

## Identification of Cyber Security Components of Internet of Things

Sayyed Mohammadreza Davoodi <sup>1\*</sup>, Abdollah Nemati <sup>2</sup>, Tahereh Sabbaghi <sup>2</sup>

1. Associate Professor, Faculty of Management, Dehaqan Branch, Islamic Azad University, Dehaqan, Iran.
2. PhD Student, Faculty of Management, Dehaqan Branch, Islamic Azad University, Dehaqan, Iran.

### OPEN ACCESS

**Article type:** Review Article

**\*Correspondence:** Sayyed Mohammadreza Davoodi  
[sm.davoodi@iau.ac.ir](mailto:sm.davoodi@iau.ac.ir)

**Received:** November 5, 2024

**Accepted:** March 12, 2025

**Published:** Winter 2025

**Citation:** Davoodi, S. M., Nemati, A. and Sabbaghi, T. (2025). Identification of Cyber Security Components of Internet of Things. *Modern Studies in Management and Organization*, 1(4), 55-73. doi: 10.22034/jmsmo.2025.220930

**Publisher's Note:** JMSMO stays neutral with regard to jurisdictional claims in published material and institutional affiliations.



**Copyright:** Authors retain the copyright and full publishing rights.

Published by Research Center of Resource Management Studies and Knowledge-Based Business. This article is an open access article licensed under the [Creative Commons Attribution 4.0 International \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)

**Abstract:** This research aims to identify the components of cybersecurity of the Internet of Things and mutual authentication. In this paper, considering the unique and specific nature of the subject, the breadth and richness of research in this field, the ease of access to resources, and the study and summary of all related articles, the metasynthesis method has been used. Metasynthesis is a method that combines data from other studies with specific steps to meet the researcher's goal and yields new results. Using the Sandelowski and Barso model, and the keywords of Internet of Things security, privacy, network security, and mutual authentication, about 65 foreign and domestic scientific research articles published from 2014 to 2023 and materials collected from foreign databases and Persian articles published in scientific and research journals and publications in the country from 2015 to 2022 were found, of which the number of foreign articles was 47 and the number of domestic articles was 18. After reviewing and filtering, 40 articles were selected to extract the required content of the article, of which 34 were foreign articles and 6 Persian articles were selected. Among the components identified were threat control, access control, technical control, firewall protection, API security, security gateways, authentication, and tokens.

**Keywords:** Internet of Things Security, Privacy, Network Security, Mutual Authentication.

DOI: [10.22034/jmsmo.2025.220930](https://doi.org/10.22034/jmsmo.2025.220930)

### Extended Abstract

#### Introduction

The introduction of the Internet of Things (IoT), a critical technology in modern society, has significant implications for cybersecurity. IoT devices are ubiquitously connected and often lack essential security features. This makes the IoT vulnerable to a wide range of cyberattacks. Cyberattacks can exploit these vulnerabilities to obtain sensitive data, launch distributed denial-of-service (DDoS) attacks, and even

compromise critical infrastructure. A large-scale cyberattack on IoT networks could have severe consequences, including disruption of essential services and widespread economic damage.

The Internet of Things is a complex network of interconnected devices and people that work together to monitor and exchange information about usage and environmental conditions. It consists of smart devices equipped with embedded systems, including processors, sensors, and connected hardware that collect, transmit, and respond to the information they receive. These devices communicate with each other in their surroundings in the IoT ecosystem through an IoT gateway with another nearby device to exchange sensor data.

### **Theoretical framework**

Various researches on cybersecurity and authentication protocols in the field of Internet of Things have been conducted by researchers, some of which are introduced: Ghasemi in research in the field of Internet of Things the Iranian Telecommunications Research Center (Communications and Information Technology Research Institute) has carried out projects to investigate the implementation of Internet of Things technology and its security in Iran. One of these projects was titled "Developing the Internet of Things Business in the Country". In this project, based on the experiences of different countries in the fields of governance, business, applications and technologies, initial studies were conducted, and Iran's roadmap was determined with the aim of using new technologies such as the Internet of Things to increase economic welfare, quality of life and environmental protection to achieve the economic vision of 1404 (Roohollah., 2015).

In their research, Arkian and colleagues show that despite the research conducted on the Internet of Things and its security, various attacks have been introduced that have affected the space of this concept and its related technologies. The results show that countermeasures are merely reactive. Although these issues are changing due to regulatory restrictions, approval by government centers does not mean security. The issue of security in the Internet of Things can be considered the most important challenge in the development of this technology. In this regard, various standards are being developed, but the security requirements of the Internet of Things and even its risks have not been well identified and analyzed. By reviewing the articles and books presented in the field of Internet of Things security, it can be seen that security must be considered at all levels of packages and services. Therefore, security features will exist at all stages of system development. This type of security development is called the "defense in depth" approach. This approach embeds security into the heart of the IoT network and allows organizations and companies to have more time to defend their resources by reciprocally engaging attackers (Arkian, 2015).

In a study, Rahnavard and Mohammadian introduced the knowledge management system as a system for covering the process of creating, collecting, organizing, disseminating, and applying knowledge in an organization, or the art of creating value from the organization's intangible assets. They consider senior management support, role modeling, knowledge architecture, people involvement, information systems infrastructure, strategy and goals, knowledge measurement, organizational infrastructure, training, human resources, motivation, organizational culture, and teamwork as basic factors for the success of any knowledge management system (Rahnavard, 2015).

### **Methodology**

This research is a review in terms of its purpose and based on the method of collecting research data of the documentary-metasyntesis type. In the present study, the statistical population

including previous research (articles, projects, and theses in the field of Internet of Things security), was selected in the conducted reviews of 65 articles and research. In this study, the seven-step metasynthesis method of Sandelowski and Barso (2006) was used.

### **Discussion and Results**

This article provides a comprehensive overview of the most critical security considerations related to the Internet of Things. Companies with an IoT presence should understand and develop comprehensive monitoring. They should also provide tools to quickly identify any unusual activity on their networks. These tools should be used. Advanced detection tools leverage powerful technologies, such as machine learning and artificial intelligence algorithms, to analyze large data sets generated during normal network operations and alert administrators to deviations. By allowing organizations to respond quickly to security incidents and anticipate potential threats before they occur, layered defense mechanisms can significantly minimize the damage caused by cyberattacks.

### **Conclusion**

The research shows that as IoT technology advances, so do the associated security risks. The increasing frequency of cyberattacks that involve exploiting a common type of IoT device to gain access and compromise the entire network has underscored the importance of IoT security. Ensuring the safety of networks that rely on IoT devices has become an essential priority. IoT security is a diverse range of techniques, strategies, protocols, and practices that aim to minimize the growing vulnerabilities posed by IoT to modern businesses. To ensure that IoT networks are protected from potential attacks, it is crucial that computer science/engineering professionals, such as researchers, scientists, and academics, stay up-to-date with the latest IoT security solutions.

A developer's focus for building a smart object should be on developing secure software and secure integration. For those deploying IoT systems, hardware security and authentication are critical measures. Similarly, for operators, keeping systems up to date, malware mitigation, auditing, infrastructure protection, and credential protection are key measures in IoT security. However, with IoT deployments, it is crucial to weigh the cost of security against the risks before committing.

### **Contribution of authors**

All authors have participated in this research in equal proportion.

### **Ethical approval**

There are no human subjects in this article and informed consent is not applicable.

### **Conflict of interest**

No conflicts of interest are declared by the authors.

# مطالعات نوین در مدیریت و سازمان

سال اول، شماره چهارم، زمستان ۱۴۰۳ - صفحه ۷۳-۵۵

Homepage: <https://www.jmsmo.ir>

## شناسایی مؤلفه‌های امنیت سایبری اینترنت اشیاء

سید محمدرضا داودی<sup>۱\*</sup>، عبدالله نعمتی<sup>۲</sup>، طاهره صباغی<sup>۲</sup>

۱. دانشیار، دانشکده مدیریت، واحد دهقان، دانشگاه آزاد اسلامی، دهقان، ایران.

۲. دانشجوی دکتری، دانشکده مدیریت، واحد دهقان، دانشگاه آزاد اسلامی، دهقان، ایران.

