Scientific Bi-Quarterly Journal of Shahed University / Political Sociology of Islamic World
Vol.12 / No.01 / Spring & Summer 2024 (Serial 24)

Research article
DOI: 10.22070/iws.2025.19837.2399

Examining the Impact of the Internet of Things on Social Security in Iran

Hossein Emamvardi [1 *]
Fardin Ghoreishi [2]

Received on: 11/11/2023
Accepted on: 16/03/2024

Abstract

As a prominent development in the field of information technology, the Internet of Things (IoT) has far-reaching impacts on various social and security aspects of societies. This technology, particularly in developing countries like Iran, has significant implications for social security. The expansion of the IoT in Iran, while offering opportunities such as increased productivity, improved urban management, and the development of smart services, has also introduced numerous security challenges. In this context, the primary research question is: What opportunities and challenges does the Internet of Things present for the social security of the Islamic Republic of Iran? The main hypothesis posits that, on one hand, this technology can enhance public security and reduce organized crime by facilitating the monitoring, control, and analysis of big data. On the other hand, the growing reliance on the Internet of Things has heightened threats such as cyberattacks on critical infrastructure, violations of citizens' privacy, and the misuse of personal data by both governmental and non-governmental actors. Furthermore, the absence of comprehensive legal frameworks and weak policymaking in cybersecurity have exacerbated structural vulnerabilities in Iran. The present study, employing an exploratory approach, examines the effects of the Internet of Things on Iran's social security. By analyzing the security challenges associated with this technology, it demonstrates that achieving social security in this context requires adopting multi-layered strategies, including formulating protection policies, promoting public awareness, and strengthening national cybersecurity infrastructures. Finally, by offering practical solutions, this study paves the way for the optimal utilization of the Internet of Things to enhance social security and mitigate potential threats.

Keywords: Internet of Things, Social Security, Privacy, Security Policy, Iran.

1*. Ph.D Student in International Relations, University of Tehran, Iran.
(Corresponding Author: h.emamverdi@ut.ac.ir)
2 . Professor of International Relations, University of Tehran, Iran. (Email: ghoraishi583@ut.ac.ir).

Scientific Bi-Quarterly Journal of Shahed University / Political Sociology of Islamic World
Vol.12 / No.01 / Spring & Summer 2024 (Serial 24)

Research article
DOI: 10.22070/iws.2025.19837.2399

Extended Abstract

The Internet of Things (IoT), as an emerging and transformative technology, significantly impacts the social, economic, and administrative dimensions of societies. The central research question of this study is: What opportunities and challenges does the IoT present for social security in Iran? The research hypothesis argues that the IoT, on one hand, creates substantial opportunities through the collection and analysis of big data, optimization of industrial and urban processes, enhanced productivity, and improved quality of life for citizens. On the other hand, the increasing reliance on connected devices and networks introduces threats such as cyberattacks, privacy violations, and vulnerabilities in critical infrastructure. Consequently, the safe and effective utilization of IoT requires the development of comprehensive security policies and standards, the strengthening of cybersecurity infrastructure, and the promotion of public awareness. This technology simultaneously presents both opportunities and significant challenges for policymakers and users, making intelligent management essential to achieving sustainable and secure development.

Purpose: This study aims to examine the social and security opportunities, challenges, and risks arising from the development of Internet of Things (IoT) technology in Iran and to propose strategies for mitigating these risks. It seeks to analyze the applications of IoT across industrial, agricultural, healthcare, transportation, and critical infrastructure sectors to identify its potential benefits and positive impacts on productivity, quality of life, and resource management. Additionally, threats such as network intrusions, cyberattacks, and privacy violations are investigated to develop effective security measures and policies that enable the safe and sustainable adoption of IoT in the country.

Methodology: This study employs a qualitative research approach with an exploratory-analytical perspective. Data were collected from primary sources, including scholarly articles, reports, and official documents. Through content and comparative analyses, the social opportunities, challenges, and risks associated with the Internet of Things in Iran were identified, and practical recommendations were developed.

Findings: The findings indicate that the Internet of Things (IoT) in Iran holds significant potential to enhance economic, social, and industrial performance. In the industrial sector, the use of sensors and intelligent systems can increase factory productivity, prevent unexpected equipment failures, and reduce maintenance costs.

In agriculture, smart irrigation systems and the monitoring of soil moisture and weather conditions enable optimal management of water resources and reduce the use of chemical fertilizers. In healthcare, wearable devices and remote monitoring systems

Scientific Bi-Quarterly Journal of Shahed University / Political Sociology of Islamic World
Vol.12 / No.01 / Spring & Summer 2024 (Serial 24)

Research article
DOI: 10.22070/iws.2025.19837.2399

contribute to improved medical care, lower hospital costs, and better management of chronic diseases. The IoT also demonstrates transformative capabilities in the defense and security industries, including the updating of military equipment, data collection and analysis, process automation, and early detection of potential threats.

In the transportation and oil and gas sectors, intelligent equipment monitoring and traffic management can simultaneously enhance productivity and safety. The development of smart cities is supported by IoT-enabled intelligent traffic management, air quality monitoring, and optimized energy consumption.

Despite these opportunities, significant social and security challenges have been identified. These include unauthorized access to private networks, distributed denial-of-service (DDoS) attacks, data encryption weaknesses, privacy violations, and vulnerabilities in critical infrastructure. Limitations in software updates, constrained device resources, and the lack of unified security standards further exacerbate cyber threats.

Such vulnerabilities can disrupt public service delivery, reduce user trust, and potentially trigger social crises. Ultimately, the findings emphasize the urgent need for comprehensive security policies, strengthened data protection infrastructure, increased user awareness, and the adoption of robust security protocols. These measures are essential to ensure the safe and effective use of IoT technologies while minimizing associated social and political risks, thereby enabling Iran to harness the full potential of IoT in a secure and sustainable manner.

Conclusion: This study demonstrates that the Internet of Things (IoT), as a transformative technology, holds significant potential to enhance quality of life, increase productivity, and reduce costs in Iran. IoT can optimize processes and enable intelligent resource management across sectors such as industry, agriculture, healthcare, transportation, smart cities, and national defense. Simultaneously, the development of IoT also presents social and political security challenges, including unauthorized access to private networks, cyberattacks, privacy violations, and infrastructure vulnerabilities. The findings indicate that mitigating these threats requires comprehensive security policies, standardized protocols, continuous device updates, and increased public awareness.

Intelligent management and centralized monitoring of critical infrastructure, combined with collaboration among policymakers, service providers, and users, can ensure the safe and effective utilization of IoT. Overall, the responsible and secure deployment of this technology enables societies to harness its opportunities while minimizing associated social and political risks.

Keywords: Internet of Things, social security, privacy, security policy, Iran.

دوفصلنامه علمی جامعه‌شناسی سیاسی جهان اسلام، دوره ۱۲، شماره ۱، بهار و تابستان ۱۴۰۳ (پیاپی۲۴)

مقاله پژوهشی
DOI: 10.22070/iws.2025.19837.2399

بررسی تأثیر اینترنت اشیا بر امنیت اجتماعی ایران

حسین امام وردی [1*]
فردین قریشی [2]

تاریخ دریافت: ۱۴۰۲/۰۸/۲۰
تاریخ پذیرش: ۱۴۰۲/۱۲/۲۶

چکیده

اینترنت اشیاء به‌عنوان یکی از تحولات برجسته در عرصه فناوری اطلاعات، تأثیرات گسترده‌ای بر ابعاد مختلف اجتماعی و امنیتی جوامع دارد. این فناوری، به‌ویژه در کشورهای در حال توسعه مانند ایران، پیامدهای قابل‌توجهی در حوزه امنیت اجتماعی به همراه دارد. گسترش اینترنت اشیا در ایران ضمن فراهم آوردن فرصت‌هایی نظیر افزایش بهره‌وری، بهبود مدیریت شهری و توسعه خدمات هوشمند، چالش‌های امنیتی فراوانی نیز ایجاد کرده است. در این راستا، سؤال اصلی این پژوهش این است که اینترنت اشیاء چه فرصت‌ها و چالش‌هایی بر امنیت اجتماعی جمهوری اسلامی ایران به همراه دارد؟ فرضیه اصلی این است که از یک‌سو، این فناوری با تسهیل نظارت، کنترل و تحلیل داده‌های کلان، می‌تواند به تقویت امنیت عمومی و کاهش جرائم سازمان‌یافته کمک کند. از سوی دیگر، وابستگی روزافزون به اینترنت اشیاء، تهدیداتی نظیر حملات سایبری به زیرساخت‌های حیاتی، نقض حریم خصوصی شهروندان و سوءاستفاده از داده‌های شخصی توسط بازیگران دولتی و غیردولتی را افزایش داده است. علاوه بر این، فقدان چارچوب‌های قانونی جامع و ضعف سیاست‌گذاری در حوزه امنیت سایبری، آسیب‌پذیری‌های ساختاری را در ایران تشدید کرده است. پژوهش حاضر با رویکردی اکتشافی، به بررسی تأثیرات اینترنت اشیاء بر امنیت اجتماعی ایران پرداخته و با تحلیل چالش‌های امنیتی مرتبط با این فناوری، نشان می‌دهد که تحقق امنیت اجتماعی در این بستر نیازمند اتخاذ راهبردهای چندلایه‌ای از جمله تدوین سیاست‌های حفاظتی، ارتقای آگاهی عمومی و تقویت زیرساخت‌های امنیت سایبری در سطح ملی است. در نهایت، این مطالعه با ارائه راهکارهای عملی، زمینه‌ساز بهره‌برداری بهینه از اینترنت اشیاء در راستای تأمین امنیت اجتماعی و کاهش تهدیدات احتمالی می‌شود.

واژگان کلیدی: اینترنت اشیاء، امنیت اجتماعی، حریم خصوصی، سیاست‌گذاری امنیتی، ایران.

۱*. دانشجوی دکتری روابط بین االملل، دانشگاه تهران، ایران. (صفحه ۱۴۷-۱۸۰)
(نویسنده مسئول: h.emamverdi@ut.ac.ir)
۲. استاد گروه علوم سیاسی و روابط بین الملل، دانشگاه تهران، ایران. (ghoraishi583@ut.ac.ir)

مقدمه

تحولات معاصر عمدتاً ناشی از پیشرفت‌های قابل‌توجه در عرصه‌های علمی و فناوری است که تأثیرات عمیق و گسترده‌ای بر تمامی ابعاد زندگی انسانی گذاشته است. این تحولات، به‌ویژه در حوزه فناوری اطلاعات، به‌طور روزافزون موجب ظهور مفاهیم و اصطلاحات جدیدی می‌شوند که نه تنها نحوه زندگی، بلکه شیوه تعاملات اجتماعی، فرهنگی و اقتصادی جوامع را دگرگون کرده‌اند. در این زمینه، فناوری اطلاعات به‌ویژه در دهه‌های اخیر، در تغییر ماهیت زندگی روزمره انسان‌ها نقشی محوری ایفا کرده است. این امر به‌ویژه در حوزه‌های اجتماعی، فرهنگی و سیاسی نمایان است، زیرا فناوری‌های نوین همچون اینترنت و شبکه‌های ارتباطی توانسته‌اند ساختارهای حکمرانی و امنیت ملی کشورهای مختلف را تحت تأثیر قرار دهند. از اواخر قرن بیستم، با گسترش سریع ارتباطات رایانه‌ای و دسترسی روزافزون مردم به اینترنت و شبکه‌های رایانه‌ای، تحولات بنیادینی در روابط بین‌الملل و حکمرانی به وقوع پیوسته است. ویژگی‌های منحصر به فرد اینترنت مانند تعامل‌پذیری، هم‌زمانی ارتباطات، فراگیری و غیرمتمرکز بودن، آن را از رسانه‌های جمعی سنتی مانند تلویزیون و رادیو متمایز کرده و موجب شده که این ابزار به ابزاری قدرتمند در تغییر سیاست‌ها و حتی تهدیدات امنیت ملی کشورها تبدیل گردد. با ظهور و گسترش سریع فضای سایبری، مفاهیم مرتبط با جنبه‌های مختلف زندگی انسانی دچار تحولات بنیادین شده‌اند. در این راستا، مفاهیمی همچون هویت، فرهنگ، حاکمیت و تعاملات فردی و اجتماعی معانی جدید و پیچیده‌تری به خود گرفته‌اند که این تغییرات ناشی از تأثیرات فضای دیجیتال بر ساختارهای اجتماعی، سیاسی و فرهنگی جوامع است.

