X., Zhou, Z., Danso, S., Zheng, J., & Xiang, Y. (2023). **Linked or unlinked: A systematic review of linkable ring signature schemes**. Journal of Systems Architecture, 134, 102786.

39. Patil, A. P., & Hurali, L. C. M. (2023). **Discerning the traffic in anonymous communication networks using machine learning: concepts, techniques and future trends**. International Journal of Information and Decision Sciences, 15(1), 94-115.

40. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability,

pseudonymity, and identity managementa consolidated proposal for terminology, v0.31," Febuary 2008. [Online]. Available: http://dud.inf.tudresden.de/Anon_Terminology.shtml

41. Qian, J., Jiang, H., Yu, Y., Wang, H., & Miao, D. (2024). **Multi-level personalized k-anonymity privacy-preserving model based on sequential three-way decisions**. Expert Systems with Applications, 239, 122343.

42. Saxena, R., Arora, D., & Nagar, V. (2023). **Classifying blockchain cybercriminal transactions using hyperparameter tuned supervised machine learning models**. International Journal of Computational Science and Engineering, 26(6), 615-626.

43. Shirali, M., Tefke, T., Staudemeyer, R. C., & Pöhls, H. C. (2023). **A Survey on Anonymous Communication Systems with a Focus on Dining Cryptographers Networks**. IEEE Access, 11, 18631-18659.

44. Souad Benmeziane, Nadjib Badache, and Sihem Bensimessaoud, "Tor Network Limits," IEEE 2011 **International Conference on Network Computing and Information Security, 2011**.

45. **The crux of the NSA story in one phrase: 'collect it all'** . http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all. Retrieved on 2014.12.13.

46.Winkler, K., & Buchmann, E. (2018). **Dummy-based anonymization for voice-controlled IoT devices**. In Proceedings of the 12th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (pp. 1-8).