International Journal of Communication and Information Technology

E-ISSN: 2707-6628
P-ISSN: 2707-661X
www.computersciencejournals.com/ijcit
IJCIT 2024; 5(1): 01-05
Received: 04-12-2023
Accepted: 02-01-2024

U Satchithanantham
Assistant Professor, Department of Computer Science with Data Analytics, Ajk College of Arts and Science, Coimbatore, Tamil Nadu, India

Corresponding Author:
U Satchithanantham
Assistant Professor, Department of Computer Science with Data Analytics, Ajk College of Arts and Science, Coimbatore, Tamil Nadu, India

Significant Security Challenges in IOT Analytics

U Satchithanantham

DOI: https://doi.org/10.33545/2707661X.2024.v5.i1a.71

Abstract
The Internet of Things (IoT) is a community of bodily devices, vehicles, domestic appliances, and other items embedded with sensors, software, and connectivity that enable them to connect and exchange data with other devices and systems over the Internet. The IoT has been growing in importance in various industries, including healthcare, manufacturing, transportation, and agriculture, among others. Data analytics, or truly IoT analytics, is the act of studying statistics generated and collected from IoT devices by utilizing a specific set of data analytics tools and techniques. The actual concept in the back of IoT Data analytics is to show great portions of unstructured information from diverse gadgets and sensors within the Internet of Things ecosystem, which is heterogeneous, into valuable and actionable insights for driving sound business decision-making and further data analysis. Furthermore, IoT analytics enable identifying the patterns in data sets, including both current states And ancient data, that could be utilized to make predictions and modifications approximately destiny events. By analyzing this data, businesses can gain valuable insights that can help them improve operational efficiency, reduce costs, and enhance the customer experience. With the increasing adoption of IoT devices across various industries, The amount of data generated is growing exponentially. Data analytics can help organizations to unlock this value and make data-driven decisions that can have a significant impact on their business. It is crucial for related gadgets to paintings collectively for maximum IoT use cases, however this technique raises security issues. The universal safety profile is most effective as powerful because the weakest device. If the security is on a specific vendor's outdoor sensor is weak and the sensor is connected to other devices, the likelihood of indirect critical impact is high. Attackers can compromise the sensor, modify its data, or exploit the connection to other devices to cause damage.

Keyword: Healthcare, ecosystem, predictions, unlock, security, attackers, damage

Introduction
Internet of Things (IoT) data analytics, or simply IoT analytics is the act of analyzing data generated and collected from IoT devices by utilizing a specific set of data analytics tools and techniques. The true idea behind IoT data analytics is to turn vast quantities of unstructured data from various devices and sensors within the Internet of Things ecosystem, which is heterogeneous, into valuable and actionable insights for driving sound business decision-making and further data analysis. Furthermore, IoT analytics allows figuring out the styles in data sets, including both current states and historical data, which can be utilized to make predictions and adjustments about future events. There is no doubt that the deployment of connected devices and sensors has increased exponentially in various industries in recent years, which has driven the development of IoT data analytics to a great extent. IoT analytics is being broadly utilized in diverse industries starting from healthcare, retail, and e Commerce to manufacturing, transportation, and more.

Different Types of Iot Analytics
As IoT analytics are achieved to collect insights that serve specific purposes, it could be damaged down into 4 number one types.

Descriptive Analytics
Descriptive IoT analytics mainly focus on what happened in the past. The ancient facts gathered from gadgets are processed and analyzed to generate a record that describes what took place, while it occurred, and the way regularly it did. This sort of IoT evaluation is beneficial for imparting solutions to particular questions on the conduct of factors or humans and also can be used to come across any anomalies.

Diagnostic Analytics
Different from descriptive IoT analytics, diagnostic analytics pass one step in addition to reply the query of why something took place via way of means of drilling down into the information to discover the basis cause of a specific issue. Diagnostic analytics employ strategies like statistics mining and statistical evaluation to discover hidden styles and relationships in statistics which can provide actionable insights into the reasons of specific problems.

Predictive Analytics
As its name suggests, predictive IoT analytics is used to predict future events by analyzing historical data and trends. This type of analytics makes use of various statistical and machine learning algorithms to build models that can be used for making predictions about future events. This form of analytics performs a considerable position in helping commercial enterprise selections associated with stock management, call for forecasting, etc.