در این میان، یکی از مفاهیم نوظهور و تأثیرگذار در حوزه فناوری اطلاعات، «اینترنت اشیاء»[1] است که برای نخستین بار در سال ۱۹۹۹ توسط «کوین اشتوین»[2] مطرح شد. این فناوری که به‌عنوان بخشی از تکامل فناوری‌های سایبری و ابزارهای ارتباطی نوین به شمار می‌رود، نویددهنده ایجاد جهانی است که در آن تمامی اشیاء روزمره از جمله وسایل خانگی، خودروها و زیرساخت‌های شهری به اینترنت متصل شده و بدون دخالت انسان با یکدیگر تعامل خواهند داشت. در دنیای اینترنت اشیاء، اشیاء بی‌جان نیز هویت دیجیتالی خاص خود را کسب کرده‌اند و از این رو، دستگاه‌هایی نظیر کامپیوترها، موبایل‌ها، وسایل خانگی و تجهیزات دیگر با یکدیگر و کاربران خود

1. Internet of Things (IoT)
2. Kevin Ashton

به‌طور دو سویه در تعامل هستند تا به بهبود کیفیت زندگی کمک کنند. اینترنت اشیاء با تغییر جهت فناوری از سیستم‌هایی که بر مبنای تعامل دستگاه‌ها با چندین کاربر بودند، به سوی پارادایمی جدید پیش رفته است. در این پارادایم نوین، هر کاربر ممکن است چندین دستگاه داشته باشد و اشیاء با یکدیگر متصل شوند. این فناوری که به نوعی نمایانگر انقلاب جدیدی در عرصه اینترنت است، این امکان را فراهم می‌آورد که اشیاء با قابلیت شناسایی خود، به تبادل اطلاعات پرداخته و هویت هوشمند خود را ایجاد کنند. خدمات ارائه شده از سوی اینترنت اشیاء، کاربردهای آن را به‌طور چشمگیری افزایش داده‌اند، به‌گونه‌ای که نه تنها به بهبود کیفیت زندگی کمک می‌کنند، بلکه احتمال تغییر در سبک زندگی افراد را نیز در پی دارند. گسترش اینترنت اشیاء در کشور و تجاری‌سازی اشیاء پوشیدنی هوشمند نظیر عینک‌های هوشمند، گوشی‌های هوشمند، تلویزیون‌ها، یخچال‌ها، خودروها و سایر تجهیزات منجر به تولید حجم عظیمی از داده‌ها می‌شود که به سمت سرورهای صاحبان فناوری ارسال می‌گردد. این جریان گسترده داده‌ها فرصت‌هایی را برای تحلیل‌های عمیق‌تر و بهبود خدمات و محصولات ارائه شده ایجاد می‌کند.

در این مقاله، هدف اصلی شناسایی و تحلیل الگوهای پنهان موجود در داده‌ها است که از همگرایی اطلاعات با اشیاء در بستر اینترنت اشیاء ناشی می‌شود. این همگرایی، به دلیل ارتباط مستقیم میان داده‌ها و اشیاء فیزیکی، می‌تواند به‌طور قابل‌توجهی زمینه‌ساز دستکاری، تقلب یا سرقت داده‌ها گردد. چنین تهدیداتی می‌توانند پیامدهای جدی و غیرقابل پیش‌بینی بر امنیت اجتماعی جمهوری اسلامی ایران داشته باشند. از آنجا که امنیت اجتماعی به‌عنوان یکی از ارکان حیاتی ثبات اجتماعی و سیاسی هر کشور مطرح است، نفوذ و آسیب‌پذیری‌های ناشی از اینترنت اشیاء می‌تواند به‌طور عمده چالش‌های جدیدی را در زمینه حفظ امنیت عمومی ایجاد کند. در این راستا، این پژوهش به بررسی فرصت‌ها و چالش‌های ناشی از اینترنت اشیاء بر امنیت اجتماعی جمهوری اسلامی ایران می‌پردازد. این پژوهش در سه بخش اصلی سامان یافته است. در بخش نخست، پیشینه تحقیق مورد بررسی قرار می‌گیرد و ضمن مرور پژوهش‌های پیشین، وجوه تمایز این مطالعه با تحقیقات پیشین تبیین می‌شود. بخش دوم به مرور مفاهیم اساسی اختصاص دارد و در آن، مفاهیمی نظیر ارتباطات ماشین به ماشین، اینترنت اشیا و ظهور فناوری‌های نوین در حوزه امنیت اجتماعی و معماری اینترنت اشیا مورد بررسی قرار می‌گیرد. در بخش سوم، تجزیه‌وتحلیل یافته‌های تحقیق انجام می‌شود. در این بخش، ضمن بررسی وضعیت اینترنت اشیا در ایران، فرصت‌ها و چالش‌های مرتبط با توسعه آن در امنیت اجتماعی

کشور تحلیل می‌شود و در نهایت، راهکارهای پیشنهادی برای کاهش مخاطرات اجتماعی ناشی از اینترنت اشیا در ایران ارائه خواهد شد.

الف- مروری بر پیشینه پژوهش

با وجود اهمیت بالای موضوع، پژوهش‌های علمی و جامع خاصی در زمینه تبیین فرصت‌ها و چالش‌های گسترش اینترنت اشیاء بر امنیت اجتماعی جمهوری اسلامی ایران به‌طور خاص انجام نشده است. با این حال، تعدادی از پژوهش‌های محدود در این حوزه وجود دارند که به شرح زیر ارائه می‌شوند.

- حمید دژگیر و هانیه هوشمند (۱۳۹۶) در مقاله‌ای با عنوان «مروری بر امنیت در اینترنت اشیاء»، بر این نکته تأکید کرده‌اند که چالش‌های امنیتی اینترنت اشیاء فراتر از تهدیدات اینترنت است و به دنبال ارائه سناریوهایی برای مقابله با حملات بالقوه اینترنت اشیاء هستند. آن‌ها در این مقاله با معرفی فناوری «باند باریک»[1] که به ادغام اطلاعات، فشرده‌سازی و کاهش حجم داده‌ها می‌پردازد، چارچوبی را برای کاهش تأثیرات حملات بر حریم خصوصی و امنیت مصرف‌کنندگان ارائه کرده‌اند.

- قدسی، امیر (۱۳۹۲) در مقاله‌ای با عنوان «تأثیر فضای مجازی بر امنیت جمهوری اسلامی ایران و ارائه راهبرد»، به آسیب‌پذیری امنیت ملی کشور در برابر کارکرد سیاسی فضای مجازی پرداخته و بررسی چالش تهدید را به‌عنوان اولویت نخست مطرح کرده است. وی به ضرورت مواجهه فعال با تهدیدات فضای سایبر از جمله تأسیس مرکز سیاست‌گذاری مدیریت یکپارچه، بهره‌گیری از ظرفیت‌های جامعه و تقویت سرمایه اجتماعی به‌عنوان راهبردهای کلیدی اشاره می‌کند.

صالحی، سید جواد و همکاران (۱۳۹۲) در مقاله «بررسی نقش اینترنت در جنبش اجتماعی مصر»، نشان دادند که اینترنت و به‌ویژه شبکه‌های اجتماعی در جنبش اجتماعی مصر سال ۲۰۱۱ نقشی تعیین‌کننده ایفا کرده‌اند. به باور آنان، رسانه‌های اجتماعی همچون فیس‌بوک، توییتر و وبلاگ‌ها با ایجاد بستر آگاهی‌بخشی، عبور از سانسور دولتی و تسهیل ارتباطات سیاسی، زمینه بسیج مردمی و سازماندهی اعتراض‌ها را فراهم ساختند. این فرایند نه‌تنها سرعت و گستره اعتراض‌ها را افزایش داد، بلکه الگویی نوین از جنبش‌های اجتماعی و انقلاب‌های مردمی را در خاورمیانه و شمال آفریقا به نمایش گذاشت.

- میر محمدیان، سید میلاد و همکاران (۱۳۹۶) در پژوهشی با عنوان «مروری بر چالش‌ها و

1 . Narrowband

راهکارهای پیشگیری از چالش‌های اینترنت اشیاء»، به بررسی سیستم‌های مختلف امنیتی برای مقابله با چالش‌های امنیتی اینترنت اشیاء پرداخته و فیلترهای چهارگانه در استراتژی دفاع امنیتی را معرفی کرده‌اند. این فیلترها شامل محاسبه خطر، کشف تهدید، تشخیص امنیت و پاسخ به تهدیدات امنیتی هستند.

– محمدرضا مصلحی و حسین ابراهیم پور کومله (۱۳۹۶) در مقاله‌ای با عنوان «اینترنت اشیاء و چالش‌های امنیتی آن»، به نبود توافق جامع بر روی معماری و استانداردهای مورد نیاز در امنیت اینترنت اشیاء اشاره کرده و این عامل را به‌عنوان یکی از مهم‌ترین موانع به‌کارگیری یکپارچه مکانیزم‌های امنیتی معرفی کرده‌اند. آن‌ها با تمرکز بر رویکرد خانه‌های هوشمند در فضای اینترنت اشیاء، به قابلیت نفوذ به حریم خصوصی افراد و داده‌های صریح مرتبط با ساکنان خانه‌ها توجه کرده‌اند. این مقاله همچنین مؤلفه‌های امنیتی مختلفی را مطرح می‌کند، از جمله استفاده از موقعیت جغرافیایی، سطوح مختلف حریم خصوصی برای داده‌ها، شناسه‌های قوی و تقویت روش‌های متمرکز شبکه جهت جلوگیری از حملات. در نهایت، آن‌ها بر لزوم اتخاذ پروتکل‌هایی برای کاهش تأخیر یا ایجاد اتصال‌های گذرا با قابلیت تحمل بیشتر تأکید کرده‌اند.

با توجه به اهمیت موضوع و لزوم بررسی تأثیرات اینترنت اشیاء بر امنیت اجتماعی در ایران، پژوهش‌های پیشین عمدتاً بر جنبه‌های فنی، تهدیدات سایبری و چالش‌های امنیتی این فناوری تمرکز داشته‌اند، اما مطالعه‌ای جامع و علمی در زمینه بررسی فرصت‌ها و چالش‌های اینترنت اشیاء بر امنیت اجتماعی جمهوری اسلامی ایران صورت نگرفته است. به‌ویژه، تأثیرات این فناوری بر ساختارهای اجتماعی، فرهنگی و امنیتی کشور در راستای ایجاد فرصت‌ها برای بهبود وضعیت امنیت اجتماعی و همچنین چالش‌های احتمالی آن برای امنیت عمومی و نظم اجتماعی، به‌طور ملموس مورد توجه قرار نگرفته است. این مقاله در پی پرکردن این خلأ پژوهشی است و به‌طور خاص به بررسی فرصت‌ها و چالش‌های اینترنت اشیاء در تأمین و تهدید امنیت اجتماعی ایران می‌پردازد.

ب- مرور مفاهیم اساسی

۱- ارتباطات ماشین به ماشین تا اینترنت اشیاء

«ارتباطات ماشین به ماشین»[1] مفهومی گسترده در حوزه فناوری است که به سامانه‌هایی اطلاق

1. Machine to Machine communications

می‌شود که امکان تبادل خودکار داده‌ها میان دستگاه‌های مکانیکی و الکترونیکی را بدون نیاز به مداخله انسانی فراهم می‌کنند. این فناوری که عمدتاً بر بستر شبکه‌های بی‌سیم توسعه یافته است، امکان تعامل سنسورها و دستگاه‌ها را با یکدیگر و با کاربرانشان فراهم می‌آورد. از نمونه‌های ساده آن می‌توان به ارتباط یک گوشی هوشمند با تلویزیون اشاره کرد، درحالی‌که نمونه‌های پیچیده‌تر شامل نظارت بر زیرساخت‌های شهری، مدیریت ترافیک و توسعه شبکه‌های هوشمند است. چنین تعاملاتی نه‌تنها کارایی سیستم‌ها را افزایش می‌دهد، بلکه به بهینه‌سازی عملکرد و ارتقای کیفیت خدمات نیز منجر می‌شود (Fadlullah et al, 2016). بحث اولیه درباره ظهور ارتباطات ماشین به ماشین نخستین بار توسط «خوان کونتی»[1] مطرح شد. این فناوری از آن زمان تاکنون به‌شدت گسترش یافته و بر تمامی ابعاد زندگی تأثیر گذاشته است. حوزه‌های متنوعی ازجمله فناوری اطلاعات، صنایع غذایی، کشاورزی، انرژی، معدن و صنایع نفت و گاز به‌طور گسترده از این فناوری بهره می‌برند. رشد ارتباطات ماشین به ماشین را می‌توان به سه عامل کلیدی نسبت داد: (۱) افزایش تعداد ماشین‌های صنعتی و لوازم خانگی مجهز به پردازنده‌های قدرتمند و کم‌هزینه، (۲) گسترش اینترنت به‌عنوان یک بستر استاندارد ارتباطی و (۳) کاهش هزینه فناوری‌های ارتباطی بی‌سیم (Bandyopadhyay & Sen, 2011).

مفهوم اینترنت اشیاء ارتباط نزدیکی با ارتباطات ماشین به ماشین دارد. بااین‌حال، تفاوت اصلی میان این دو در حوزه کاربرد و مقیاس آن‌ها نهفته است. درحالی‌که اینترنت اشیاء بیشتر در فضای مصرف‌کننده و زندگی روزمره پذیرفته شده است، ارتباطات ماشین به ماشین ماهیت صنعتی‌تری دارد و بیشتر در سامانه‌های زیرساختی و تجاری به کار گرفته می‌شود. در واقع، اینترنت اشیاء را می‌توان نسخه تکامل‌یافته ارتباطات ماشین به ماشین دانست که مبتنی بر شبکه‌های «پروتکل اینترنت»[2] توسعه یافته و قادر است طیف گسترده‌تری از دستگاه‌های ناهمگن و اشیاء هوشمند را در یک اکوسیستم واحد ادغام کند. علاوه بر این، اینترنت اشیاء با قابلیت مدیریت حجم عظیمی از داده‌های تولیدشده توسط دستگاه‌های متصل، ارتباطی مقیاس‌پذیر و یکپارچه را فراهم می‌سازد (Bandyopadhyay & Sen, 2011). این ویژگی‌ها، اینترنت اشیاء را به یک بستر حیاتی در تحول دیجیتال و توسعه زیرساخت‌های هوشمند تبدیل کرده است.