**چکیده:** هدف از این تحقیق، شناسایی مؤلفه‌های امنیت سایبری اینترنت اشیاء و احراز هویت متقابل می‌باشد. در این مقاله، با توجه به بکر و خاص بودن موضوع و گستردگی و غنی بودن تحقیق و پژوهش در این زمینه و سهولت دسترسی به منابع و از سوی دیگر مطالعه و جمع بندی تمامی مقاله‌های مرتبط از روش فراترکیب استفاده شده است. فراترکیب روشی است که با گام‌های مشخص، داده‌های نتایج حاصل از سایر مطالعات را برای پاسخگویی به هدف پژوهشگر ترکیب نموده و نتایج جدیدی به دست می‌دهد. با استفاده از الگوی سندلوسکی و بارسو، و کلید واژه‌های امنیت اینترنت اشیاء، حریم خصوصی، امنیت شبکه و احراز هویت متقابل، حدود ۶۵ مقاله خارجی و داخلی علمی پژوهشی چاپ شده از سال ۲۰۱۴ تا ۲۰۲۳ و مطالب جمع آوری شده از بانک‌های اطلاعاتی خارجی و مقالات فارسی چاپ شده در مجلات و نشریه‌های علمی و پژوهشی داخل کشور از سال ۱۳۹۴ تا ۱۴۰۱ یافت شد که تعداد مقاله خارجی ۴۷ و مقاله داخلی ۱۸ عنوان بود. تعداد ۴۰ مقاله پس از بررسی و پالایش جهت استخراج مطالب مورد نیاز مقاله انتخاب شد که تعداد ۳۴ عنوان مقاله خارجی و تعداد ۶ عنوان مقاله فارسی انتخاب شد. از جمله مؤلفه‌های کنترل تهدید، کنترل دسترسی، کنترل فنی، حفاظت فایروال، امنیت API، دروازه‌های امنیتی، احراز هویت و توکن‌ها شناسایی شد.

**واژگان کلیدی:** امنیت اینترنت اشیاء، حریم خصوصی، امنیت شبکه، احراز هویت متقابل.

DOI: [10.22034/jmsmo.2025.220930](https://doi.org/10.22034/jmsmo.2025.220930)

### دسترسی آزاد

نوع مقاله: مقاله مروری

\*نویسنده مسئول: سید محمدرضا داودی

sm.davoodi@iau.ac.ir

تاریخ دریافت: ۱۴۰۳/۰۸/۱۵

تاریخ پذیرش: ۱۴۰۳/۱۲/۲۲

تاریخ انتشار: زمستان ۱۴۰۳

استناد: داودی، سید محمدرضا، نعمتی، عبدالله و صباغی، طاهره. (۱۴۰۳). شناسایی مؤلفه‌های امنیت سایبری اینترنت اشیاء. مطالعات نوین در مدیریت و سازمان، ۱(۴)، ۷۳-۵۵.

یادداشت ناشر: JMSMO درخصوص ادعاهای قضایی در مطالب منتشر شده و وابستگی‌های سازمانی بی‌طرف می‌ماند.

### مقدمه

معرفی اینترنت اشیاء (IoT) که به عنوان یک فناوری حیاتی در جامعه مدرن ظهور کرده، با پیامدهای قابل توجهی برای امنیت سایبری مواجه می‌باشد. دستگاه‌های اینترنت اشیاء همه جا به هم متصل هستند و اغلب فاقد ویژگی‌های امنیتی ضروری می‌باشند. این امر اینترنت اشیاء را در برابر طیف وسیعی از حملات سایبری آسیب پذیر می‌کند.



کپی‌رایت: نویسندگان حق نشر و حقوق کامل انتشار را برای خود محفوظ می‌دارند.

منتشر شده توسط مرکز تحقیقات مطالعات مدیریت منابع و کسب و کار دانش بنیان. این مقاله، یک مقاله با دسترسی آزاد است که تحت مجوز

[Creative Commons Attribution 4.0 International \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/) منتشر شده است.

حملات سایبری می‌توانند از این آسیب‌پذیری‌ها برای به دست آوردن داده‌های حساس سوء استفاده کنند و حملاتی راه اندازی کنند که سرویس (DDoS) توزیع شده و حتی کنترل زیرساخت‌های حیاتی را به دست بگیرند. یک حمله سایبری در مقیاس بزرگ به شبکه‌های اینترنت اشیاء می‌تواند عواقب شدیدی، از جمله ایجاد اختلال در خدمات ضروری و آسیب‌های اقتصادی گسترده داشته باشد.

اینترنت اشیاء یک شبکه پیچیده از دستگاه‌های به هم پیوسته و افراد است که با یکدیگر همکاری می‌کنند. برای نظارت و تبادل اطلاعات در مورد استفاده و شرایط محیطی این سیستم متشکل از دستگاه‌های هوشمند مجهز به سیستم‌های تعبیه شده شامل پردازنده‌ها، حسگرها و سخت افزار متصل است که اطلاعات به دست آمده را جمع آوری، انتقال و پاسخ می‌دهد. این دستگاه‌ها در محیط اطراف خود در اکوسیستم اینترنت اشیاء با درگاه اینترنت اشیاء با دستگاه مجاور دیگری برای تبادل داده‌های حسگر با یکدیگر ارتباط برقرار می‌کنند.

گسترش دستگاه‌های اینترنت اشیاء بسیار سریع بوده و زمینه چالش‌های منحصر به فرد در مورد قابلیت همکاری دستگاه‌ها، حریم خصوصی داده‌ها و امنیت اینترنت اشیاء نه تنها افراد را قادر می‌سازد تا کارآمدتر زندگی و کار کنند، همچنین به آنها کمک می‌کند برای کنترل بیشتر بر زندگی خود و کسب و کارها به شدت به اینترنت اشیاء متکی باشند. با اینترنت اشیاء، سازمان‌ها می‌توانند بینش‌هایی در زمان واقعی در مورد نحوه عملکرد سیستم‌های مختلف به دست آورده و به آنها اجازه می‌دهد فرآیندها را بهینه کنند و هزینه‌های نیروی کار را کاهش دهند. علاوه بر این، اینترنت اشیاء باعث دیده شدن کسب و کارها می‌شود. هزینه‌های معاملات، تولید و حمل و نقل را کاهش و کارایی خدمات را افزایش می‌دهد.

برنامه‌های هوشمند اینترنت اشیاء که به سیستم‌های پیش ساخته SaaS نیز معروف هستند، مجهز به تکنیک‌های یادگیری ماشین برای تجزیه و تحلیل هستند و حجم وسیعی از داده‌های جمع آوری شده از حسگرهای به هم پیوسته را پردازش و تحلیل نموده، ارائه دیدگاه عملی به کاربران شرکت از طریق رابطه با نظارت بر KPI ها (کلید شاخص‌های عملکرد)، نرخ‌های MTBF (میانگین زمان بین شکست) و سایر معیارها در داشبوردها و هشدارهای بی‌درنگ IoT می‌توانند به شناسایی بی‌نظمی‌ها و شروع خودکار کمک کند.

یکی از بزرگترین موانع تضمین امنیت اینترنت اشیاء، تعمیرات یا اقدامات پیشگیرانه آن است. داده‌های حساس برای این دستگاه‌ها جمع می‌شوند، مانند آنچه در خانه و محل کار می‌گویید و انجام می‌دهید. اعتماد کاربران به اینترنت اشیاء به قابلیت اطمینان آن بستگی دارد. دستگاه‌های زیاد متصل به سیستم با مدیریت نادرست، از داده‌های کاربران در حالی که داده‌ها ذخیره شده و در حال انتقال است، به اندازه کافی محافظت نمی‌شود. حتی در برنامه‌های به خوبی تثبیت شده، آسیب پذیری نرم افزار به طور مداوم کشف می‌شوند. با این حال بسیاری از دستگاه‌های اینترنت اشیاء را نمی‌توان به روز کرد و به دلیل عدم حفاظت ذاتی آنها برای همیشه آسیب پذیر بوده و باعث می‌شود آنها بلااستفاده شوند.