Prescriptive Analytics
Prescriptive IoT analytics is the most advanced type of IoT analytics that not only predicts what will happen in the future but also provides recommendations on what should be done to achieve the desired business outcomes. This type of analytics makes use of optimization algorithms to identify the best course of action that should be taken to achieve a specific goal

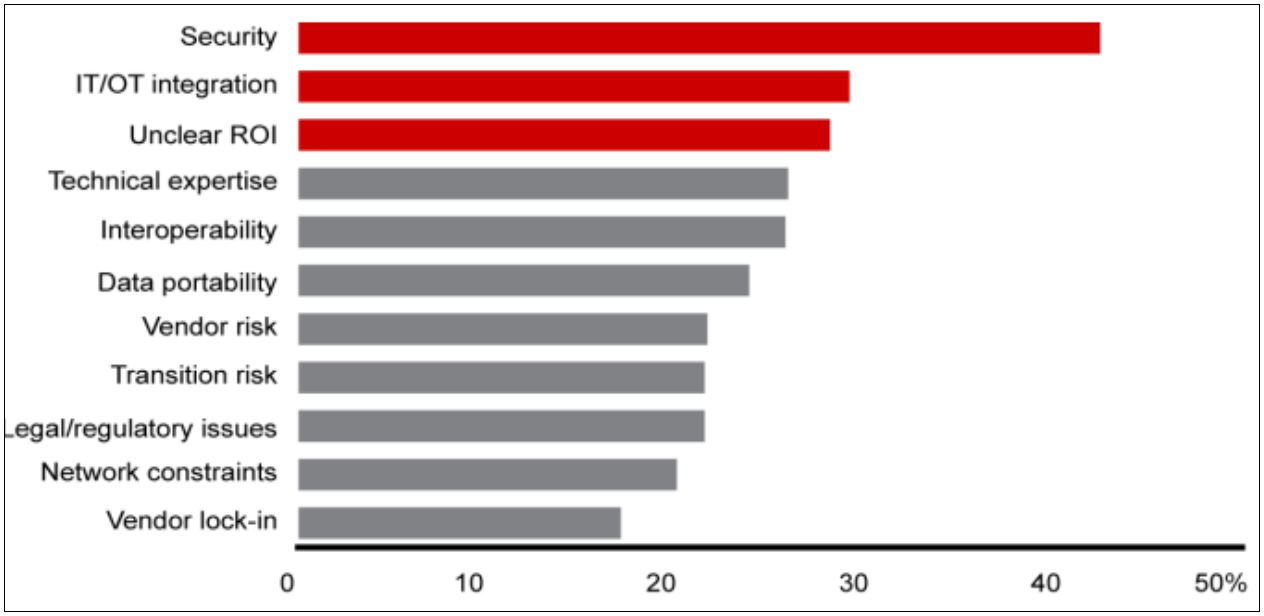
Use cases of IoT Analytics
IoT analytics can assist optimize advertising and marketing and income for groups promoting big portions of bodily items:

Forecasting customer needs
Helps examine purchaser traits and desires primarily based totally on product critiques and usage, assume destiny purchases, and assists with the improvement of consumable resupply models.

Helps deliver new services
Aggregates records from number one reasserts to carry out evaluation and make predictions.

Flexible pricing and billing
Captures pertinent data from sources, helps create outcome-based subscription and pricing models.

4. What is IoT Security
IoT safety is an umbrella time period that covers the strategies, tools, processes, systems, and strategies used to shield all factors of the net of things. Included in IoT protection is the safety of the bodily components, applications, data, and community connections to make sure the availability, integrity, and confidentiality of IoT ecosystems. Security demanding situations abound, due to the excessive extent of flaws frequently determined in IoT systems. IoT safety vulnerabilities are discovered in the whole thing from motors and clever grids to watches and clever domestic devices.
For example, researchers determined webcams that would be effortlessly hacked to advantage get admission to to networks and smart watches containing protection vulnerabilities that allowed hackers to tune the wearer's vicinity and eavesdrop on conversations. As stated earlier, IoT gadgets generally pop out of the container with primary safety, making them an excellent goal for assault and a critical safety weak point for his or her owners.