1. Juan Conti
2. Internet Protocol

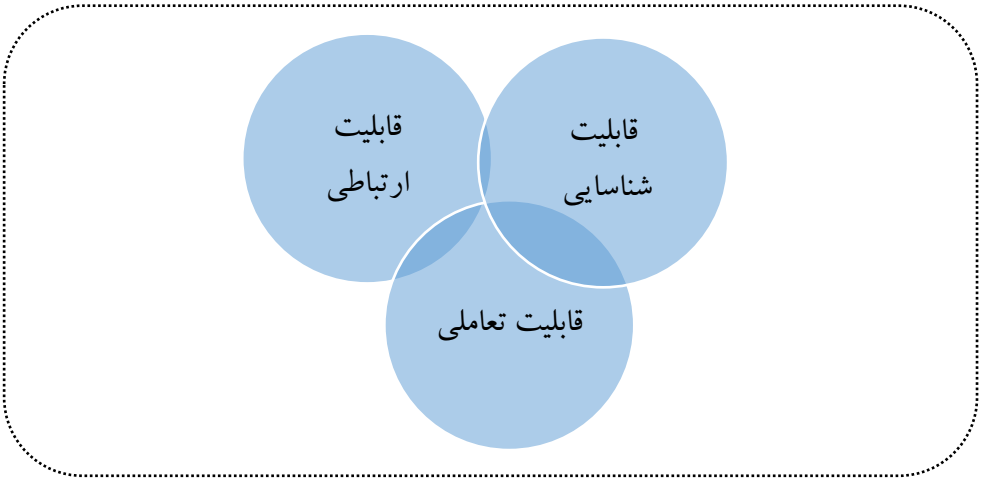
مفهوم اینترنت اشیاء نخستین بار در سال ۱۹۹۹ توسط «کوین اشتون» مطرح شد. این فناوری به یک شبکه گسترده از اشیاء و دستگاه‌های متصل اشاره دارد که می‌توانند به‌صورت هوشمند و خودکار داده‌ها را دریافت، پردازش و منتقل کنند. این شبکه شامل دستگاه‌های ناهمگن (با قابلیت‌ها و استانداردهای متفاوت) و دستگاه‌های همگن (با ویژگی‌های مشترک) است که در تعامل با یکدیگر، عملکردی یکپارچه و کارآمد ایجاد می‌کنند. اینترنت اشیاء طیف وسیعی از دستگاه‌های تعبیه‌شده و هوشمند را در برمی‌گیرد که با اتصال به یکدیگر، امکان ایجاد سیستم‌های پیشرفته و هوشمند را فراهم می‌سازند. هدف اصلی این فناوری، تسهیل ارتباطات، افزایش کارایی و بهینه‌سازی فرایندها در حوزه‌های مختلف از جمله حمل‌ونقل، سلامت، مدیریت شهری، امنیت و صنعت است. ویژگی کلیدی اینترنت اشیاء امکان اتصال هر شیء، در هر مکان، در هر زمان و از طریق هر وسیله‌ای است که به تحولی بنیادین در شیوه زندگی و تعاملات اجتماعی منجر شده است. شکل شماره (۱) این نکته را به تصویر می‌کشد.

شکل شماره ۱- ویژگی‌های اینترنت اشیاء

(منبع: محقق ساخته)

به‌طور کلی، اینترنت اشیاء شامل سه مؤلفه اصلی است: نخست، شبکه‌ای که امکان اتصال میان دستگاه‌های همگن و ناهمگن هوشمند را فراهم می‌کند؛ دوم، فناوری‌های زیربنایی مورد نیاز برای پشتیبانی و تحقق این ارتباطات، ازجمله حسگرها و عملگرها؛ و سوم، خدمات و برنامه‌های کاربردی

که در حوزه‌های مختلف از این قابلیت‌ها بهره مـی‌برنـد (Abdul-Qawy & Tadisetty, 2015). شـکل شماره (۲) شرایط لازم برای ساخت اینترنت اشیاء را نمایش می‌دهد.



شکل شماره ۲- شرایط ساخت اینترنت اشیاء

(منبع: محقق ساخته)

با این حال، پیچیدگی اینترنت اشیاء صرفاً بـه گسـترش و تکامـل اینترنـت و ادغـام فنـاوری‌هـای کلیدی با شبکه‌های مبتنی بر پروتکل‌های اینترنت محدود نمی‌شود، بلکه در توانایی تعبیه اطلاعات در اشیاء نهفته است، به‌گونه‌ای که این اشیاء بتوانند به‌طور خودکار و مستقل عمـل کننـد. قابلیـت اتصـال مستقیم اشیاء به یکدیگر و امکان تعامل و تبادل اطلاعات میـان آن‌هـا، از دیگـر ابعـاد پیچیـدگی ایـن فناوری است. یکی از ویژگی‌های کلیدی اینترنت اشیاء، هوش تعبیه‌شده در اشیاء هوشـمند اسـت کـه مستقل از شبکه عمل کرده و لزوماً به اینترنت متصل نیست. علاوه بر این، اینترنـت اشـیاء سـه هـدف اساسی را دنبال می‌کند: **نخست**، برقراری ارتباط گسترده‌تر کـه بـه تعـداد دسـتگاه‌هـای متصـل، نـوع فناوری‌های به‌کاررفته و شیوه اتصال آن‌ها وابسته است؛ **دوم**، ادراک و یکپارچه‌سازی اطلاعات کـه بـا چالش‌هایی همچون ناهماهنگی، ناسازگاری و عدم دقت داده‌ها مواجه است؛ **و سـوم**، ارائـه خـدمات هوشمند جامع‌تر که در آن اشیاء هوشمند قادرند بـه‌طـور کارآمـد محـیط را تحـت کنتـرل درآورده و خدمات پیشرفته‌ای ارائه دهند (Miorandi et al, 2012).

۲- پیدایش فناوری‌های نوظهور در زمینه امنیت اجتماعی

پیشرفت‌های فناورانه در حوزه‌هایی مانند ارتباطات، هوش مصنوعی و روباتیک، تحولات مهمی در امنیت اجتماعی و سیاسی ایجاد کرده‌اند. در این چارچوب، هنجارها و مکانیسم‌های حاکمیتی بر تقویت امنیت سایبری و ثبات بین‌المللی تأکید دارند. با این حال، حمایت ناکافی برخی دولت‌ها از این هنجارها و افزایش تهدیدات سایبری، به‌ویژه در بخش‌های حیاتی مانند مراقبت‌های بهداشتی و صنعتی، نگرانی‌های جدیدی را برانگیخته است. فناوری‌های نوظهور از طریق تأثیرگذاری بر فعالیت‌های نظامی و اطلاعاتی، به یکی از عناصر کلیدی امنیت ملی تبدیل شده‌اند. ازاین‌رو، مدیریت این فناوری‌ها مستلزم راهکارهای چندجانبه‌ای است که با مشارکت بازیگران مختلف، به توسعه سازوکارهای فنی و نظارتی منجر شود (Kavanagh, 2019).

بر اساس گزارش گارتنر، چالش‌ها و فرصت‌های فناوری‌های نوظهور در امنیت اجتماعی و سیاسی در سه حوزه اصلی مطرح می‌شوند. نخست، «اعتماد مهندسی»[1] که به امنیت، قابلیت اطمینان و شیوه‌های کاری مرتبط است. برای هدایت تحول دیجیتال، گروه‌های فناوری اطلاعات باید یک زیرساخت تجاری قابل اعتماد ایجاد کنند که بر شیوه‌های کاری مقیاس‌پذیر و نوآورانه متکی باشد. دوم، «تسریع رشد»[2] که بر ابتکاراتی تمرکز دارد که فرصت‌های جدیدی برای سازمان‌ها فراهم کرده و تعادل میان ریسک فناوری و اهداف اقتصادی را حفظ می‌کند. سوم، «تغییر مکانیسم»[3] که بر کاهش ریسک از طریق هدایت تغییرات تأکید دارد. در این راستا، فناوری‌ها می‌توانند نقش کلیدی در مدیریت تغییر و جلوگیری از بی‌ثباتی ایفا کنند (Gartner, 2021).

فناوری‌های دیجیتال نوظهور، از جمله هوش مصنوعی، اینترنت اشیاء، محاسبات ابری، بلاک‌چین و محاسبات کوانتومی، در رفع نیازهای روزمره افراد و جامعه نقش اساسی ایفا می‌کنند. این فناوری‌ها که به عنوان «فناوری‌های مرزی»[4] شناخته می‌شوند، از دیجیتالی‌شدن و اتصال بهره برده و ترکیب آن‌ها تأثیر چشمگیری دارد. تعاملات دیجیتال به حجم بالایی از داده‌ها متکی است که توسعه ابزارهای «ابر داده‌ها»[5] را تسهیل می‌کند. همچنین، رایانش ابری، برون‌سپاری نرم‌افزار و سخت‌افزار و اتوماسیون

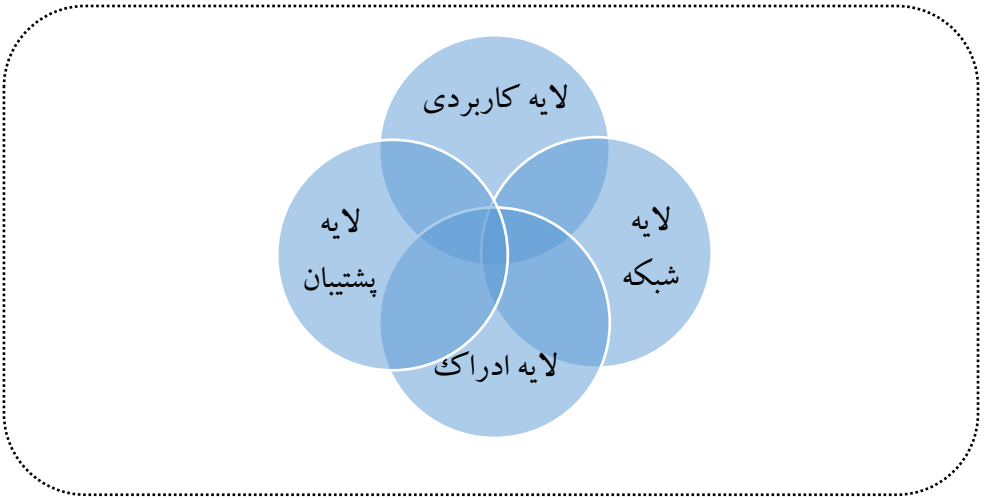
1. Engineering Trust
2. Accelerate growth
3. change mechanism
4. frontier technologies
5. Big Data

فرآیندها به پیشرفت اینترنت اشیاء کمک کرده است. این فناوری، زندگی اجتماعی را متحول کرده و با توسعه برنامه‌های کاربردی، ارائه خدمات به افراد را بهبود می‌بخشد، به‌ویژه در تلفن‌های همراه و رسانه‌های اجتماعی (Shnurenko et al, 2020).

با ظهور عصر عظیم اینترنت اشیاء، چالش‌های شبکه‌ای از جمله کیفیت خدمات، قابلیت اطمینان، هزینه، مصرف انرژی و زمان خدمات مطرح می‌شوند. از مهم‌ترین مسائل آن، امنیت و حریم خصوصی است که به کنترل و محافظت از اطلاعات شخصی مربوط می‌شود. علاوه بر این، کمبود متخصصان و آموزش ناکافی نیز از موانع اصلی توسعه این فناوری محسوب می‌شود (Madra et al, 2020: 27). اینترنت اشیاء مبتنی بر هوش مصنوعی در راستای اتوماسیون عمل کرده و قابلیت توسعه الگوریتم‌های پیشرفته امنیت سایبری را دارد. در سال‌های اخیر، این فناوری پارادایم‌های امنیتی و استراتژی‌های فناورانه را دگرگون ساخته است. ابتدا در خانه‌های هوشمند و خودروها به کار گرفته شد، اما امروزه در ترکیب با سایر فناوری‌ها در حوزه‌های حیاتی مورد استفاده قرار می‌گیرد .استفاده از اینترنت اشیاء در زیرساخت‌های حیاتی و دفاعی می‌تواند به تحقق اهداف امنیتی کمک کند، هرچند همواره چالش‌های امنیت ملی را نیز به همراه دارد؛ بنابراین، پیاده‌سازی آن در حوزه‌های حساس مستلزم پژوهش‌های دقیق و تحلیل‌های راهبردی است.

۳- معماری اینترنت اشیاء: چالش‌ها و ملاحظات امنیتی

اینترنت اشیاء به شبکه‌ای از اشیاء فیزیکی اشاره دارد که از طریق اینترنت به یک سکوی مشترک متصل شده و امکان تعامل و ارتباط میان افراد و اشیاء را در هر زمان و مکان از طریق شبکه‌ها و خدمات مختلف فراهم می‌کند. با وجود آنکه تنها ۰.٦ درصد از دستگاه‌های بالقوه به اینترنت اشیاء متصل شده‌اند، پیش‌بینی می‌شود تا سال ۲۰۲۳ بیش از ۵۰ میلیارد دستگاه به این شبکه متصل شوند (Baniya et al, 2024: 154). معماری اینترنت اشیاء که به‌طور گسترده پذیرفته شده است، از چهار لایه تشکیل شده است که در شکل زیر نمایش داده شده است. این لایه‌ها نقش کلیدی در عملکرد، امنیت و یکپارچگی این فناوری دارند و بررسی آن‌ها به درک بهتر چالش‌ها و ملاحظات امنیتی مرتبط با اینترنت اشیاء کمک می‌کند.



شکل شماره ۳- معماری چهار لایه اینترنت اشیاء

(منبع: محقق ساخته)

۳-۱- لایه کاربردی

«لایه کاربردی»[1] اینترنت اشیاء ترکیبی از نیازهای اجتماعی و صنعتی این فناوری است که با هدف تحقق همگرایی عمیق میان فناوری‌های صنعتی و اینترنت اشیاء طراحی شده است. این لایه به گونه‌ای توسعه یافته که نیازهای خاص هر صنعت را برآورده کرده و از طریق تقسیم کار هوشمند، مشابه الگوی اجتماعی انسانی، به پیشرفت جوامع کمک کند. با وجود پیشرفت‌های فناوری، اینترنت اشیاء هنوز به‌صورت گسترده در حوزه‌های کاری و زندگی روزمره انسان‌ها به کار گرفته نشده و در مراحل اولیه توسعه مقیاس‌پذیر خود قرار دارد.