دستگاه‌های IoT مانند روترها و دوربین‌ها به طور فزاینده‌ای مورد هدف هک‌هایی قرار می‌گیرند که از آنها به عنوان بخشی از بات‌های عظیم و به هم پیوسته سوء استفاده می‌کنند. بر اساس برآوردهای شرکت تحلیلگر فناوری IDC

(شرکت بین المللی داده)، دیتای دستگاه های IOT در پنج سال آینده، ZB 79.4 که برخی از این داده های اینترنت اشیا «فشرده و غیرعادی» خواهند بود. همانطور که توسط IDC پیش بینی شده است. این بدان معنی است که فقط شامل به روز رسانی های نسبتاً کوتاه مدت بوده مانند آنهایی که توسط سنسورها یا کنتورهای هوشمند ارائه می شوند (Das & Yashkova, 2022).

علاوه بر این، دستگاه هایی مانند دوربین های امنیتی با بینایی کامپیوتری داخلی ممکن است مقادیر زیادی داده تولید کند. مطابق با پیش بینی IDC، میزان داده های تولید شده توسط دستگاه های اینترنت اشیا (IoT) در سال های آتی حجم بسیار زیادی خواهد شد. این گزارش ادعا می کند که در حالی که پرچم دار فعلی در تولید داده، نظارت تصویری است، ولی سایر صنایع و کاربردهای پزشکی به زودی از آن سبقت خواهد گرفت و همچنین پیش بینی می شود پهپادهای متصل به هم با دوربین های داخلی نیز که تبدیل به یک هواپیما شوند و ابزار مهم جمع آوری داده ها از حسگرها، طیف گسترده ای از جمله صدا، تصویر، و داده های تخصصی و در آینده نزدیک وسایل نقلیه خودران، توسط حسگر خودرو تولید خواهد شد.

انجام یک بررسی کامل در خصوص آسیب پذیری شبکه اینترنت اشیا اولین گام در ایجاد یک محیط IoT-enabled است. با توجه به فرمت های داده زیاد و قابلیت های پردازش دستگاه های اینترنت اشیا، هیچ راه حل امنیت سایبری «یکسان برای همه» وجود ندارد که بتواند از وسعت استقرار اینترنت اشیا محافظت کند. در نتیجه باید تدابیری اتخاذ کنیم علاوه بر محافظت از این فناوری، فوریت این نیاز فقط در حال افزایش نیز مد نظر باشد (Alaba et al., 2017). از آنجایی که تعداد دستگاه های IoT در دسترس همچنان در حال افزایش است. به دلیل ظرفیت محدود و طراحی متنوع، دستگاه های IoT در معرض خطرات امنیتی مختلف هستند. تهدیدات بی سیم شبکه های ad hoc زمانی افزایش می یابند که دستگاه ها به صورت کنترل نشده و بالقوه مستقر می شوند. محیط های خطرناک در هت نت ها معمولاً حملاتی مانند فروچاله ها، سیاهچاله ها، کرم چاله ها، سیبیل ها، انکار سرویس DoS، جذب گره و تزریق گره مورد استفاده هکرها قرار می گیرد (Wani et al., 2022).

### مبانی نظری و پیشینه پژوهش

تحقیقات متنوعی در مورد امنیت سایبری و پروتکل های احراز هویت در حوزه اینترنت اشیا توسط محققان انجام گرفته است که بخشی از آن ها معرفی می شوند: قاسمی در تحقیقی در حوزه اینترنت اشیا مرکز تحقیقات مخابرات ایران (پژوهشگاه ارتباطات و فناوری اطلاعات) پروژه هایی را برای بررسی پیاده سازی فناوری اینترنت اشیا و امنیت آن در ایران انجام داده است. یکی از این پروژه ها با عنوان «تدوین کسب و کار اینترنت اشیا در کشور» انجام شده است. در این پروژه بر اساس تجربیات کشورهای مختلف در حوزه های حاکمیت، کسب و کار، کاربردها و فناوری ها مطالعات اولیه صورت گرفت و نقشه راه ایران با هدف استفاده از فناوری های نوین نظیر اینترنت اشیا برای افزایش رفاه اقتصادی، کیفیت زندگی و حفاظت از محیط زیست برای رسیدن به چشم انداز اقتصادی ۱۴۰۴ تعیین شده است (Roohollah., 2015).

ارکیان و همکاران در تحقیق انجام گرفته نشان می‌دهند که علیرغم تحقیقات صورت گرفته مرتبط با اینترنت اشیاء و امنیت آن، حملات مختلفی معرفی می‌شود که فضای این مفهوم و فناوری‌های مرتبط با آن را درگیر کرده است. نتایج نشان می‌دهد اقدامات متقابل صرفاً واکنشی است. اگرچه این مسائل به خاطر محدودیت‌های نظارتی در حال تغییر است، اما با این حال تأیید مراکز دولتی به معنای امنیت نخواهد بود. مسئله امنیت در اینترنت اشیاء را می‌توان مهم‌ترین چالش توسعه این فناوری در نظر گرفت. در این رابطه استانداردهای مختلفی در حال توسعه است ولی همچنان نیازمندی‌های امنیتی اینترنت اشیاء و حتی مخاطرات آن به خوبی شناسایی و تحلیل نشده است. با بررسی مقالات و کتابهایی که در حوزه امنیت اینترنت اشیاء ارائه شده‌اند، می‌توان دریافت که امنیت باید در تمام سطوح بسته‌ها و سرویس‌ها نیز در نظر گرفته شود. بنابراین، در تمام مراحل توسعه سیستم، ویژگی‌های امنیتی وجود خواهند داشت. به این نوع توسعه امنیت، رویکرد «دفاع در عمق» گفته می‌شود. این رویکرد، امنیت را در دل شبکه اینترنت اشیاء گنجانده و به سازمان‌ها و شرکت‌ها اجازه می‌دهد تا با درگیر کردن مهاجمین به صورت متقابل، زمان بیشتری برای دفاع از منابع خود داشته باشند (Arkian, 2015).

رهنورد و محمدیان در تحقیقی، سیستم مدیریت دانش را سیستمی برای پوشش فرایند خلق، جمع‌آوری، سازماندهی، اشاعه و کاربرد دانش در سازمان یا هنر خلق ارزش از دارایی‌های نامشهود سازمان معرفی کردند و حمایت مدیر ارشد، الگوگیری، معماری دانش، درگیری افراد، زیرساخت سیستم‌های اطلاعاتی، راهبرد و اهداف، سنجش دانش، زیرساخت سازمانی، آموزش، منابع انسانی، ایجاد انگیزه، فرهنگ سازمان و کار تیمی را عوامل پایه‌ای برای موفقیت هر سیستم مدیریت دانش می‌دانند (Rahnavard, 2015).

آلامر و همکاران در بررسی پیرامون پروتکل احراز هویت متقابل  $RFID^1$  بر اساس رمزنگاری منحنی بیضوی  $ECC^2$  برای اینترنت اشیاء به منظور حذف تهدیدات امنیتی ناشی از کانال آسیب‌پذیر بین بارکدها و قرائت گر‌ها ارائه دادند. علاوه بر این، از پروتکل مبادله کلید  $ECDH^3$  برای تولید کلید موقتی اشتراکی برای رمزنگاری پیام‌های جدید انتقال داده شده استفاده می‌کند. تحلیل امنیتی پروتکل پیشنهادی نشان می‌دهد که پروتکل پیشنهادی ویژگی‌های امنیتی مانند احراز هویت متقابل، ناشناس بودن، امنیت پیشرو، حریم خصوصی مکان را تضمین می‌کند و همچنین در مقابل حملات جعل هویت، تکرار مقاوم می‌باشد (Alamr et al., 2018).