Sources: Bain IoT customer survey, 2016 (n=533); Bain IoT) survey, 2018 (n=627); market participant interviews

Fig 1: Percentage of respondents (top three barriers)

Some not unusual place safety demanding situations for IoT gadgets include
Weak Authentication
IoT gadgets are infamous for his or her use of susceptible and default passwords. Several huge botnets, together with Mirai, inflamed many gadgets genuinely via way of means of logging in the use of default and hardcoded passwords.

Data Encryption
IoT devices commonly collect large amounts of sensitive data, but they don't always protect it properly.
For example, IoT gadgets often fail to encrypt records saved

on gadgets or travelling over the network.

Vulnerable Software
IoT tool creators do now no longer constantly comply with improvement safety nice practices, inclusive of the usage of authentic and up to date libraries. These problems are exacerbated via way of means of the truth that IoT gadgets are regularly hard to patch, leaving vulnerabilities uncovered for exploitation.

Insecure Protocols
IoT gadgets frequently use insecure community interfaces and protocols. For example, a few IoT gadgets permit connections through Telnet, which exposes credentials and different information in plaintext at the network.

Lack of Standardization
One of the primary individuals to vulnerable IoT protection is the shortage of protection requirements and requirements. For IoT devices, maximum protection requirements are non-compulsory recommendations, in the event that they exist at all. The bad kingdom of IoT protection affects each the tool proprietors and others. IoT gadgets may be exploited to leak data, furnish unauthorized access, or carry out numerous assaults in opposition to different systems.

IoT security best practices
Some first-rate practices for handling an organization's publicity to IoT safety dangers encompass the following:

Device Discovery and Risk Analysis
IT groups can be blind to the lifestyles of IoT gadgets linked to company networks. Automated tool discovery can assist to discover unknown IoT gadgets and check the ability safety dangers that they pose to the organization.

Zero-Trust Network Access (ZTNA)
IoT gadgets may be used as a get admission to factor via way of means of cybercriminals who then pass laterally via an organization's systems. ZTNA facilitates to phase IoT gadgets from the relaxation of the community and bounds their get admission to, lowering their potential to get admission to touchy records and different systems