۳- ۲- لایه ادراک

«لایه ادراک»[2] را می‌توان به عنوان حواس اینترنت اشیاء در نظر گرفت که وظیفه اصلی آن شناسایی اشیا و جمع‌آوری داده‌ها است. این لایه از فناوری‌هایی مانند بارکدخوان‌ها، برچسب‌های دو بعدی، دوربین‌ها، سیستم‌های GPS، پایانه‌ها و شبکه‌های حسگر تشکیل شده است. نقش کلیدی آن،

1. Application layer
2. Perception layer

تسهیل فرآیند تشخیص و ادراک محیط پیرامون از طریق جمع‌آوری و انتقال اطلاعات برای پردازش و تحلیل در سطوح بالاتر معماری اینترنت اشیاء است.

۳-۳- لایه پشتیبان

«لایه پشتیبان»[1] مسئولیت‌های متعددی را بر عهده دارد که شامل تجزیه و تحلیل داده‌ها، کنترل امنیت، مدل‌سازی فرآیندها، مدیریت دستگاه‌ها و مدیریت جریان داده‌ها و اطلاعات است. این لایه همچنین به یکپارچه‌سازی مکانیسم‌های دسترسی به اطلاعات پرداخته و به دلیل حجم بالای داده‌ها، ضرورت فیلترینگ در فرآیند استخراج اطلاعات بسیار حائز اهمیت است. هدف از این فیلترینگ، تسهیل پردازش داده‌های کلان و دستیابی به یک چشم‌انداز جامع و معتبر از اطلاعات موجود است.

۳-٤- لایه شبکه

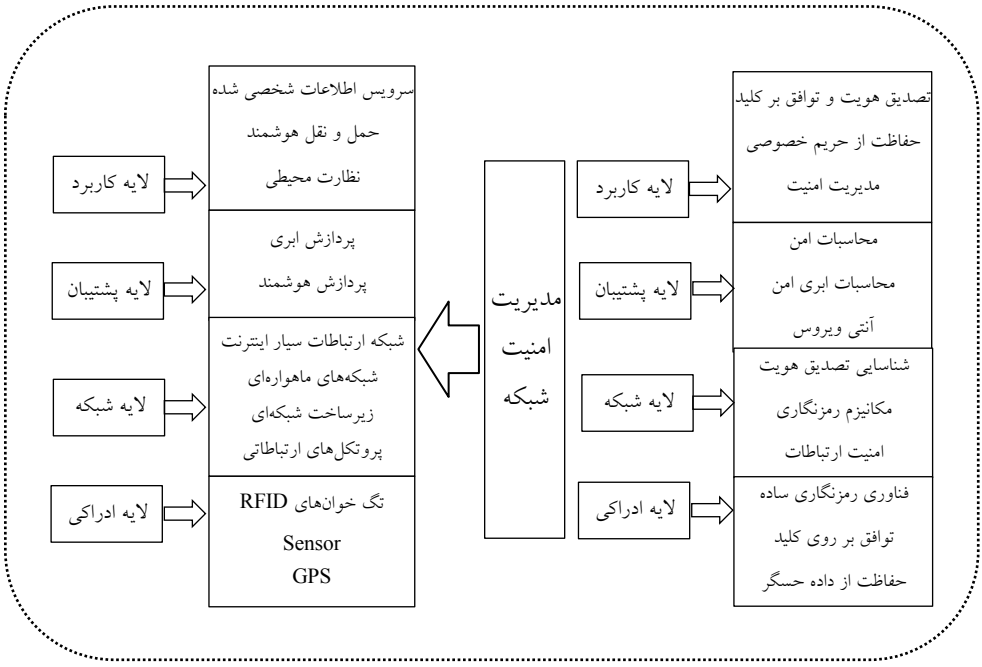
«لایه شبکه»[2] به عنوان مغز و شبکه عصبی اینترنت اشیاء عمل می‌کند و وظیفه اصلی آن پردازش و انتقال اطلاعات است. این لایه شامل یک شبکه یکپارچه است که هم اینترنت و هم شبکه‌های ارتباطی را در بر می‌گیرد و اجزای ضروری مانند پردازش هوشمند، مرکز اطلاعات و مرکز مدیریت شبکه را شامل می‌شود. لایه شبکه داده‌هایی را که از لایه ادراک دریافت کرده است، پردازش کرده و به مقاصد مختلف ارسال می‌کند.

پیاده‌سازی اینترنت اشیاء باید با رعایت قوانین، استانداردهای اخلاقی، نیازهای اجتماعی و سیاست‌های مربوطه انجام شود. در این راستا، چالش‌های قانونی، رویکردهای سیستمی، چالش‌های فنی و تجاری باید به دقت بررسی شوند. امنیت در اینترنت اشیاء باید از مراحل ابتدایی طراحی تا ارائه خدمات به‌طور جامع پوشش داده شود. چالش‌های تحقیقاتی اصلی در این زمینه شامل مسائل محرمانگی داده‌ها، حریم خصوصی و اعتماد هستند. الزامات امنیتی اینترنت اشیاء بر اساس معماری سه لایه‌ای آن تعریف می‌شوند که هر یک از این لایه‌ها ظرفیت ارائه کنترل‌های امنیتی متناظر خود را دارند. این کنترل‌ها شامل کنترل دسترسی، احراز هویت دستگاه، حفظ یکپارچگی و محرمانگی داده‌ها در حین انتقال و همچنین تضمین دسترسی‌پذیری و مقاومت در برابر ویروس‌ها و حملات سایبری هستند. این رویکرد چند لایه به تقویت امنیت جامع سیستم‌های اینترنت اشیاء کمک می‌کند.

1. Backing layer
2. network layer

دنیای دیجیتال امروز با حجم عظیمی از داده‌های شخصی، اشتراکی و ثبت‌شده توسط افراد روبه‌رو است که این موضوع نگرانی‌های جدی در زمینه امنیت و حفاظت از اطلاعات افراد و دولت‌ها ایجاد کرده است. افزایش تبادل و پردازش داده‌ها، به ویژه داده‌های ناخواسته، موجب بروز چالش‌های زیادی از جمله نقض حریم خصوصی، استفاده غیرمجاز از اطلاعات و عدم شفافیت در نحوه جمع‌آوری و پردازش داده‌ها شده است. این نگرانی‌ها ضرورت تدوین و اجرای قوانین سخت‌گیرانه‌تر و بهبود پروتکل‌های امنیتی را ایجاب می‌کند تا اعتماد کاربران به سیستم‌های دیجیتال بازگردد و حقوق بنیادین آن‌ها محافظت شود (Whitmore & Agarwal, 2014).

با گسترش سریع کاربردهای اینترنت اشیاء، مسائل امنیت اجتماعی و سیاسی به یکی از نگرانی‌های اصلی تبدیل شده‌اند. این نگرانی‌ها عمدتاً به موضوعات محرمانگی اطلاعات و ناتوانی افراد در کنترل حریم خصوصی خود مرتبط است. نظارت بر فعالیت‌های روزانه افراد و تولید داده‌های مستمر توسط آن‌ها می‌تواند تأثیرات جدی بر فعالیت‌های سیاسی، اقتصادی و اجتماعی داشته باشد و



شکل شماره ٤- معماری امنیتی اینترنت اشیاء و نیازمندی‌های امنیتی

(منبع: شفیعی، ۱۳۹۴)

نگرانی‌های قابل توجهی در خصوص حریم خصوصی ایجاد کند. نقض امنیت، حملات سایبری و اختلال در عملکرد سیستم‌ها می‌تواند به کاهش مزایای اینترنت اشیاء منجر شود. در آینده‌ای نزدیک،حجم عظیمی از اطلاعات توسط دستگاه‌های متصل و سیستم‌های مدیریتی منتقل خواهد شد و رویکردهای تبادل اطلاعات به طور قابل توجهی تغییر خواهد کرد (Gang & Zeyong & Jun, 2011). جدول بالا نمای کلی از معماری امنیتی اینترنت اشیاء را نشان می‌دهد که هر لایه آن نیازمند توجه ویژه به جنبه‌های امنیتی برای محافظت از اطلاعات و سیستم‌ها در برابر تهدیدات است.

٤- تهدیدات اجتماعی و سیاسی توسعه اینترنت اشیاء

اینترنت اشیاء به دلیل گسترش سریع کاربردها و اتصالات، با چالش‌ها و آسیب‌پذیری‌های زیادی در زمینه امنیت اجتماعی و سیاسی مواجه است. این آسیب‌پذیری‌ها می‌توانند به پاشنه آشیل اینترنت اشیاء تبدیل شوند و نگرانی‌های جدی را در خصوص حریم خصوصی، امنیت داده‌ها و یکپارچگی سیستم‌ها به وجود آورند. برخی از این چالش‌ها و آسیب‌پذیری‌ها عبارت‌اند از: (Atzori et al, 2010).

- **احراز هویت ضعیف:** بسیاری از دستگاه‌های اینترنت اشیاء از رمزهای عبور ساده و غیرقابل قبول استفاده می‌کنند که به راحتی قابل حدس یا شکستن هستند. این موضوع فضای مناسبی برای حملات سایبری ایجاد می‌کند.
- **امنیت ناکافی در نرم‌افزار:** بسیاری از دستگاه‌های اینترنت اشیاء با نرم‌افزارهایی تولید می‌شوند که به‌روزرسانی‌های امنیتی را دریافت نمی‌کنند یا به راحتی قابل به‌روزرسانی نیستند. این مسئله می‌تواند به نفوذ مهاجمین منجر شود.
- **نقص در رمزنگاری:** داده‌های منتقل شده بین دستگاه‌ها معمولاً به‌طور کامل رمزنگاری نمی‌شوند که این موضوع می‌تواند باعث افشای اطلاعات حساس گردد.
- **حریم خصوصی و جمع‌آوری داده‌ها:** بسیاری از دستگاه‌های اینترنت اشیاء به صورت مداوم داده‌ها را جمع‌آوری می‌کنند و این داده‌ها ممکن است بدون اطلاع و رضایت کاربران به اشتراک گذاشته شوند.
- **درجه بالای اتصالات:** با اتصال تعداد زیادی از دستگاه‌ها به یکدیگر، هر آسیب‌پذیری در یک دستگاه می‌تواند به نفوذ در سیستم‌های دیگر منجر شود. این شبکه اتصالات می‌تواند به سرعت

گسترش یابد و تهدیدات امنیتی را پیچیده‌تر کند.

- **عدم استانداردهای امنیتی:** در حال حاضر استانداردهای مشخص و جامعی برای امنیت در اینترنت اشیاء وجود ندارد. این موضوع می‌تواند منجر به استفاده از روش‌ها و پروتکل‌های امنیتی غیر مؤثر شود.

در برخی از اسناد آژانس امنیت ملی آمریکا که در بازه سال‌های ۲۰۱۳ تا ۲۰۱۵ میلادی افشا گردیده است، به موضوع مهمی اشاره شده که تلویحاً «اینترنت جدید»[1] نام دارد (Greenberg, 2013). پایگاه گلوبال ریسرچ در گزارشی با عنوان «جنگ سایبری آژانس امنیت ملی از دستگاه‌های متصل به اینترنت به عنوان بستر تسلیحاتی استفاده می‌کند» صراحتاً اشاره نمود: «آژانس امنیت ملی در جنگ سایبری از اینترنت اشیاء به عنوان یک پلتفرم تسلیحاتی استفاده می‌نماید؛ از این رو خانه‌های شما به نبردگاه تبدیل خواهد شد» (Global Research, 2015). جیمز کالپر، رئیس اطلاعات ملی آمریکا، اعلام کرد: «در آینده، سرویس‌های اطلاعاتی از بستر اینترنت اشیاء برای شناسایی، نظارت، مانیتورینگ، ردیابی مکانی و هدف‌یابی استفاده خواهند نمود» (Clapper, 2015). همچنین، در نشست ویژه‌ای با موضوع «کاربردهای نظامی مبتنی بر اینترنت اشیاء» در مورخ ۵ فوریه ۲۰۱۸ که توسط «انستیتو مهندسان برق و الکترونیک» برگزار شد، بیانیه‌ای انتشار یافت که در بخشی از آن آمده است: «عملیات‌های نظامی نوین در محیط‌های پیچیده، چندبعدی، بسیار پویا و مخرب انجام می‌شوند. گاهی اوقات هم با شرکای غیرمنتظره و دشمنان نامنظم. از این رو فرماندهان نظامی تحت فشار زیاد زمانی و ریتم عملیاتی بالا عمل می‌کنند. فرماندهان مجبور هستند در بازه‌های زمانی کوتاه‌تر برای حصول ارزیابی دقیق از وضعیت و همچنین ارزیابی دوره‌های بالقوه، تصمیم‌گیری و اقدام کنند. علاوه بر این، آن‌ها باید از تمام منابع احتمالی استفاده کنند تا اطمینان حاصل شود که اولاً تصویری کامل و مناسب‌تر از وضعیت در زمان کوتاه ایجاد شده و ثانیاً مفهوم تصمیمات و زمان اجرای آن‌ها به درستی درک گردیده است. یک راه برای پاسخ به چالش‌های فوق، ورود اینترنت اشیاء به حوزه نظامی است. اینترنت اشیاء ضمن توسعه گسترده در سراسر جهان، بر بخشی از کاربردهای غیرنظامی تمرکز نموده است که به حوزه نظامی کمک می‌کند» (Gope & Sikdar, 2019).