کالرا و همکاران طی تحقیقی پیرامون پروتکل احراز هویت متقابل برای دستگاه‌های تعبیه شده و سرورهای ابری بر اساس رمزنگاری منحنی بیضوی پیشنهاد کردند. پروتکل پیشنهادی، احراز هویت بین دستگاه‌ها و خدمات دهنده ابری را با استفاده از کوکی‌های HTTP تضمین می‌کند. این پروتکل نیازمندی‌های امنیتی احراز هویت متقابل، محرم بودن، ناشناس بودن و امنیت پیشرو را تضمین می‌کند و در برابر حملات امنیتی مانند حمله مکرر و سرقت کوکی، استراق

<sup>1</sup> Radio-Frequency Identification

<sup>2</sup> Elliptic Curve Cryptography

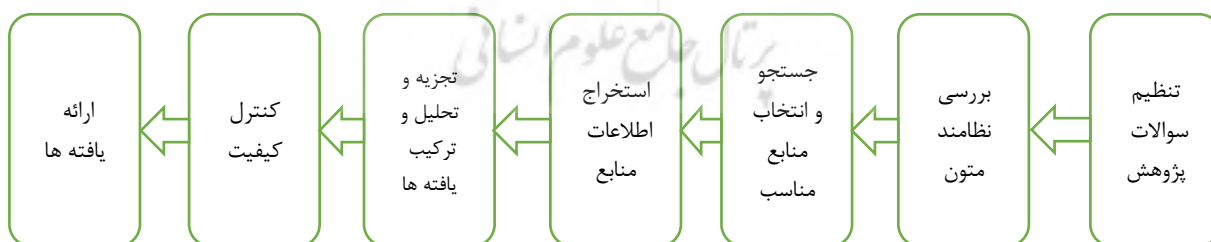
<sup>3</sup> Elliptic Curve Diffie-Hellman

سمع، جستجوی فراگیر، دیگشتری برون خط و حمله نشت تصدیق کننده مقاوم می باشد. الگوریتم های رمز نگاری مبتنی بر منحنی بیضوی، راه حل های امنیتی بهتری در مقایسه با دیگر الگوریتم های رمز نگاری کلید عمومی ( $PKC^1$ ) به علت کلید کوچکتر و محاسبات کاراکتر ارائه می کنند و برای محیط هایی با دستگاه های منبع محدود از نظر حافظه و قدرت پردازشی بسیار مناسب هستند (Kalra & Sood, 2015).

کمیسر و همکاران طی تحقیقی پیرامون پروتکلی، پیشنهاد دادند که با توجه به گسترش اینترنت اشیاء درهای زیادی را به سمت کاربردهای مختلف خواهد گشود. شبکه های حسگر بی سیم WSN به عنوان یکی از واقعی ترین و مؤثرترین کاربردهای شبکه اینترنت اشیاء می باشند. این تحقیق بر روی تعامل بین گره حسگر با کاربر راه دور متمرکز شده و یک پروتکل سبک وزن برای این محیط های منبع محدود ارائه می دهد. پروتکل پیشنهادی این امکان را فراهم می کند که گره حسگر و کاربر راه دور به یک روش امن یکدیگر را احراز هویت کنند. پروتکل پیشنهادی از رشته اعداد تصادفی، عملیات XOR و  $HMAC^2$  برای بررسی یکپارچگی پیام های مبادله شده استفاده می کند. تحلیل امنیتی نشان می دهد پروتکل پیشنهادی در مقابل انواع حملات مقاوم بوده و بسیاری از نیازمندی های امنیتی را برآورده می کند (Khemissa & Tandjaoui, 2016).

### روش پژوهش

این پژوهش از نظر هدف مروری و بر اساس شیوه گردآوری داده های پژوهش از نوع اسنادی – فراترکیب است. در پژوهش حاضر جامعه آماری شامل پژوهش های پیشین (مقالات، طرح ها و پایان نامه ها در زمینه امنیت اینترنت اشیاء) در بررسی های انجام شده ۶۵ مقاله و پژوهش انتخاب شد. در این پژوهش، از روش هفت مرحله ای فراترکیب سندلوسکی و بارسو<sup>۳</sup> (۲۰۰۶) استفاده شده است. که مراحل آن به شرح نمودار شماره ۱ می باشد.



نمودار ۱. روش سندلوسکی و بارسو (Chenail, 2009)

<sup>1</sup> Public Key Cryptography

<sup>2</sup> Hash-based Message Authentication Code

<sup>3</sup> Sandelowski & Barroso

## یافته‌های پژوهش

### گام نخست: تنظیم پرسش‌های پژوهش

نخستین گام در روش فراترکیب، تنظیم پرسش‌های فرا ترکیب است. این پرسش‌ها عموماً براساس چهار پارامتر چه چیزی، چه کسی، چه زمانی، و چگونه، قابل تنظیم است. در گروه‌بندی و تحلیل ابعاد امنیت سایبری اینترنت اشیا مورد سؤال قرار گرفته است.

جدول ۱. پرسش‌های پژوهش (Chenail, 2009)

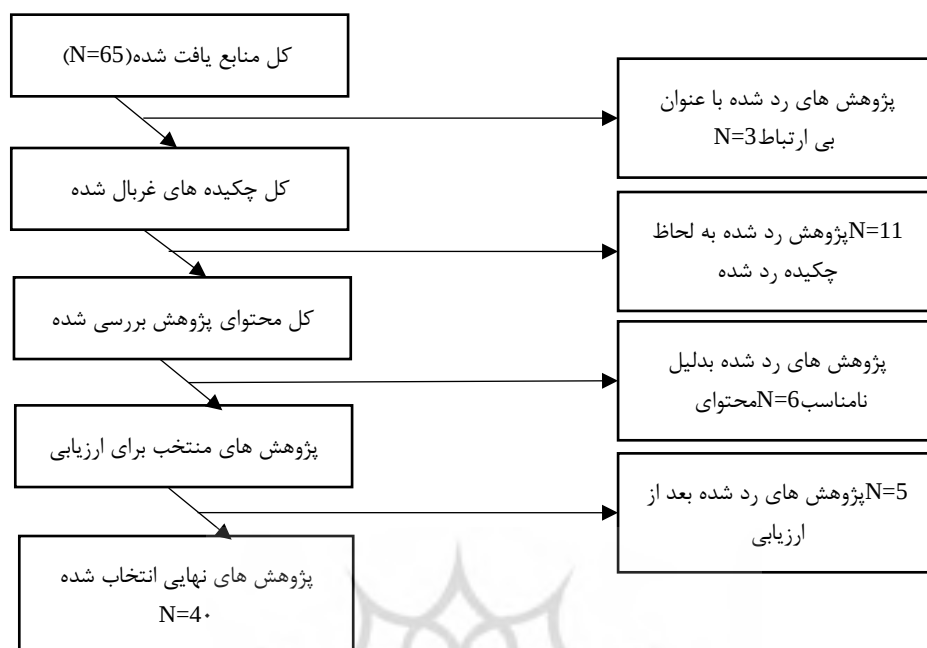
| پارامتر             | پرسش پژوهش                                                         |
|---------------------|--------------------------------------------------------------------|
| چه چیزی (What)      | مقوله زیربنایی امنیت سایبری IOT کدامند؟                            |
| چه کسی (Who)        | چه افرادی در بررسی امنیت IOT نقش آفرین هستند؟                      |
| محدوده زمانی (When) | انتخاب آثار موجود در محدوده زمانی ۱۳۹۴ تا ۱۴۰۱ شمسی و ۲۰۱۴ تا ۲۰۲۳ |
| چگونه (How)         | مقوله‌های امنیت سایبری IOT چه ارتباطی با یکدیگر دارند؟             |

### گام دوم: بررسی نظام‌مند متون

روش تحقیق در این مقاله با توجه به تخصصی بودن موضوع و فراگیر نبودن تکنولوژی اینترنت اشیا، از روش فرا ترکیب با الگوی سندلوسکی و بارسو و مطالعات مروری چالش‌ها و کاربردها و با استفاده از کلید واژه‌های امنیت اینترنت اشیا، حریم خصوصی، امنیت شبکه و احراز هویت متقابل، تعداد حدود ۶۵ مقاله خارجی و داخلی علمی پژوهشی چاپ شده از سال ۲۰۱۴ تا ۲۰۲۳ و مطالب جمع‌آوری شده از بانک‌های اطلاعاتی، ScienceDIRECT, Google, CINAHL, Scholar و ... و مقالات فارسی چاپ شده در مجلات و نشریه‌های علمی و پژوهشی داخل کشور از سال ۱۳۹۴ تا ۱۴۰۱ یافت شد که تعداد مقاله خارجی ۴۷ و مقاله داخلی ۱۸ عنوان بود و تعداد ۳۴ عنوان مقاله خارجی و تعداد ۶ عنوان مقاله فارسی انتخاب شد.

### گام سوم: جستجو و انتخاب متون مناسب

در ادامه با استفاده از روش CASP با شروط کیفی، هر مقاله به لحاظ کیفی مورد ارزیابی قرار گرفت. هریک از مقالات وزن دهی و امتیاز بندی شده و مقالاتی که مجموع امتیاز ۲۵ به بالا شود به لحاظ کیفی مورد تأیید و بقیه حذف شدند. فرآیند بازبینی در این تحقیق بطور خلاصه در نمودار شماره ۲ نشان داده می‌شود.