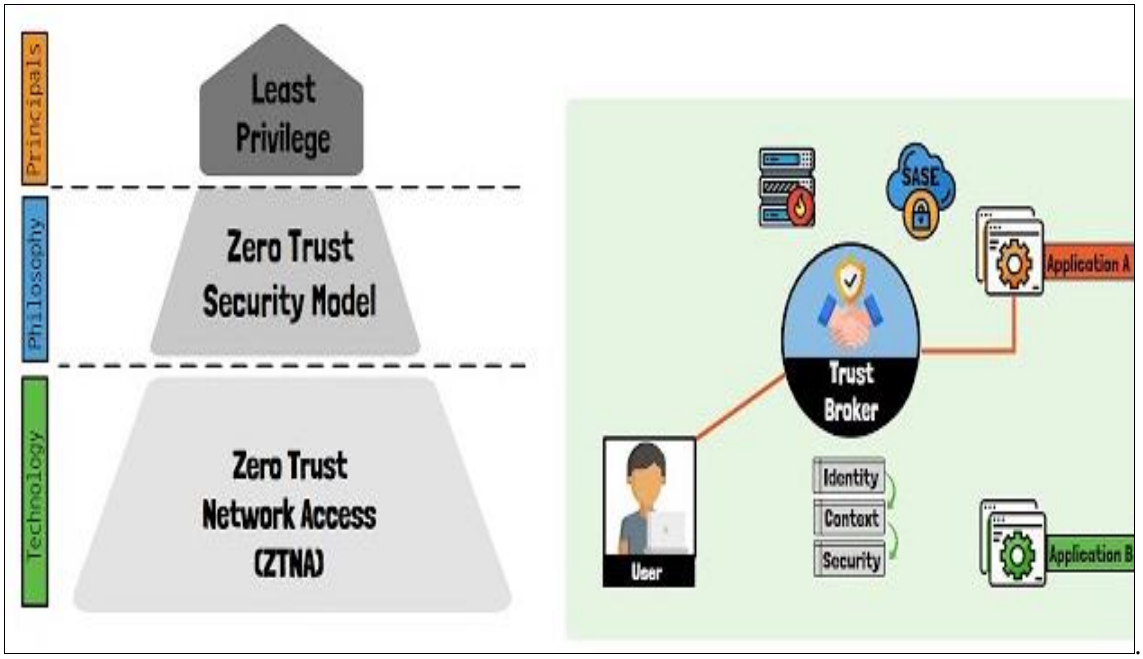


Fig 2: Show Least Privilege, Zero Trust Security Model and Zero Trust Network Access (ZTNA)

IoT Threat Prevention
IoT gadgets can comprise exploitable vulnerabilities, however conventional endpoint protection answers regularly do now no longer paintings on those gadgets (e.g., useful resource constraints, numerous ecosystems, specialised functionality, lack of user interfaces and more). Also, a few IoT structures aren't or can't be up to date via way of means of their owners.
IoT hazard prevention answers assist to save you attackers from exploiting vulnerabilities in those devices.
Specific functions required for securing IoT gadgets encompass the following:

- API security.
- Broader and deep IoT device inventory.
- Continuous software updates.
- DNS filtering.
- Education and training staff, vendors, and partners.
- Encryption for data at rest and in transit.
- Honeypot decoy programs.
- Multi-factor authentication.
- Network security.
- Network traffic monitoring analysis.
- Password management.
- Patch management.
- Security gateways.
- Unauthorized IoT device scans.

Most popular encryption algorithms in IoT
Data Encryption Standard (DES) and Triple-DES
Both are the Symmetric encryption algorithms in which DES is the oldest and keystone of the cryptography, now phased out (because of low encryption key). The Triple-DES overcomes all DES challenges, consisting of prone meet-in-the-center attacks, applies 3 56-bit keys to each

information block, and provides the overall key period as much as 168-bit.

However, there's the case of a mid-degree vulnerability that depreciates its protection degree to a 112-bit key. Due to this, it's far phasing out (changed with the aid of using AES). But a few IoT merchandise and economic offerings nevertheless put it to use due to its dependability, compatibility, and flexibility.