آمریکا که خود مبدع اینترنت اشیاء است و برنامه استفاده از آن برای مقاصد امنیتی و نظامی در جهان را رسماً اعلام نموده، با احتمال اینکه ممکن است دشمنان فرامرزی ایالات‌متحده بتوانند به

1. New Internet

شبکه‌های اینترنت اشیاء در این کشور نفوذ کرده و از این طریق تهدیداتی را ایجاد نمایند، در خصوص خطرات امنیتی این تکنولوژی راهبردی علیه امنیت ملی هشدار داده است. پایگاه خبری- تحلیلی هیل در گزارشی با عنوان «اینترنت اشیاء برای امنیت ملی، اینترنت مشکلات است» در خصوص تهدیدات ناشی از آن چنین اذعان می‌دارد: «نکته این است که امنیت ضعیف این تکنولوژی (اینترنت اشیاء) که اکثر آن از بیرون از مرزهای آمریکا نشأت می‌گیرد، بستری است برای شکل‌گیری تسلیحات سایبری با قابلیت تخریب وسیع که آمریکا را نشانه گرفته‌اند. عملکرد اینترنت اشیاء برای دشمنان اینگونه است که سنگ کوچک آن‌ها را به یک موشک تبدیل می‌کند» (Li & Zhao, 2015).

پ- تجزیه‌وتحلیل یافته‌ها

۱- اینترنت اشیاء در ایران

با مصوبه شورای عالی فضای مجازی تحت عنوان «الزامات حاکم بر اینترنت اشیاء در شبکه ملی اطلاعات» در تاریخ ۳۰ مهر ۱۳۹۷، اولین و یکی از مراحل اصلی سیاست‌گذاری در حوزه اینترنت اشیاء در کشور به حساب می‌آید. این مصوبه به‌منظور ایجاد یک چارچوب قانونی و فنی برای استفاده و توسعه اینترنت اشیاء در کشور به تصویب رسیده است و هدف آن بهبود امنیت، حریم خصوصی و کنترل بر داده‌های تولید شده توسط دستگاه‌های متصل به شبکه می‌باشد (بنار، ۱۳۹۹: ۲). با وجود اینکه مقطع زمانی توجه ایران به فناوری اینترنت اشیاء در بعد سیاست‌گذاری از بسیاری از کشورهای جهان پیشگام بود، اما در عمل تا به امروز گزارشی از اقدامات پیش‌بینی شده در مصوبه و اجرای آن منتشر نشده است. با این حال، افزایش تجهیزات مبتنی بر اینترنت اشیاء در ایران، در حوزه‌های مختلفی مانند صنایع، کشاورزی، بهداشت و حمل و نقل فرصت‌های زیادی را به همراه داشته است. این تجهیزات می‌توانند به بهبود مدیریت منابع، کاهش هزینه‌ها و افزایش بهره‌وری کمک کنند. برای مثال، در بخش کشاورزی، سنسورها و دستگاه‌های متصل به اینترنت می‌توانند شرایط خاک و هوا را به‌طور دقیق نظارت کرده و به کشاورزان کمک کنند تا با استفاده بهینه از منابع، محصولات بهتری برداشت کنند؛ اما با گسترش تجهیزات اینترنت اشیاء، مخاطرات امنیت سایبری نیز افزایش یافته‌اند. هر دستگاه متصل به شبکه می‌تواند یک نقطه ضعف بالقوه برای حملات سایبری باشد. حملات اختلال سرویس توزیع‌شده، نفوذ به شبکه‌های خصوصی و سرقت اطلاعات حساس تنها بخشی از

تهدیداتی هستند که می‌توانند توسط هکرها و بازیگران مخرب انجام شوند. این تهدیدات نه تنها امنیت اطلاعات را به خطر می‌اندازند، بلکه می‌توانند تأثیرات مخربی بر عملکرد سیستم‌ها و فرآیندهای حیاتی کشور داشته باشند (حسین‌زاده و رضایی، ۱۴۰۲: ۳). بی‌شک با افزایش آگاهی و اتخاذ تدابیر مناسب می‌توان از مزایای بی‌شمار اینترنت اشیاء بهره‌مند شد و در عین حال، از تهدیدات اجتماعی و سیاسی آن کاست.

۲- فرصت‌ها و چالش‌های توسعه اینترنت اشیاء بر امنیت اجتماعی ایران

۲-۱- فرصت‌های اجتماعی

توسعه اینترنت اشیاء در ایران می‌تواند تحولی اساسی در مدیریت امنیت اجتماعی ایجاد کرده و به کاهش آسیب‌های اجتماعی، بهبود کنترل بحران‌ها و افزایش تاب‌آوری اجتماعی کمک کند. این فناوری، از طریق جمع‌آوری و تحلیل داده‌های کلان، امکان پیش‌بینی و واکنش سریع‌تر به چالش‌های اجتماعی را فراهم کرده و به نهادهای مسئول در اتخاذ تصمیمات مؤثر یاری می‌رساند. در این بخش، مهم‌ترین فرصت‌های اینترنت اشیاء در بهبود امنیت اجتماعی ایران بررسی می‌شود:

۲-۱-۱- افزایش بهره‌وری و کاهش هزینه‌ها

توسعه اینترنت اشیاء در ایران می‌تواند تأثیر عمیقی بر افزایش بهره‌وری و کاهش هزینه‌ها در بخش‌های صنعتی، کشاورزی و خدماتی داشته باشد. با توجه به چالش‌های اقتصادی و محدودیت‌های منابع در کشور، استفاده از فناوری‌های هوشمند می‌تواند گامی مؤثر در راستای مدیریت بهینه منابع، کاهش هزینه‌های عملیاتی و ارتقای بهره‌وری باشد.

۲-۱-۲- بهینه‌سازی فرآیندهای صنعتی و تولیدی

کارخانه‌های ایرانی، به‌ویژه در صنایع خودروسازی، فولاد، پتروشیمی و نساجی، با مشکلات متعددی همچون فرسودگی تجهیزات، اتلاف انرژی و هزینه‌های بالای تعمیر و نگهداری روبه‌رو هستند. اینترنت اشیاء از طریق نظارت لحظه‌ای بر عملکرد ماشین‌آلات، می‌تواند با ارسال داده‌های دقیق به سیستم‌های کنترلی، از خرابی‌های ناگهانی جلوگیری کند. این امر نه‌تنها هزینه‌های تعمیرات را کاهش می‌دهد، بلکه از توقف خط تولید و کاهش بهره‌وری نیز جلوگیری می‌کند. برای مثال، در

صنایع فولاد ایران، استفاده از حسگرهای هوشمند در کنترل دمای کوره‌ها می‌تواند به کاهش مصرف انرژی و افزایش بازدهی تولید کمک کند (اعتدادی، ۱٤۰۳).

۲-۱-۳- بهینه‌سازی مصرف منابع در کشاورزی ایران

ایران با چالش کمبود منابع آبی مواجه است و کشاورزی سنتی سهم قابل‌توجهی از مصرف آب را به خود اختصاص داده است. اینترنت اشیاء از طریق سنجش خودکار رطوبت خاک، دما و میزان تابش خورشید می‌تواند به مدیریت بهینه آبیاری و مصرف کودهای شیمیایی کمک کند. برای مثال، در استان‌های اصفهان و خراسان که با بحران کم‌آبی مواجه‌اند، استفاده از سامانه‌های آبیاری هوشمند مبتنی بر اینترنت اشیاء می‌تواند تا ٤۰ درصد در مصرف آب صرفه‌جویی کند (رهبانی، ۱۳۹۹: ٤۲). علاوه بر این، مدیریت هوشمند گلخانه‌ها در شهرهایی مانند محلات و یزد موجب افزایش تولید و کاهش هزینه‌های انرژی شده است.

۲-۱-٤- بهبود کیفیت زندگی و رفاه عمومی

توسعه اینترنت اشیاء در ایران می‌تواند نقش بسزایی در ارتقای کیفیت زندگی و رفاه عمومی ایفا کند. این فناوری با ایجاد امکانات هوشمند در حوزه سلامت، مسکن، مدیریت شهری و انرژی می‌تواند زندگی شهروندان را راحت‌تر، ایمن‌تر و مقرون‌به‌صرفه‌تر سازد. با توجه به چالش‌های موجود در زیرساخت‌های بهداشتی، مصرف بالای انرژی و مشکلات زیست‌محیطی در ایران، بهره‌گیری از اینترنت اشیاء می‌تواند تحولات اساسی در بهبود شرایط زندگی ایجاد کند.

سیستم بهداشت و درمان ایران با چالش‌هایی همچون تراکم بیماران در بیمارستان‌ها، کمبود نیروی متخصص در مناطق محروم و هزینه‌های بالای درمان روبه‌رو است. اینترنت اشیاء با ارائه دستگاه‌های پوشیدنی هوشمند، امکان پایش لحظه‌ای علائم حیاتی بیماران را فراهم می‌کند. این دستگاه‌ها می‌توانند داده‌های مربوط به فشارخون، قند خون و ضربان قلب را به پزشکان ارسال کنند و در صورت مشاهده علائم هشداردهنده، امکان مداخله زودهنگام را فراهم نمایند. برای مثال، در مناطق محروم ایران که دسترسی به پزشکان متخصص محدود است، استفاده از سیستم‌های پایش از راه دور مبتنی بر اینترنت اشیاء می‌تواند به بهبود مراقبت‌های پزشکی و کاهش هزینه‌های بیمارستانی منجر شود (فعله کری، – ۱٤۰۰: ٤–۵). همچنین، این فناوری می‌تواند در مدیریت بیماری‌های مزمن مانند دیابت و بیماری‌های قلبی که در ایران شیوع بالایی دارند، مؤثر باشد.

۲-۱-۵- تحول در حوزه نظامی

اینترنت اشیاء در حوزه نظامی، با ایجاد سیستم‌های هوشمند و خودکارسازی فرآیندهای دفاعی و امنیتی، تحولات چشمگیری را در افزایش توانمندی نیروهای مسلح، بهینه‌سازی عملیات و کاهش هزینه‌های دفاعی ایجاد کرده است. ایران به عنوان کشوری با موقعیت ژئوپلیتیکی حساس و تهدیدات متنوع، می‌تواند با بهره‌گیری از این فناوری، امنیت ملی را تقویت کرده و قابلیت‌های دفاعی خود را ارتقا دهد. در این راستا، کاربردهای کلیدی اینترنت اشیاء در حوزه نظامی ایران را می‌توان در محورهای زیر بررسی کرد:

- به‌روزرسانی جنگ‌افزارها؛
- جمع‌آوری و تجزیه‌وتحلیل داده‌ها؛
- خودکار سازی تجهیزات؛
- شناسایی و نظارت بر نیروها؛
- کنترل و مانیتورینگ جنگ‌افزارها؛
- امنیت و حفاظ؛
- پیش‌بینی و آماده‌سازی برای تهدیدات.

۲-۱-٦- تحول در صنایع

فناوری اینترنت اشیاء به‌عنوان یکی از پیشرفته‌ترین نوآوری‌ها در دنیای امروزی، ظرفیت بالایی برای تحول در صنایع مختلف ایران دارد. این فناوری با ایجاد ارتباط میان دستگاه‌ها، ماشین‌آلات و سیستم‌ها، قادر است فرآیندها را بهینه‌سازی کرده، بهره‌وری را افزایش دهد و هزینه‌ها را کاهش دهد. در ایران، با توجه به چالش‌های اقتصادی و صنعتی موجود، بهره‌برداری از اینترنت اشیاء در صنایع مختلف می‌تواند تحول چشمگیری ایجاد کند.

صنعت حمل و نقل ایران از جمله صنایعی است که می‌تواند از فناوری اینترنت اشیاء به طور گسترده بهره‌برداری کند. در این حوزه، استفاده از خودروهای متصل به اینترنت می‌تواند به بهبود مدیریت ترافیک، کاهش تصادفات و مصرف سوخت کمک کند. خودروهای متصل با زیرساخت‌های جاده‌ای و سایر خودروها در ارتباط بوده و به‌طور هوشمند مسیرها را بهینه‌سازی می‌کنند. به‌طور مثال، سامانه‌های مدیریت هوشمند ترافیک در تهران از دستگاه‌های حسگر و دوربین‌های هوشمند برای

کنترل وضعیت ترافیکی و پیشنهاد مسیرهای مناسب استفاده می‌کنند (میرزائی و همتی، ۱٤۰۲). در صنعت نفت و گاز که به عنوان یکی از ارکان اصلی اقتصاد ایران شناخته می‌شود، اینترنت اشیاء می‌تواند نقش بسزایی در پایش مستمر تجهیزات ایفا کند. سنسورهای هوشمند می‌توانند به طور مداوم وضعیت تجهیزات استخراج و پالایش را نظارت کرده و از خرابی‌ها و مشکلات غیرمنتظره جلوگیری کنند. این فناوری همچنین به افزایش ایمنی در میادین نفتی کمک می‌کند. شرکت‌های نفت و گاز ایران با استفاده از سنسورهای هوشمند برای نظارت بر وضعیت خطوط انتقال نفت، توانسته‌اند کارایی عملیات خود را بهبود بخشند (مهرآبادی، ۱٤۰۲).