نمودار ۲. فرآیند بازبینی و انتخاب (Source: By author)

#### گام چهارم: استخراج اطلاعات پژوهش

در این پژوهش، اطلاعات پژوهش‌ها در جدول ۲ دسته بندی شد. این جدول شامل اطلاعات زیر می‌باشد: اطلاعات شناسنامه‌ای پژوهش (عنوان، نام و نام خانوادگی پدید آورندگان و سال انتشار، اطلاعات روش کلیدی (روش و هدف پژوهش)، اطلاعات یافته‌های اصلی (نتایج و یافته‌های پژوهش).

جدول ۲. اطلاعات مقالات داخلی و خارجی منتخب (Source: By author)

| ردیف | نویسنده/سال انتشار        | هدف پژوهش                                                         | روش پژوهش                      | نتایج پژوهش                                                                               |
|------|---------------------------|-------------------------------------------------------------------|--------------------------------|-------------------------------------------------------------------------------------------|
| ۱    | Gholichi, 2016            | تهدیدات امنیتی در اینترنت و روشهای مقابله با آن                   | www.gartner.com<br>پیش بینی    | تخمین بیش از ۲۵٪ حملات سایبری روی تجهیزات اینترنت اشیاء                                   |
| ۲    | Hussein & Nhlabatsi, 2022 | ویژگی های DBMS اینترنت اشیاء                                      | مطالعات مروری و تحقیقات میدانی | استفاده از پروتکل های رمز گذاری و رمز گشایی روی پلتفرم ها برای حفاظت از داده ها و اطلاعات |
| ۳    | Agrawal et al., 2019      | حفظت و امنیت داده‌ها                                              | تحقیقات و مطالعات مروری        | جلوگیری از تخریب داده ها از طریق محدودیت دسترسی غیرمجاز                                   |
| ۴    | Scott, 2017               | چگونه دستگاه های IoT خود را از بات نت ها و سایر تهدیدات ایمن کنیم | تحقیقات و مطالعات مروری        | نقص در تجهیزات ذخیره سازی داده‌ها، خطاهای انسانی، حملات ویروسی، خطاهای نرم افزاری         |

| ردیف    | نویسنده/سال انتشار                             | هدف پژوهش                                                                                                                                      | روش پژوهش                                        | نتایج پژوهش                                                                                                                                                                                                        |
|---------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ۵       | Fei, 2016                                      | امنیت و حریم خصوصی در مدل‌ها، الگوریتم‌ها و پیاده‌سازی اینترنت اشیا (IoTs)                                                                     | مطالعات مروری و کتابخانه‌ای                      | امنیت حریم خصوصی، اصلی‌ترین چالش امنیت IOT و حفاظت از آن بروش‌های امنیتی بایستی مورد توجه قرار گیرد.                                                                                                               |
| ۶       | Moaveni, 2016                                  | چگونگی تأمین امنیت دستگاه‌های متصل به اینترنت و مقابله با تهدیدات                                                                              | تحقیقات و مطالعات مروری                          | دستگاه‌ها برای تصدیق در برابر سیستم‌های دیگر نیاز به یک شناسه منحصر به فرد و کلمه عبور دارند                                                                                                                       |
| ۷       | Biplob, 2014                                   | چارچوب امنیتی RFID مقیاس پذیر و پروتکل IOT پشتیبانی از                                                                                         | تحقیقات و مطالعات مروری                          | پیشنهاد رویکرد ترکیبی که با استفاده از بازرسی دستی امنیت به همراه فناوری ردیابی و مدیریت اشیاء امکان پذیر خواهد شد                                                                                                 |
| ۸       | Lu & Da, 2103                                  | تحقیق امنیت سایبری اینترنت اشیا: مروری بر موضوعات تحقیقاتی جاری                                                                                | تحقیقات کتابخانه‌ای                              | استفاده از فن آوری بلاکچین برای افزایش امنیت مبتنی بر محدود کردن دسترسی به اپلیکیشن‌ها                                                                                                                             |
| ۹ و ۱۰  | Matheu et al., 2020; Nam & Sukhomlin, 2023     | در مورد امنیت سایبری سیستم‌های اینترنت اشیا - بررسی صدور گواهینامه امنیت سایبری برای اینترنت اشیا                                              | مطالعه مروری و کتابخانه‌ای                       | آنالیز ارائه الگوی کاربری از طرف اشیا هوشمند و ایمن سازی برای جلوگیری از آسیب‌های ناشی از حملات هکرها و هزینه‌های مربوط به باز یابی داده‌ها و تحلیل پیشگیرانه در اینترنت اشیا                                      |
| ۱۱ و ۱۲ | Seoane et al., 2022; Tsai et al., 2022         | ارزیابی عملکرد CoAP و MQTT با پشتیبانی امنیتی برای IoT - مکانیسم به‌روزرسانی خودکار کلید برای ارتباطات سبک وزن M2M و افزایش امنیت اینترنت اشیا | مطالعه موردی CoAP با استفاده از کتابخانه Libcoap | قابلیت همکاری بین دستگاه‌های IOT و شبکه‌های ارتباطات آنها با استفاده از کلید برنامه لایه بین فعالیت‌های IoT و دستگاه واسطه و روشی کاربردی و بهینه برای انتقال داده‌ها به شبکه و تعیین کاربرد محدودیت پروتکل (CoAP) |
| ۱۳ و ۱۴ | Park et al., 2018                              | بر اساس MQTT یک SDN Multicast IoT / بهره‌برداری مبتنی بر MQTT از آسیب‌پذیری‌های امنیتی IoT در شبکه‌های ZigBee                                  | مطالعه موردی و کتابخانه‌ای                       | انتقال تله‌متری پیام                                                                                                                                                                                               |
| ۱۵      | Venkatraman & Overmars, 2019                   | روش جدید حملات مبتنی بر فاکتورسازی اولیه به احراز هویت RSA در اینترنت اشیا بروش رمزنگاری                                                       | مطالعات کتابخانه‌ای                              | انتقال اطلاعات در CoAP از طریق UDP                                                                                                                                                                                 |
| ۱۶ و ۱۷ | Hung & Hsu, 2018; Sreekanth & Jeyachitra, 2022 | تجزیه و تحلیل نیاز مصرف AES FOR WSN IoT / پیاده‌سازی AES کارآمد منطقه با استفاده از FPGA برای برنامه‌های IOT                                   | آیین نامه استانداردسازی مصرف برق IOT             | (Rivest-Shamir-Adleman), AES-RSA (استاندارد پیشرفته استاندارد رمزگذاری)                                                                                                                                            |