۲-۱-۷- توسعه شهرهای هوشمند

اینترنت اشیاء به عنوان یکی از ارکان اصلی شهرهای هوشمند، می‌تواند زیرساخت‌های شهری را متحول کرده و کیفیت زندگی شهروندان را بهبود بخشد. با توجه به چالش‌های کلان‌شهرهای ایران، از جمله ترافیک سنگین، آلودگی هوا، ناکارآمدی سیستم‌های مدیریت شهری و افزایش هزینه‌های خدمات عمومی، بهره‌گیری از فناوری‌های هوشمند برای مدیریت بهینه این چالش‌ها ضرورتی اجتناب‌ناپذیر است. یکی از مهم‌ترین کاربردهای اینترنت اشیاء در شهرهای هوشمند، مدیریت هوشمند ترافیک است. سیستم‌های کنترل ترافیک مبتنی بر اینترنت اشیاء می‌توانند از طریق دوربین‌های هوشمند و حسگرهای جاده‌ای، وضعیت ترافیک را در لحظه پایش کرده و مسیرهای جایگزین را به رانندگان پیشنهاد دهند. این امر می‌تواند باعث کاهش ازدحام و کاهش میزان آلاینده‌های زیست‌محیطی در کلان‌شهرهایی مانند تهران و مشهد شود. نظارت بر کیفیت هوا از دیگر مزایای مهم شهرهای هوشمند مبتنی بر اینترنت اشیاء است. در شهرهای آلوده‌ای مانند تهران، سنسورهای اینترنت اشیاء می‌توانند داده‌های مربوط به کیفیت هوا را در زمان واقعی پایش کرده و اطلاعات دقیق را در اختیار مسئولان شهری قرار دهند تا اقدامات لازم، مانند محدودیت‌های تردد یا افزایش پوشش فضای سبز، اتخاذ شود.

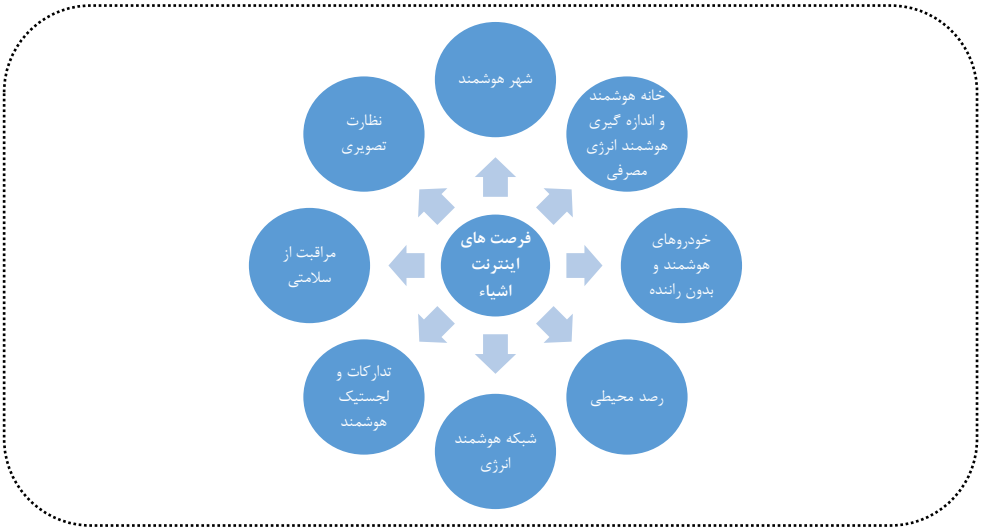
۲-۱-۸- ایجاد فرصت‌های شغلی جدید

توسعه فناوری اینترنت اشیاء در ایران می‌تواند به ایجاد فرصت‌های شغلی جدید در بخش‌های مختلف اقتصادی منجر شود. این فناوری نیازمند تخصص‌های نوظهوری مانند مهندسی داده، هوش مصنوعی، امنیت سایبری و مدیریت سیستم‌های هوشمند است که در سال‌های اخیر اهمیت بیشتری

یافته‌اند. با گسترش این فناوری، بازار کار ایران شاهد افزایش تقاضا برای نیروی متخصص در این حوزه‌ها خواهد بود. یکی از مهم‌ترین اثرات توسعه اینترنت اشیاء، افزایش اشتغال در بخش فناوری اطلاعات و ارتباطات است. شرکت‌های فناوری‌محور می‌توانند از فرصت‌های ایجاد شده بهره‌برداری کرده و در زمینه‌های مرتبط با اینترنت اشیاء، از جمله توسعه نرم‌افزارهای هوشمند، تحلیل داده‌های بزرگ و طراحی سیستم‌های امنیت سایبری، سرمایه‌گذاری کنند. این امر می‌تواند به رونق صنعت فناوری اطلاعات در ایران و افزایش اشتغال پایدار منجر شود (قربانی، ۱۴۰۲: ۱۱۵).

۲-۱-۹- بهبود مدیریت منابع و محیط‌زیست

اینترنت اشیاء در بخش محیط‌زیست نیز تحول‌آفرین است. این فناوری می‌تواند به مدیریت بهتر منابع طبیعی و حفاظت از محیط زیست کمک کند. در مدیریت منابع آب، سنسورها و سیستم‌های هوشمند می‌توانند به بهینه‌سازی مصرف آب و کاهش هدر رفت آن کمک کنند. در کشاورزی، سیستم‌های هوشمند می‌توانند مصرف آب و مواد شیمیایی را بهینه کنند و به حفظ محیط‌زیست کمک کنند. همان‌طور که پیش‌تر ذکر شد، سیستم‌های نظارت بر کیفیت هوا و آب نیز می‌توانند به کاهش آلودگی و حفظ سلامت عمومی کمک کنند. به این ترتیب، اینترنت اشیاء می‌تواند نقش مهمی در حفاظت از محیط‌زیست و مدیریت پایدار منابع ایفا کند. به طور خلاصه، فرصت‌های توسعه اینترنت اشیاء در شکل زیر نشان داده شده است.



شکل شماره ٤- فرصت‌های توسعه اینترنت اشیاء

(منبع: محقق ساخته)

۲-۲- چالش‌های اجتماعی

فناوری‌های نوین دیجیتال، از جمله اینترنت اشیاء، با ایجاد شبکه‌های هوشمند و داده‌محور، تحولات شگرفی در زندگی اجتماعی، اقتصادی و امنیتی ایجاد کرده‌اند؛ اما همان‌گونه که این فناوری‌ها می‌توانند بهبود کیفیت زندگی و افزایش بهره‌وری را به دنبال داشته باشند، در صورت عدم مدیریت صحیح، می‌توانند تهدیدات و چالش‌های عمیقی را برای امنیت اجتماعی کشورها به وجود آورند. در ایران، توسعه اینترنت اشیا به دلیل ضعف زیرساخت‌های قانونی، خلأهای امنیتی و کمبود آگاهی عمومی، می‌تواند پیامدهای اجتماعی متعددی را به همراه داشته باشد. برخلاف تصور رایج، تهدیدات اجتماعی ناشی از اینترنت اشیا بیشتر به مدیریت نادرست، ضعف در تنظیم‌گری و عدم تدوین سیاست‌های حفاظتی مناسب بازمی‌گردد تا ذات خود فناوری. ازاین‌رو، مسئله اصلی، طراحی و اجرای سیاست‌های مؤثر برای کاهش مخاطرات امنیتی و اجتماعی است.

۲-۲-۱- حملات اختلال سرویس توزیع شده

توسعه اینترنت اشیاء در ایران، در کنار مزایای متعدد، چالش‌های امنیتی و اجتماعی قابل‌توجهی را نیز به همراه دارد که یکی از مهم‌ترین آن‌ها، «حملات اختلال سرویس توزیع‌شده»[1] است. اینترنت اشیاء شامل مجموعه‌ای از فناوری‌های متنوع نظیر شبکه‌های حسگر بی‌سیم، رایانش ابری و مجازی‌سازی است که هر یک دارای نقاط ضعف خاص خود هستند. در چنین محیطی، امنیت کل سیستم وابسته به ضعیف‌ترین حلقه زنجیره است که در امنیت سایبری به‌عنوان «پاشنه آشیل» شناخته می‌شود. یک نقص امنیتی کوچک در یکی از این بخش‌ها می‌تواند کل سیستم را در معرض تهدیدات گسترده قرار دهد.

حملات اختلال سرویس توزیع‌شده یکی از جدی‌ترین تهدیدات برای امنیت اجتماعی ایران در بستر اینترنت اشیاء محسوب می‌شوند. در این حملات، مهاجمان از هزاران یا حتی میلیون‌ها دستگاه متصل به اینترنت برای ارسال حجم عظیمی از درخواست‌ها به سمت سرورها و زیرساخت‌های حیاتی استفاده می‌کنند که منجر به اختلال یا از دسترس خارج شدن آن‌ها می‌شود. چنین حملاتی می‌توانند صنایع حیاتی، از جمله سیستم‌های بانکی، بهداشت و درمان، نیروگاه‌ها و حمل‌ونقل عمومی را هدف قرار دهند و باعث ایجاد نارضایتی عمومی و حتی بحران‌های اجتماعی شوند. نمونه‌هایی از

1. Distributed service disruption attacks

این حملات در کشورهای مختلف، از جمله حمله سایبری سال ۲۰۲۰ به سیستم حمل‌ونقل اسرائیل، نشان داده است که زیرساخت‌های مبتنی بر اینترنت اشیاء می‌توانند به‌راحتی هدف قرار گیرند. (Chen et al, 2021).

در ایران، با گسترش وابستگی سیستم‌های ریلی، مترو و حمل‌ونقل عمومی به فناوری‌های متصل، خطر حملات اختلال سرویس توزیع‌شده افزایش یافته است. در سال‌های اخیر، نمونه‌هایی از اختلالات سایبری در برخی زیرساخت‌های کشور گزارش شده که نشان‌دهنده آسیب‌پذیری بالای این سیستم‌ها در برابر تهدیدات سایبری است. به‌عنوان‌مثال، در سال ۲۰۲۱، حمله‌ای به سامانه فروش بلیت قطارهای ایران منجر به اخلال در خدمات مسافری شد که نشان‌دهنده ضرورت تقویت تدابیر امنیتی در این حوزه است.

۲-۲-۲- نفوذ به شبکه‌های خصوصی

نفوذ به شبکه‌های خصوصی یکی دیگر از چالش‌های اساسی توسعه اینترنت اشیاء بر امنیت اجتماعی در ایران محسوب می‌شود. اینترنت اشیاء در حوزه‌های متعددی از جمله سلامت الکترونیکی، خانه‌های هوشمند، صنایع و شهرهای هوشمند کاربرد دارد که هر یک از این حوزه‌ها الزامات امنیتی خاص خود را دارند. با این حال، تنوع در کاربردها و نبود استانداردهای یکپارچه امنیتی موجب شده تا برخی از این حوزه‌ها بیش از سایرین در معرض تهدیدات امنیتی قرار گیرند.

یکی از مهم‌ترین تهدیدات در این زمینه، نفوذ غیرمجاز هکرها به شبکه‌های خصوصی از طریق دستگاه‌های متصل به اینترنت اشیاء است. بسیاری از این دستگاه‌ها به شبکه‌های داخلی کاربران متصل می‌شوند و در صورت ضعف در تدابیر امنیتی، می‌توانند به مسیری برای ورود هکرها و عاملان مخرب تبدیل شوند. این نفوذها می‌توانند به سرقت اطلاعات حساس از جمله داده‌های شخصی و مالی کاربران، نظارت غیرمجاز بر فعالیت‌های آن‌ها و حتی کنترل از راه دور دستگاه‌های متصل منجر شوند. چنین شرایطی نه‌تنها حریم خصوصی شهروندان را تهدید می‌کند، بلکه باعث ایجاد ناامنی روانی و اجتماعی می‌شود (Li & Zhao, 2021).

در ایران، با افزایش استفاده از فناوری‌های هوشمند در منازل، سازمان‌ها و زیرساخت‌های حیاتی، این تهدیدات اهمیت بیشتری پیدا کرده‌اند. بسیاری از دستگاه‌های اینترنت اشیاء مورد استفاده در کشور، به دلیل نبود قوانین و استانداردهای امنیتی مشخص، در برابر حملات سایبری آسیب‌پذیر هستند. به‌عنوان‌مثال، مطالعات نشان داده‌اند که تعداد زیادی از دوربین‌های مداربسته و دستگاه‌های

خانه‌های هوشمند در ایران به‌راحتی قابل هک شدن هستند و می‌توانند به‌عنوان ابزاری برای جاسوسی و نظارت غیرمجاز مورد استفاده قرار گیرند.

۲-۲-۳- محدودیت‌های منبع و به‌روزرسانی

یکی دیگر از چالش‌های اساسی اینترنت اشیاء در ایران، محدودیت‌های منبع و به‌روزرسانی امنیتی دستگاه‌های متصل است. اکثر دستگاه‌های اینترنت اشیاء دارای منابع سخت‌افزاری و نرم‌افزاری محدودی از جمله فضای ذخیره‌سازی، توان پردازشی و انرژی باتری هستند. این محدودیت‌ها باعث می‌شود که این دستگاه‌ها به‌راحتی در معرض حملات سایبری، به‌ویژه حملات عدم پذیرش سرویس قرار گیرند. در این نوع حملات، مهاجمان با ارسال درخواست‌های بیش‌ازحد به دستگاه‌ها، منابع محدود آن‌ها را به‌طور کامل اشغال کرده و موجب اختلال در عملکردشان می‌شوند. این موضوع می‌تواند در مقیاس گسترده‌تری بر زیرساخت‌های حیاتی، خدمات شهری هوشمند و امنیت اجتماعی تأثیر منفی بگذارد (زرافشان و شیربندی، ۱٤۰۰: ۳۰). یکی دیگر از چالش‌های امنیتی مهم، ضعف در به‌روزرسانی مداوم نرم‌افزارهای دستگاه‌های متصل است. بسیاری از این دستگاه‌ها پس از ورود به بازار، به‌طور منظم به‌روزرسانی‌های امنیتی دریافت نمی‌کنند یا مکانیزم‌هایی برای نصب خودکار این به‌روزرسانی‌ها ندارند. این امر باعث می‌شود که هکرها بتوانند از آسیب‌پذیری‌های شناخته‌شده سوءاستفاده کرده و به شبکه‌های متصل نفوذ کنند. برای مثال، در ایران بسیاری از دستگاه‌های اینترنت اشیاء در حوزه‌های نظارت تصویری و خانه‌های هوشمند از نرم‌افزارهای قدیمی استفاده می‌کنند که در برابر حملات سایبری آسیب‌پذیرند. بررسی‌های اخیر نشان داده‌اند که درصد بالایی از دستگاه‌های متصل در کشور به‌دلیل ضعف در به‌روزرسانی‌های امنیتی، در معرض نفوذ غیرمجاز قرار دارند.