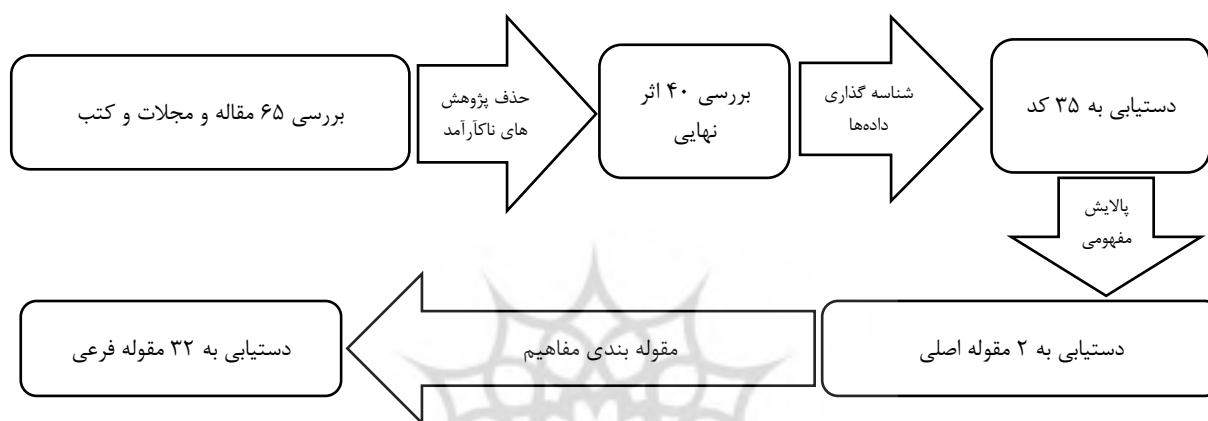
| ردیف    | نویسنده/سال انتشار                         | هدف پژوهش                                                                                                                                                                | روش پژوهش                                                          | نتایج پژوهش                                                                                                                                                                                                                      |
|---------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ۱۸ و ۱۹ | Debro et al., 2019; Vaclavova et al., 2022 | IoT پیشنهاد راه حل دستگاه بر اساس مفهوم صنعت حسگرها / مسیریابی کارآمد انرژی با آگاهی از طیف IoT برای ارتباطات دستگاه به دستگاه.                                          | تحقیق و مطالعه کتابخانه ای                                         | MQTT به عنوان یک سیستم پیام انتشار/اشتراک / MQTT یک گزینه عالی برای شبکه های بی سیم / پشتیبانی پروتکل MQTT دارای قابلیت امنیتی TLS                                                                                               |
| ۲۰      | Yu & Park, 2021                            | طراحی و پیاده سازی دستگاه لبه IoT برای جمع آوری داده های ماشین نا همگن                                                                                                   | مطالعات کتابخانه ای                                                | ایجاد اختلال در گره ها با اعمال تغییرات در آنها / تحت کنترل گرفتن کامل گره ها / آسیب زدن به اکسپلورر و کاهش سطح دسترسی                                                                                                           |
| ۲۱      | Pappalardo & Virdis, 2022                  | یک پروکسی MxLWM مبتنی بر لبه اینترنت اشیاء آگاه از QoS                                                                                                                   | مطالعه و تحقیق کتابخانه ای                                         | اصطلاح "تزریق وابستگی" برای ایجاد برنامه های کاربردی نرم افزاری / هنگامی که یک دشمن گره های جعلی را به یک شبکه کامل تزریق می کند، این تزریق به عنوان گره جعلی شناخته می شود.                                                     |
| ۲۲ و ۲۳ | Agrawal et al., 2019; Che et al., 2020     | مکانیسم تخمین گره کلیدی بر اساس نمودار حمله برای امنیت اینترنت اشیاء / تشخیص حمله ضبط گره در شبکه های حسگر بی سیم. سیستم IEEE                                            | تحقیقات و مطالعات کتابخانه ای                                      | گرفتن یک گره و استخراج بعدی آن از داده های رمزگذاری شده ، فریب گره های ناشناس یا تغییر با پخش مجدد سیگنال ها                                                                                                                     |
| ۲۴ و ۲۵ | Alharbi et al., 2022; Kim & Suh, 2021      | استراق سمع آسیب پذیری و اقدامات متقابل در ارتباطات IoT مادن قرمز برای حسگرها/ حمله دستگاه های پروفایل به دستگاه های اینترنت اشیاء مبتنی بر WiFi با استفاده از استراق سمع | مطالعات کتابخانه ای                                                | حملات جذب گره اینترنت اشیاء ، از جمله جعل، پارازیت، سازش فیزیکی، حمله زنجیره تامین، حمله سیستم عامل و بدافزار. حملات مبتنی بر اینترنت اشیاء استراق سمع. عدم رمزگذاری، نرم افزار یا سخت افزار قدیمی ، آلودگی به بدافزار یا ترکیبی |
| ۲۶ و ۲۷ | Abbasi et al., 2022; Yoon, 2020            | بهبود نرخ تشخیص حمله فروچاله از طریق قانون مشخصات مبتنی بر دانش برای تکنیک تشخیص نفوذ حمله فروچاله                                                                       | مطالعات کتابخانه ای                                                | به خطر افتادن یکپارچگی بعثت تزریق بد افزار و ایجاد شرایط سرقت اطلاعات و داده ها و آسیب پذیر بودن دستگاه های اینترنت اشیاء / حملات انکار سرویس، مانند TDA                                                                         |
| ۲۸ و ۲۹ | Kareem et al., 2023; Zeng et al., 2022     | استفاده از توزیع پواسون برای تقویت تشخیص حمله LDoS NB-IoT مبتنی بر CNN.                                                                                                  | در مجموعه مقالات کنفرانس IEEE 2022 مورد محاسبات قابل اعتماد و ایمن | انواع حمله (DDoS) با ارائه مکرر درخواست های نامشخص پروتکل انتقال ابر متن (HTTP) اشکال مختلف حمله . (Slowloris) از جمله سیل HTTP ، سیل SYN، تقویت DNS، SQLi، حمله سیل ICMP درخواست اکو                                            |

| ردیف    | نویسنده/سال انتشار               | هدف پژوهش                                                                                                                                                                                    | روش پژوهش                    | نتایج پژوهش                                                                                                                                                                                        |
|---------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ۳۰ و ۳۱ | An & Cho, 2022; Shiranzaei, 2018 | بهبود نرخ تشخیص حمله فروچاله از طریق قانون مشخصات مبتنی بر دانش برای تکنیک تشخیص نفوذ حمله فروچاله اینترنت اشیاء بین المللی / رویکردی برای کشف فروچاله و حمله هدایت انتخابی در اینترنت اشیاء | مطالعات کتابخانه ای          | حمله حفره امنیتی (DNS پیکربندی شده) حملات جایگزین ، مانند حملات ضبط گره ، تصدیق حمله باز پخش تایید، و جداول مسیریابی حذف شده یا تغییر یافته.. / اختلال در ارتباطات. IP بسته های داده ها و رمز عبور |
| ۳۲      | Vaclavova et al., 2022           | دیدگاه تحلیل بازار                                                                                                                                                                           | مطالعه میدانی                | افزایش حجم داده های اینترنت اشیاء                                                                                                                                                                  |
| ۳۳      | Alaba et al., 2017               | امنیت اینترنت اشیاء                                                                                                                                                                          | مطالعه کتابخانه ای           | بررسی کامل آسیب پذیری اینترنت اشیاء اولین گام امنیت می باشد                                                                                                                                        |
| ۳۴      | Wani et al., 2022                | یک رویکرد جدید برای ایمن سازی داده ها در برابر دشمن                                                                                                                                          | مطالعه کتابخانه ای           | بررسی حملات در محیط های هت نت ها مانند فروچاله ها و سیاه چاله ها و کرم چاله ها و اکار سرویس                                                                                                        |
| ۳۵      | Rahnavard, 2015                  | سیستم مدیریت دانش جهت پوشش فرآیند خلق، سازماندهی، اشاعه و کاربرد دانش                                                                                                                        | مطالعه کتابخانه ای           | سیستم مدیریت دانش پوشش فرایند خلق، جمع آوری، سازماندهی، اشاعه و کاربرد دانش در سازمان یا هنر خلق ارزش دارایی های نامشهود                                                                           |
| ۳۶      | Roohollah., 2015                 | حاکمیت اینترنت اشیاء                                                                                                                                                                         | مطالعه کتابخانه ای           | بررسی پیاده سازی فناوری اینترنت اشیاء و امنیت آن                                                                                                                                                   |
| ۳۷      | Arkian, 2015                     | امنیت و حریم خصوصی در اینترنت اشیاء                                                                                                                                                          | مقاله علمی ترویجی            | امنیت اینترنت اشیاء بعنوان چالش اساسی در زمینه توسعه فرآیند فوق                                                                                                                                    |
| ۳۸      | Alamr et al., 2018               | احراز هویت متقابل                                                                                                                                                                            | مجله علمی تحقیقاتی           | بکارگیری پروتکل احراز هویت متقابل RFID بر مبنای رمز نگاری منحنی بیضوی                                                                                                                              |
| ۳۹      | Kalra & Sood, 2015               | طرح امنیت با سرویس ابری                                                                                                                                                                      | مجله موبایل و سرویس های ابری | پروتکل احراز هویت متقابل با استفاده از رمز نگاری منحنی و کوکی HTTP                                                                                                                                 |
| ۴۰      | Khemissa & Tandjaoui, 2016       | یک طرح جدید احراز هویت سبک وزن در شبکه های بی سیم ناهمگن در زمینه اینترنت اشیاء                                                                                                              | مقاله سمپوزیوم مخابرات       | معرفی شبکه های حسگر بیسیم WSN بعنوان واقعی ترین و موثرترین کاربردهای شبکه اینترنت اشیاء                                                                                                            |