۲-۲-٤- حملات سایبری به زیرساخت‌های حیاتی

ایران به‌شدت به زیرساخت‌های حیاتی مانند برق، آب، گاز و ارتباطات وابسته است که بسیاری از آن‌ها با فناوری‌های اینترنت اشیاء مدیریت و کنترل می‌شوند. هرگونه حمله سایبری به این زیرساخت‌ها می‌تواند پیامدهای گسترده‌ای بر امنیت اجتماعی و ملی کشور داشته باشد. با دیجیتالی شدن مدیریت شبکه‌های برق، گاز و سایر زیرساخت‌های حیاتی، تهدیدات مشابهی می‌تواند امنیت ملی را با چالش‌های جدی مواجه کند. به‌ویژه در شرایط بحرانی منطقه‌ای یا در صورت وقوع جنگ سایبری، حملات سایبری به این زیرساخت‌ها می‌تواند موجب اختلالات گسترده در ارائه خدمات

عمومی و ایجاد ناآرامی‌های اجتماعی شود. علاوه بر این، بررسی‌های اخیر نشان داده‌اند کـه برخـی از سامانه‌های صنعتی و زیرساخت‌های حیاتی کشور به دلیل استفاده از نرم‌افزارهای قدیمی و ضـعف در تدابیر امنیتی، در برابر حملات سایبری آسیب‌پذیر هستند (رحمتی لارهنگ و همکاران، ۱۴۰۱: ۹۷).

۲-۲-۵- اختلال داده‌ها در مکان‌های دورافتاده

در بسیاری از کاربردهای اینترنت اشیا، به ویژه در زمینه‌هایی چون شـبکه‌هـای هوشـمند، خطـوط ریلی و حاشیه‌های جاده‌ها، دستگاه‌های اینترنت اشـیا (اغلـب حسـگرها) در مکـان‌هـای دورافتـاده و غیرقابل‌دسترس برای انسان نصب می‌شوند. این وضعیت باعث می‌شود که این دستگاه‌ها به راحتی در معرض خطر قرار گیرند، زیرا مهاجمان می‌توانند بدون اینکه دیده شوند، به ایـن تجهیـزات دسترسـی پیدا کرده و آن‌ها را مختل کنند. این قبیل سناریوها چالش‌های امنیتی خاصی را به همـراه دارنـد؛ زیـرا عدم دسترسی انسانی به این دستگاه‌ها، امکان نظارت و نگهداری منظم را دشوار می‌سـازد. بـه همـین دلیل، نیاز به پیاده‌سازی راهکارهای امنیتی قوی، مانند احراز هویت، رمزنگاری و سیستم‌های تشخیص نفوذ برای حفاظت از این دستگاه‌ها از اهمیت بالایی برخـوردار اسـت (زرافشـان و شـیربندی، ۱۴۰۰: ۲۸). همچنین، طراحی مکانیزم‌های واکنش خودکار به تهدیدات نیز می‌توانـد بـه کـاهش آسـیب‌هـا و حفظ امنیت سیستم کمک کنـد. از سـوی دیگـر، اسـتفاده از رمزنگـاری ضـعیف یـا عـدم اسـتفاده از رمزنگاری در انتقال داده‌ها نیز یک خطر جدی است. در بسیاری از دستگاه‌های اینترنت اشـیاء داده‌هـا بدون هیچ‌گونه رمزنگاری از طریق شبکه‌ها منتقل می‌شوند. امری که به هکرها اجازه مـی‌دهـد تـا بـه راحتی این داده‌ها را رهگیری و به آن‌ها دسترسی پیـدا کننـد. حملـۀ «اسـتاکس نـت»[1] بـه تأسیسـات هسته‌ای ایران نمونه‌ای از آسیب‌پذیری سیستم‌های متصل به فناوری است.

۲-۲-۶- نقض حریم خصوصی

یکی از ابعاد امنیتی اساسی در اینترنت اشیاء، حریم خصوصی است که اهمیت ویژه‌ای دارد. عـدم تضمین حریم خصوصی می‌تواند منجر به عدم پذیرش این سیستم‌ها و خدمات توسط عموم مـردم و نهادهای مختلف شود که این امر در نهایت به شکست اهداف کلی اینترنت اشیاء می‌انجامد. بـه دلیـل افزایش حجم داده‌های جمع‌آوری شده در اینترنت اشیاء نسـبت بـه اینترنـت معمـولی، مسـئله حـریم خصوصی در این زمینه اهمیت بیشتری پیدا می‌کند. این امر خطر افشای اطلاعات شخصـی را نیـز بـه

1. Stuxnet

طور قابل‌توجهی افزایش می‌دهد. برای مثال، در سال ۲۰۲۱ نگران‌هایی درباره استفاده از دوربین‌های نظارتی هوشمند در چین برای نظارت بر شهروندان مطرح شد. در ایران نیز ممکن است اینترنت اشیاء برای جمع‌آوری داده‌های حساس به کار رود که این امر می‌تواند امنیت ملی را تهدید کند.

۳- راهکارهای پیشنهادی برای کاهش مخاطرات اجتماعی اینترنت اشیاء

سیاست‌گذاران باید قوانین و مقررات جامعی را برای تضمین امنیت دستگاه‌های اینترنت اشیاء تدوین و اجرا نمایند. این مقررات می‌توانند شامل الزام به استفاده از پروتکل‌های امنیتی پیشرفته، رمزنگاری داده‌ها و به‌روزرسانی منظم نرم‌افزارها باشند. علاوه بر این، تعیین استانداردهای مشخص برای تولیدکنندگان و ارائه‌دهندگان خدمات اینترنت اشیاء می‌تواند به تقویت امنیت کمک کند. با وجود این که شورای عالی فضای مجازی در سال ۱۳۹۷ «الزامات حاکم بر اینترنت اشیاء در شبکه ملی اطلاعات» را تصویب و ابلاغ کرده است، اما تحولات سریع این حوزه در سال‌های اخیر نیاز به بازنگری و به‌روزرسانی این سیاست‌ها را به امری ضروری تبدیل کرده است.

۳-۱- پیشنهاداتی برای سیاست‌گذاران

۳-۱-۱- وضع قوانین و مقررات جامع امنیتی

سیاست‌گذاران باید قوانین و مقررات جامعی را برای تضمین امنیت دستگاه‌های اینترنت اشیاء تدوین و اجرا نمایند. این مقررات می‌توانند شامل الزام به استفاده از پروتکل‌های امنیتی پیشرفته، رمزنگاری داده‌ها و به‌روزرسانی منظم نرم‌افزارها باشند. علاوه بر این، تعیین استانداردهای مشخص برای تولیدکنندگان و ارائه‌دهندگان خدمات اینترنت اشیاء می‌تواند به تقویت امنیت کمک کند. با وجود این که شورای عالی فضای مجازی در سال ۱۳۹۷ «الزامات حاکم بر اینترنت اشیاء در شبکه ملی اطلاعات» را تصویب و ابلاغ کرده است، اما تحولات سریع این حوزه در سال‌های اخیر نیاز به بازنگری و به‌روزرسانی این سیاست‌ها را به امری ضروری تبدیل کرده است.

۳-۱-۲- حمایت از تحقیقات و نوآوری در امنیت سایبری

سیاست‌گذاران می‌توانند با تخصیص بودجه و منابع لازم، از تحقیقات و نوآوری در حوزه امنیت سایبری حمایت کنند. این امر می‌تواند به توسعه فناوری‌های جدید و کارآمد برای مقابله با تهدیدات

امنیتی اینترنت اشیاء منجر شود. ایجاد مراکز تحقیقاتی و دانشگاهی متمرکز بر امنیت سایبری و اینترنت اشیاء نیز می‌تواند به تقویت این حوزه کمک کند.

۳-۱-۳- افزایش آگاهی عمومی

برگزاری کمپین‌های آگاهی بخشی و آموزش عمومی درباره مخاطرات امنیتی اینترنت اشیاء و راه‌های پیشگیری از آن‌ها می‌تواند به افزایش دانش و آگاهی کاربران و کسب‌وکارها کمک کند. سیاست‌گذاران می‌توانند با همکاری نهادهای آموزشی و رسانه‌ها، این آموزش‌ها را به‌طور گسترده ارائه دهند.

۳-۲- پیشنهاداتی برای ارائه‌دهندگان خدمات

۳-۲-۱- تضمین به‌روزرسانی منظم نرم‌افزارها

ارائه‌دهندگان خدمات و تولیدکنندگان دستگاه‌های اینترنت اشیاء باید به‌روزرسانی‌های منظم نرم‌افزاری و امنیتی را برای محصولات خود ارائه دهند. این به‌روزرسانی‌ها باید شامل رفع آسیب‌پذیری‌های شناخته شده و بهبودهای امنیتی باشند. همچنین، ایجاد مکانیزم‌های خودکار برای به‌روزرسانی دستگاه‌ها می‌تواند به افزایش امنیت تجهیزات مذکور کمک کند.

۳-۲-۲- پیاده‌سازی پروتکل‌های امنیتی قوی

استفاده از پروتکل‌های امنیتی قوی برای انتقال داده‌ها و ارتباطات بین دستگاه‌ها نیز امری ضروری است. رمزنگاری داده‌ها، استفاده از گواهینامه‌های امنیتی معتبر و احراز هویت چند مرحله‌ای، از جمله اقداماتی هستند که می‌توانند به افزایش امنیت کمک کنند و باید از سوی ارائه‌دهندگان خدمات این حوزه مورد توجه قرار گیرند.

۳-۲-۳- ارائه آموزش‌های امنیتی به کاربران

ارائه دهندگان خدمات همچنین باید آموزش‌های لازم را به کاربران خود ارائه دهند تا آن‌ها با مخاطرات امنیتی موجود آشنا شوند و بدانند چگونه از دستگاه‌های خود به صورت امن استفاده کنند. این آموزش‌ها می‌توانند شامل دستورالعمل‌های ساده و قابل فهم برای تنظیمات امنیتی و به‌روزرسانی‌ها باشند.

۳-۳- پیشنهاداتی برای کاربران

۳-۳-۱- استفاده از رمزهای عبور قوی و منحصر به فرد

کاربران باید برای دستگاه‌های اینترنت اشیا خود از رمزهای عبور قوی و منحصر به فرد استفاده کنند. استفاده از رمزهای عبور پیچیده و تغییر منظم آن‌ها می‌تواند به افزایش امنیت کمک کند. همچنین، اجتناب از استفاده رمزهای عبور پیش‌فرض که به راحتی قابل حدس زدن هستند، برای کاربران بسیار حیاتی است.

۳-۳-۲- به‌روزرسانی منظم دستگاه‌ها

کاربران باید به‌روزرسانی‌های امنیتی و نرم‌افزاری دستگاه‌های خود را به طور منظم انجام دهند. بسیاری از تولیدکنندگان به‌روزرسانی‌هایی را برای رفع آسیب‌پذیری‌ها ارائه می‌دهند و کاربران باید اطمینان حاصل کنند که دستگاه‌هایشان همواره به‌روز و آماده مقابله با تهدیدات هستند.

۳-۳-۳- استفاده از شبکه‌های امن

کاربران باید از شبکه‌های امن و رمزنگاری شده برای اتصال دستگاه‌های اینترنت اشیا خود استفاده کنند. اجتناب از اتصال به شبکه های عمومی و ناشناس و استفاده از شبکه‌های خانگی حفاظت شده با رمز عبور قوی، می‌تواند به افزایش امنیت کمک کند.

نتیجه‌گیری

فناوری اینترنت اشیاء، به‌عنوان یکی از پیشرفت‌های تحول‌آفرین قرن بیست و یکم، ظرفیت بالایی برای تغییرات اساسی در بخش‌های مختلف اقتصادی، اجتماعی و صنعتی کشورها دارد. در ایران، این فناوری می‌تواند به‌طور قابل توجهی در بهبود کیفیت زندگی، ارتقاء بهره‌وری و کاهش هزینه‌ها در حوزه‌های مختلف مانند بهداشت، کشاورزی، صنعت و حمل‌ونقل تأثیرگذار باشد. توانمندی‌های اینترنت اشیاء در اتصال دستگاه‌ها و تجزیه‌وتحلیل داده‌ها، فرصت‌هایی را برای بهینه‌سازی فرآیندها و مدیریت هوشمند فرآیندها فراهم می‌آورد. با این حال، در کنار فرصت‌های عظیم این فناوری، چالش‌های قابل توجهی در زمینه امنیت اجتماعی کشور به‌ویژه در حوزه‌های امنیت سایبری و حفظ حریم خصوصی وجود دارد. تهدیدات ناشی از نفوذ غیرمجاز به شبکه‌های متصل، دسترسی به

اطلاعات حساس و آسیب‌پذیری‌های موجود در دستگاه‌های اینترنت اشیاء می‌تواند موجب بروز مشکلات جدی در حفظ امنیت اجتماعی شود. از این رو، نیاز به رویکردهای امنیتی جامع و تدابیر پیشگیرانه برای جلوگیری از تهدیدات سایبری در برابر زیرساخت‌های حیاتی کشور امری ضروری است. در ایران، با گسترش استفاده از اینترنت اشیاء در حوزه‌های مختلف، زندگی اجتماعی و فرهنگی کشور شاهد تحولات بنیادینی خواهد بود. این تحولات می‌تواند باعث تحول در الگوهای اجتماعی، شیوه‌های ارتباطی و حتی مدیریت منابع شهری و دولتی شود. در این راستا، توسعه و تقویت زیرساخت‌های امنیتی برای حفظ حریم خصوصی و امنیت اجتماعی امری حیاتی است. نظارت و مدیریت هوشمند منابع شهری و دولتی می‌تواند به بهبود عملکرد سیستم‌های دولتی و ارتقاء کیفیت خدمات عمومی منجر شود، ولی در عین حال چالش‌های نظارتی و امنیتی جدیدی به‌وجود خواهد آورد. برای بهره‌برداری ایمن و مؤثر از این فناوری، ایران نیازمند تدوین سیاست‌های امنیتی مناسب و همکاری مستمر بین سیاست‌گذاران، ارائه‌دهندگان خدمات و کاربران است. آگاهی‌بخشی در زمینه امنیت، اجرای پروتکل‌های امنیتی معتبر و تقویت سیاست‌های دسترسی، می‌تواند کمک کند تا از این فناوری به‌طور امن بهره‌برداری شود و چالش‌های اجتماعی و سیاسی ناشی از آن به حداقل برسد.

منابع

الف- منابع فارسی

- اعتدادی، حسین (۱۴۰۳)، «*بهینه‌سازی مصرف انرژی دستگاه‌های اینترنت اشیاء در شبکه‌های نسل پنجم*»، بیست و سومین کنفرانس ملی مهندسی برق، کامپیوتر و مکانیک.
- بنار، محسن (۱۳۹۹)، «اینترنت اشیاء: چارچوب مقررات‌گذاری، امنیت سایبری و مقررات‌گذاری داده در اینترنت اشیاء برای ایران»، مرکز پژوهش‌های مجلس شورای اسلامی، شماره ۱۷۰۱۲.
- حسین‌زاده، مرضیه و رضائی، علیرضا (۱۴۰۲)، «امنیت سایبری در حوزه اینترنت اشیاء»، *فصلنامه تخصصی آرمان پردازش*، سال ۴، شماره ۱. 10.22034/apj.2023.706757
- دژگیر، حمید، و هوشمند، هانیه (۱۳۹۶)، «مروری بر امنیت در اینترنت اشیا»، همایش ملی پژوهش‌های نوین در علوم و فناوری.

- رحمتی لارهنگ، رضا و همکاران (۱۴۰۱)، «ارائه الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی جمهوری اسلامی ایران»، *فصلنامه مطالعات راهبردی فضای سایبر*، سال ۱، شماره ۳.
https://ssc.sndu.ac.ir/article_2554.html
- رهبانی، محمد صادق (۱۳۹۹)، «کاربرد اینترنت اشیاء در کشاورزی هوشمند»، *نشریه علمی-ترویجی صنعت سبز نوین*، سال ۵، شماره ۲.
- زرافشان، فرزانه و شیربندی، رامین. (۱۴۰۰)، «بررسی حملات و راهکارهای امنیت اینترنت اشیاء»، *دوفصلنامه محاسبات و سامانه‌های توزیع شده*، سال ۴، شماره ۱.
https://www.jdcs.ir/article_191108.html
- شفیعی، ساناز (۱۳۹۴)، «تحلیل چالش‌های فراروی توسعه فناوری اینترنت اشیاء: تهدیدات امنیتی و شکاف دیجیتالی»، *ماهنامه نوشتار کوتاه*، سال ۱، شماره ۷.
- صالحی، سید جواد، فرج زاده، ایوب فرج زاده و فرح بخش، عباس (۱۳۹۱)، «بررسی نقش اینترنت در جنبش اجتماعی مصر»، *جامعه‌شناسی سیاسی جهان اسلام*، سال ۱ شماره ۳، ۱-۱۶.
10.22070/iws.2012.57
- فعله کری، زهره (۱۴۰۰)، «واکاوی چالش‌های اینترنت اشیاء در حوزه سلامت»، *فصلنامه رویکردهای پژوهشی نوین در مدیریت و حسابداری*، سال ۵، شماره ۷۲.
https://majournal.ir/index.php/ma/article/view/943
- قدسی، امیر (۱۳۹۲)، «تأثیر فضای مجازی بر امنیت ملی ج. ا. ایران و ارائه راهبرد (با تأکید بر ایفای نقش سرمایه اجتماعی)»، *راهبرد دفاعی*، سال۱۱، شماره ۴۴.
- قربانی, مصطفی (۱۴۰۲)، «بنیان‌ها و عوامل ماندگاری جمهوری اسلامی ایران»، *جامعه‌شناسی سیاسی جهان اسلام، سال ۱۱*، شماره ۲۳، ۱۱۱-۱۳۴. 10.22070/iws.2025.19963.2406
- مصلحی، محمد و حسین ابراهیم پور کومله (۱۳۹۶)، «اینترنت اشیا و چالش‌های امنیتی آن»، کنفرانس ملی فناوری‌های نوین در مهندسی برق و کامپیوتر.
- مهرآبادی، حجت (۱۴۰۲)، «*مروری بر به‌کارگیری اینترنت اشیاء در صنعت نفت و گاز*»، اولین همایش ملی پژوهش‌های نو پدید در حسابداری، مالی، مدیریت و اقتصاد با رویکرد توسعه اکوسیستم نوآوری.
https://civilica.com/doc/1922777/

- میرزایی، رضا و همتی، سینا (۱۴۰۲)، «*چالش‌ها و راه‌حل‌های مدیریت ترافیک پایدار برای شهرهای هوشمند مبتنی بر اینترنت اشیاء با استفاده از سیستم‌های حمل و نقل هوشمند*»، سومین کنگره بین‌المللی مهندسی عمران، معماری، مصالح ساختمانی و محیط.
https://civilica.com/doc/1969891/
- میرمحمدیان، سیدمیلاد، برهلیا، ساسان، بابامحمودی، رمضان، و آخوندی، زهرا (۱۳۹۶)، «مروری بر چالش‌ها و راهکارهای پیشگیری از چالش‌های اینترنت اشیا»، همایش ملی پژوهش‌های نوین در علوم و فناوری. https://civilica.com/doc/697207

ب- منابع انگلیسی

- Abdul-Qawy, A., & Tadisetty, S. (2015). The Internet of Things (IoT): An overview. *Journal of Engineering Research and Applications, 5*(12), Part 2. http://www.ijera.com
- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010
- Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69. https://doi.org/10.1007/s11277-011-0288-5
- Baniya, A., Agrawal, A., Abid, K., Nath, J., Chaudhary, B., & Kunwar, B. (2024). The Internet of Things: Security challenges and opportunities. In *2024 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*. https://doi.org/10.1109/PARC59193.2024.10486356
- Benar, M. (2020). *Internet of Things: Regulatory framework, cybersecurity, and data regulation in IoT for Iran* (Research Center of the Islamic Consultative Assembly, No. 17012) [In Persian].
- Botta, A., de Donato, W., Persico, V., & Pescape, A. (2016). The integration of cloud computing and Internet of Things: A survey. Proceedings of the 2nd International Conference on Future Internet of Things and Cloud (FiCloud-2014), 27-29. https://doi.org/10.1016/j.future.2015.09.021
- Chen, J., Zhang, Y., & Lee, P. (2021). Cybersecurity threats in IoT-based smart infrastructures: A case study of DDoS attacks. *Journal of Cyber Security and Digital Forensics, 7*(3), 112–125.

- Clapper, J. (2015). US Intelligence and the Future of the Internet of Things. National Intelligence. Retrieved from https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

- Dezhgir, H., & Houshmand, H. (2017). A review of security in the Internet of Things. In *National Conference on New Research in Science and Technology* [In Persian].

- Etehadi, H. (2024). Optimizing energy consumption of IoT devices in fifth-generation networks. In *23rd National Conference on Electrical, Computer, and Mechanical Engineering* [In Persian].

- Fadlullah, Z., Fouda, M., Kato, N., Takeuchi, A., Iwasaki, N., & Nozaki, Y. (2011). Toward intelligent machine-to-machine communications in smart grid. *IEEE Communications Magazine*, 49(4), 60-65. https://doi.org/10.1109/MCOM.2011.5741147

- Faleh-Kari, Z. (2021). Exploring IoT challenges in the healthcare domain. *New Research Approaches in Management and Accounting Quarterly*, 5(72). https://majournal.ir/index.php/ma/article/view/943 [In Persian]

- Gang, G., Zeyong, L., & Jun, J. (2011). Internet of things security analysis. In Internet Technology and Applications (iTAP), *2011 International Conference on (pp. 1-4). IEEE*. https://doi.org/10.1109/ITAP.2011.6006307

- Gartner. (2021). 3 themes surface in the 2021 hype cycle for emerging technologies. https://www.gartner.com/smarterwithgartner/3-themes-surface-in-the-2021-hype-cycle-for-emerging-technologies

- Ghodsi, A. (2013). The impact of cyberspace on national security of the Islamic Republic of Iran and strategy formulation (with emphasis on social capital role). *Defense Strategy*, 11(44) [In Persian].

- Ghorbani, M. (2023). Foundations and factors of the sustainability of the Islamic Republic of Iran. *Political Sociology of the Islamic World*, 11(23), 111-134. 10.22070/iws.2025.19963.2406

- Global Research. (2015). NSA uses the Internet of Things as a weapon platform. Retrieved from https://www.globalresearch.ca/

- Gope, P., & Sikdar, B. (2019). Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet of Things Journal, 6*(1), 580–589. https://doi.org/10.1109/JIOT.2018.2846299

- Greenberg, A. (2013). NSA: The Internet of Things is a military platform. *Wired*. https://www.wired.com

- Hosseinzadeh, M., & Rezaei, A. (2023). Cybersecurity in the Internet of Things domain. *Arman Pardazesh Quarterly*, 4(1). 10.22034/apj.2023.706757 [In Persian]

- Kavanagh, C. (2019). New tech, new threats, and new governance challenges: An opportunity to craft smarter responses? Retrieved from https://carnegieendowment.org/files/WP_Camino_Kavanagh___New_Tech_New_Threats.pdf

- Kavanagh, C. (2022). New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?. Carnegie Endowment for International Peace.

- Kaviani-Zadeh, E. (2018). Examining the Internet of Things and its impact on business. In *1st International Conference on New Approaches in Engineering Sciences* [In Persian].

- Li, S., & Zhao, S. (2015). The Internet of Things: A survey. *Information Systems Frontiers*, 17(2), 243-259. https://doi.org/10.1007/s10796-014-9492-7

- Madra, M. S., Paliszkiewicz, J., Svanadze, S., Nassir, A., Nestian, A. S., & Kitsing, M. (2020). The Internet of Things challenges – country and industry analyses. *Issues in Information Systems*, 21(4), 26-35. https://doi.org/10.48009/4_iis2020_26-35

- Mehrabadi, H. (2023). A review of IoT applications in the oil and gas industry. In 1st National Conference on Emerging Research in Accounting, Finance, Management, and Economics with a Focus on Innovation Ecosystem Development [In Persian]. https://civilica.com/doc/1922777/

- Miorandi, D., Sicari, S., Pellegrini, F., & Chlamtas, I. (2012). Internet of Things: Vision, applications, and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

- Mirmohammadian, S. M., Berahliya, S., Babamahmoudi, R., & Akhundi, Z. (2017). Review of challenges and solutions for preventing IoT-related issues. In *National Conference on New Research in Science and Technology* [In Persian]. https://civilica.com/doc/697207

- Mirzaei, R., & Hemmati, S. (2023). Challenges and solutions for sustainable traffic management in IoT-based smart cities using intelligent transportation systems. In *3rd International Congress on Civil Engineering, Architecture, Building Materials, and Environment*. https://civilica.com/doc/1969891/ [In Persian]

- Moslehi, M., & Ebrahimpour-Komleh, H. (2017). Internet of Things and its security challenges. In *National Conference on New Technologies in Electrical and Computer Engineering* [In Persian].

- Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context aware computing for the Internet of Things: A survey. *IEEE Communications Surveys & Tutorials, 16*(1), 414–454. https://doi.org/10.1109/SURV.2013.042313.00197

- Rahbani, M. S. (2020). Application of the Internet of Things in smart agriculture. *Green Industry Scientific-Promotional Journal*, 5(2) [In Persian].

- Rahmati Larhang, R., et al. (2022). Presenting an intelligent cyber defense model for the critical infrastructures of the Islamic Republic of Iran. *Strategic Studies of Cyberspace Quarterly*, 1(3). https://ssc.sndu.ac.ir/article_2554.html [In Persian]

- Salehi, J., Farajzadeh, A. & Farah Bakhsh, A. (2012). Examining the role of the Internet in the Egyptian social movement. *Political Sociology of the Islamic World*, 1(3), 1-16. 10.22070/iws.2012.57

- Shafiei, S. (2015). Analysis of challenges in the development of IoT technology: Security threats and digital divide. *Short Writing Monthly*, 1(7) [In Persian].

- Shnurenko, I., Murovana, T., & Kushchu, I. (2020). Artificial Intelligence: Media and Information Literacy, Human Rights and Freedom of Expression. UNESCO IITE and The Next Minds.

- Whitmore, A., Agarwal, A., & Xu, L. D. (2014). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, 1-14. https://doi.org/10.1007/s10796-014-9489-2

- Zarafshan, F., & Shirbandi, R. (2021). Review of attacks and security solutions in the Internet of Things. *Distributed Systems and Computing Biannual*, 4(1) https://www.jdcs.ir/article_191108.html [In Persian].