### گام پنجم: تجزیه و تحلیل یافته‌های کیفی

پژوهشگر در طول تجزیه و تحلیل، موضوعاتی را جستجو می کند که در میان مطالعه های موجود در فراترکیب پدیدار شده است. این مورد به عنوان ( بررسی موضوعی) شناخته می شود. به محض اینکه موضوع ها شناسایی و مشخص شد، بررسی کننده، طبقه بندی را شکل می دهد و طبقه بندی های مشابه و مربوط را در موضوعی قرار می دهد که آن را به بهترین گونه توصیف می کند. موضوع ها اساس و پایه ایجاد توضیحات، الگوها و نظریه ها یا فرضیات را ارائه می کند. در

این پژوهش، ابتدا تمام عوامل استخراج شده از مطالعه‌ها به عنوان شناسه در نظر گرفته، و سپس با در نظر گرفتن معنای هر یک از آنها، شناسه‌ها در مفهومی مشابه تعریف شده؛ سپس مفاهیم مشابه در مقولات تبیین کننده و دسته‌بندی گردید تا به این ترتیب محورهای تبیین کننده امنیت اینترنت اشیاء در مقوله‌های اصلی و فرعی پژوهش شناسایی شود. در پژوهش از فرآیند روش CASP یا Critical Appraisal Skills Program به معنای برنامه مهارت‌های ارزیابی حیاتی، ابزاری برای ارزیابی کیفیت مطالعات اولیه پژوهش‌های کیفی استفاده شده است.



نمودار ۳. الگوریتم خروجی کنترل کیفیت شاخص های پژوهش (Source:By author)

گام هفتم: در این مرحله از روش فراترکیب، یافته‌های مراحل قبل ارائه می‌شود. در ادامه به شناسایی شاخص‌های پژوهش پرداخته می‌شود. در این مرحله از کد گذاری، مقوله‌های اصلی و فرعی پژوهش مشخص شدند.

جدول ۳. نتایج حاصل از مطالعه و بررسی امنیت سایبری اینترنت اشیاء (Source:By author)

|                                         |                                      |                                      |
|-----------------------------------------|--------------------------------------|--------------------------------------|
| ۱- کنترل تهدید                          | مؤلفه‌های امنیت شبکه اینترنت         | مؤلفه‌های امنیت سایبری اینترنت اشیاء |
| ۲- کنترل دسترسی                         |                                      |                                      |
| ۳- امنیت شبکه فنی                       |                                      |                                      |
| ۴- امنیت شبکه فیزیکی                    |                                      |                                      |
| ۵- امنیت شبکه اداری                     |                                      |                                      |
| ۶- نرم افزار آنتی ویروس و آنتی بد افزار |                                      |                                      |
| ۷- حفاظت فایروال                        |                                      |                                      |
| ۸- شبکه خصوصی مجازی                     | مؤلفه‌های امنیت سایبری اینترنت اشیاء | مؤلفه‌های امنیت سایبری اینترنت اشیاء |
| ۹- امنیت API                            |                                      |                                      |
| ۱۰- رمز عبور قوی                        |                                      |                                      |
| ۱۱- ایجاد شبکه‌های مهمان                |                                      |                                      |
| ۱۲- بروز رسانی مداوم                    |                                      |                                      |
| ۱۳- بهره‌گیری از بلاکچین                |                                      |                                      |
| ۱۴- ارزیابی منظم دوره‌ای                |                                      |                                      |
| ۱۵- تحلیل پیشگیرانه                     |                                      |                                      |
| ۱۶- کنترل دسترسی به شبکه NAC            |                                      |                                      |



## بحث و نتیجه گیری

این تحقیق نشان می‌دهد که با پیشرفت فناوری اینترنت اشیا، خطرات امنیتی مرتبط با آن نیز افزایش می‌یابد. فرکانس فزاینده حملات سایبری که شامل بهره برداری از یک نوع معمولی است دستگاه اینترنت اشیا برای دسترسی و به خطر انداختن کل شبکه بر اهمیت امنیت اینترنت اشیا تأکید کرده است. اطمینان از ایمنی شبکه‌هایی که به دستگاه‌های اینترنت اشیا متکی هستند، تبدیل شده است. یک اولویت ضروری امنیت اینترنت اشیا طیف متنوعی از تکنیک‌ها، استراتژی‌ها، پروتکل‌ها و اقداماتی که با هدف به حداقل رساندن آسیب پذیری‌های رو به رشد ناشی از اینترنت اشیا به کسب و کارهای مدرن برای اطمینان از اینکه شبکه‌های اینترنت اشیا در برابر حملات احتمالی محافظت می‌شوند، بسیار مهم است که متخصصان علوم کامپیوتر/مهندسی، مانند محققان، دانشمندان، و دانشگاهیان، با آخرین راه حل‌های امنیتی اینترنت اشیا به روز باشند.

این مقاله مروری جامع از حیاتی‌ترین ملاحظات امنیتی مرتبط با اینترنت اشیا ارائه می‌دهد. شرکت‌های دارای اینترنت اشیا باید نظارت جامع را درک کرده و توسعه دهند. همچنین، ابزارهایی برای شناسایی سریع هرگونه فعالیت غیرعادی در شبکه‌های خود فراهم نمایند. این ابزار باید استفاده شود ابزارهای تشخیص پیشرفته با بهره‌برداری از فناوری‌های توانمند، مانند یادگیری ماشین و الگوریتم‌های هوش مصنوعی، برای تجزیه و تحلیل مجموعه داده‌های بزرگ تولید شده در طول عملیات عادی شبکه و هشدار به مدیران از انحراف از معیار، با اجازه دادن سازمان‌ها برای واکنش سریع به حوادث امنیتی و پیش بینی تهدیدات احتمالی قبل از وقوع، مکانیسم‌های دفاعی متمرکز بر لایه‌ای می‌توانند به طور قابل توجهی موارد آسیب‌های ناشی از حملات سایبری را به حداقل برسانند.

امنیت شبکه برای هر سازمانی که با داده‌ها و سیستم‌های شبکه کار می‌کند، باید اولویت بالایی داشته باشد. علاوه بر محافظت از دارایی‌ها و یکپارچگی داده‌ها در برابر سوء استفاده‌های خارجی نیز امنیت شبکه بسیار مهم است. امنیت شبکه همچنین می‌تواند ترافیک شبکه را به‌طور مؤثرتری مدیریت کند، عملکرد شبکه را بهبود بخشد و از اشتراک امن داده‌ها بین کارمندان و منابع داده اطمینان حاصل کند. ابزارها، برنامه‌ها و برنامه‌های کاربردی زیادی وجود دارند که می‌توانند به شما کمک کنند تا شبکه‌های خود را از حملات و خرابی‌های غیرضروری ایمن کنید. روش‌های امنیتی اینترنت اشیا بسته به کاربرد خاص اینترنت اشیا و جایگاه شما در اکوسیستم اینترنت اشیا متفاوت است. به عنوان مثال، تولیدکنندگان اینترنت اشیا - از تولیدکنندگان محصول گرفته تا شرکت‌های نیمه‌رسانا - باید از همان ابتدا بر روی ایجاد امنیت اینترنت IOT، ساخت سخت‌افزار، ساخت سخت‌افزار ایمن، اطمینان از ارتقای امن، ارائه به‌روزرسانی‌ها و صله‌های میان‌افزار و انجام تست‌های پویا تمرکز کنند. تمرکز یک توسعه‌دهنده برای ساخت یک اشیا هوشمند باید بر روی توسعه نرم‌افزار ایمن و یکپارچه‌سازی ایمن باشد. برای کسانی که سیستم‌های اینترنت اشیا را به کار می‌گیرند، امنیت سخت‌افزار و احراز هویت از اقدامات حیاتی هستند. به همین ترتیب، برای اپراتورها، به‌روز نگه‌داشتن سیستم‌ها، کاهش بدافزار، ممیزی، حفاظت از زیرساخت‌ها و حفاظت از اعتبارنامه‌ها در امنیت اینترنت اشیا از اقدامات کلیدی است. با این حال، با استقرار اینترنت اشیا، سنجیدن هزینه امنیت در برابر خطرات قبل از اجرا بسیار مهم است.

## مشارکت نویسندگان

تمام نویسندگان به نسبت سهم برابر در این پژوهش مشارکت داشته‌اند.

## تأیید اخلاقی

هیچ موضوع انسانی در این مقاله وجود ندارد و رضایت آگاهانه قابل اعمال نیست.

## تعارض منافع

هیچ گونه تعارض منافع توسط نویسندگان بیان نشده است.

## References

- Abbasi, M., Plaza-Hernandez, M., Prieto, J., & Corchado, J. M. (2022). Security in the Internet of Things Application Layer: Requirements, Threats, and Solutions. *IEEE Access*(10), 97197–97216.
- Agrawal, S., Das, M. L., & Lopez, J. (2019). Detection of Node Capture Attack in Wireless Sensor Networks. *IEEE Syst. J.*(13), 238–247.
- Alaba, F. A., Othman, M., Hashem, I. A., & Alotaibi, F. (2017). Internet of Things security: A survey. *J. Netw. Comput. Appl.*(88), 10–28.
- Alamr, A. A., Kausar, F., Kim, J., & Seo, C. (2018). A secure ECC-based RFID mutual authentication protocol for internet of things. *The Journal of Supercomputing*, 74, 4281-4294.
- Alharbi, I. A., Almalki, A. J., Alyami, M., Zou, C., & Solihin, Y. (2022). Profiling Attack on WiFi-based IoT Devices using an Eavesdropping of an Encrypted Data Frames. *Adv. Sci. Technol. Eng. Syst. J.*(7), 49–57.
- An, G. H., & Cho, T. H. (2022). Improving Sinkhole Attack Detection Rate through Knowledge-Based Specification Rule for a Sinkhole Attack Intrusion Detection Technique of IoT. *Int. J. Comput. Netw. Appl.*(9), 169.
- Arkian, H. (2015). Security and Privacy in the Internet of Things. *Bi-quarterly scientific-promotional journal, Herald of Security in the Space of Information Production and Exchange (AFTA)*, 4. [In Persian]
- Biplob, R. (2014). Scalable RFID security framework and protocol supporting Internet of Things. *Journal of Computer Networks*.
- Che, B., Liu, L., & Zhang, H. (2020). KNEMAG: Key Node Estimation Mechanism Based on Attack Graph for IoT Security. *J. Internet Things*(2), 145–162.
- Chenail, R. J. (2009). Bringing Method to the Madness: Sandelowski and Barroso's Handbook for Synthesizing Qualitative Research. *The Qualitative Report*, 13(4), 8-12. <https://doi.org/10.46743/2160-3715/2009.2820>
- Das, A., & Yashkova, O. (2022). Market Analysis Perspective: Worldwide Internet of Things. *Infrastructure and the Intelligent Edge. (IDC) from IDC: The Premier Global Market Intelligence Company*. <https://www.idc.com/etdoc.jsp?containerId=US49735922>
- Debroy, S., Samanta, P., & Bashir, A. (2019). Chatterjee, M. SpEED-IoT: Spectrum aware energy efficient routing for device-to-device IoT communication. *Future Gener. Comput. Syst.*(93), 833–848.
- Fei, H. (2016). Security and Privacy in Internet of Things (IoTs) Models. *Algorithms, and Implementations*, 144.
- Gholichi, H. (2016). Security Threats on the Internet and Methods of Counteracting Them. *Inajafy*. [In Persian]

- Hung, C. W., & Hsu, W. T. (2018). Power Consumption and Calculation Requirement Analysis of AES for WSN IoT. *Sensors*(18), 1675.
- Hussein, N., & Nhlabatsi, A. (2022). Living in the Dark: MQTT-Based Exploitation of IoT Security Vulnerabilities in ZigBee Networks for Smart Lighting Control. *IoT*(3), 450–472.
- Kalra, S., & Sood, S. K. (2015). Secure authentication scheme for IoT and cloud servers. *Pervasive and Mobile computing*, 24, 210-223.
- Kareem, M. K., Aborisade, O. D., Onashoga, S. A., Sutikno, T., & Olayiwola, O. M. (2023). Efficient model for detecting application layer distributed denial of service attacks. *Bull. Electr. Eng. Inform*(12), 441–450.
- Khemissa, H., & Tandjaoui, D. (2016). A novel lightweight authentication scheme for heterogeneous wireless sensor networks in the context of Internet of Things. *2016 Wireless Telecommunications Symposium (WTS)*, 1-6.
- Kim, M., & Suh, T. (2021). Eavesdropping Vulnerability and Countermeasure in Infrared Communication for IoT Devices. *Sensors*(21), 8207.
- Lu, Y., & Da, X. L. (2103). Internet of Things cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2), 15.
- Matheu, S., Hernandez-Ramos, J., Skarmeta, A., & Baldini, G. (2020). A survey of cybersecurity certification for the internet of things. *ACM Computing Surveys (CSUR)*, 53(6), 1-36.
- Moaveni, M. (2016). How to secure devices connected to the Internet and deal with threats. *Moaveni*. [In Persian]
- Nam, D., & Sukhomlin, V. (2023). On cybersecurity of the Internet of Things systems. *International Journal of Open Information Technologies*, 11(2), 85-97.
- Pappalardo, M., & Virdis, A. (2022). Mingozi, E. An Edge-Based LWM2M Proxy for Device Management to Efficiently Support QoS-Aware IoT Services. *IoT*(3), 169–190.
- Park, J. H., Kim, H. S., & Kim, W. T. (2018). M-MQTT: An Efficient MQTT Based on SDN Multicast for Massive IoT Communications. *Sensors*(18), 3071.
- Rahnavard, M. (2015). Knowledge Management System to Cover the Process of Creating, Organizing, Dissemination, and Applying Knowledge in Creating a Value. [In Persian]
- Roohollah, G. (2015). Internet of Things Governance: Experiences of Countries Around the World and Iran's Roadmap. *Communications and Information Technology Research Institute. ICT Policy and Strategic Management Research Institute. ICT Business Development and Entrepreneurship Group*. [In Persian]
- Scott, M. (2017). How to secure your IoT devices from botnets and other threats. *Techrepublic*.
- Seoane, V., Garcia-Rubio, C., Almenares, F., & Campo, C. (2022). Performance evaluation of CoAP and MQTT with security support for IoT.
- Shiranzaei, A. (2018). Khan, R.Z. An Approach to Discover the Sinkhole and Selective Forwarding Attack in IoT. *J. Inf. Secur. Res.*(9), 107.
- Sreekanth, M., & Jeyachitra, R. (2022). Implementation of area-efficient AES using FPGA for IOT applications. *Int. J. Embed. Syst.*(15), 354.
- Tsai, W. C., Tsai, T. H., Wang, T. J., & Chiang, M. L. (2022). Automatic Key Update Mechanism for Lightweight M2M Communication and Enhancement of IoT Security: A Case Study of CoAP Using Libcoap Library. *Sensors*(22), 340.
- Vaclavova, A., Strelec, P., Horak, T., Kebisek, M., Tanuska, P., & Huraj, L. (2022). Proposal for an IIoT Device Solution According to Industry 4.0 Concept. *Sensors*(22), 325.
- Venkatraman, S., & Overmars, A. (2019). New Method of Prime Factorisation-Based Attacks on RSA Authentication in IoT. *Cryptography*(3), 20.
- Wani, A. R., Gupta, S. K., Khanam, Z., Rashid, M., Alshamrani, S. S., & Baz, M. (2022). A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme. *IET Intell. Transp. Syst.*, 1-19.
- Yoon, J. (2020). Deep-learning approach to attack handling of IoT devices using IoT-enabled network services. *Internet Things*(11), 100241.

- Yu, H., & Park, Y. (2021). Design and implementation of IIoT edge device for collecting heterogeneous machine data. *J. Internet Electron. Commer. Resarch*(21), 23–32.
- Zeng, J. Y., Chang, L. E., Cho, H. H., Chen, C. Y., Chao, H. C., & Yeh, K. H. (2022). Using Poisson Distribution to Enhance CNN-based NB-IoT LDoS Attack Detection. *In Proceedings of the 2022 IEEE Conference on Dependable and Secure Computing (DSC)*, Edinburgh, UK, 1–7.