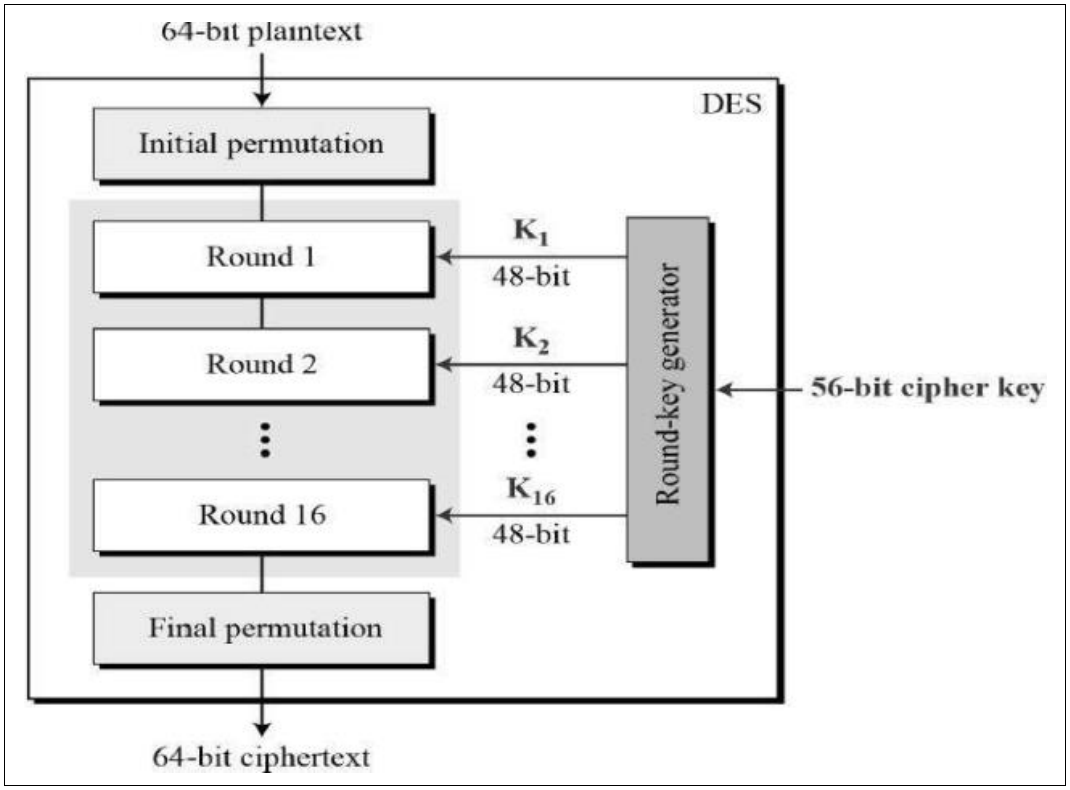


Fig 3: Show round-key generator

Advanced Encryption Standard (AES)

It is the maximum famous and sturdy symmetric encryption algorithm, which matches on block ciphers from fundamental 128 to heavy-obligation 192 and 256-bit keys.

It is unbreakable (due to longer key length) and immune to cyber-attacks except for brute force. Also, it is the futuristic "best-fit standard application" for the private sector. Both are the symmetric encryption algorithms wherein DES is the oldest and keystone of the cryptography, now phased out (due to low encryption key). Due to this, it is phasing out (replaced by AES). But some IoT products and financial services still utilize it because of its dependability, compatibility, and flexibility.

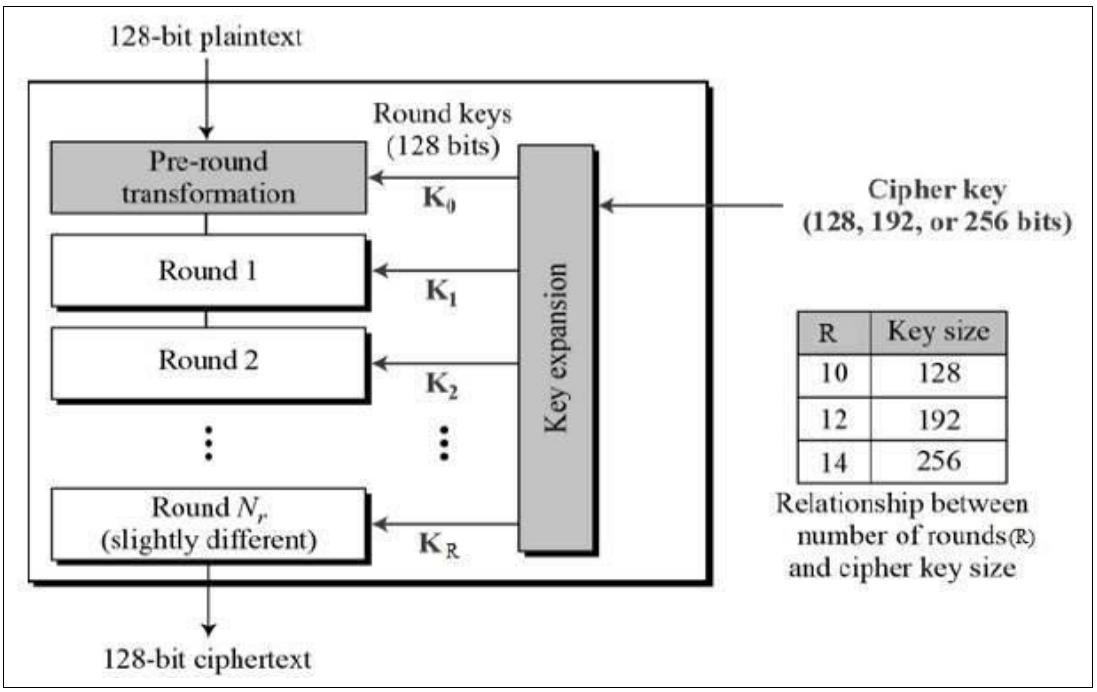


Fig 3: Show Relationship between number of rounds (R) and cipher key size

Conclusion

The main emphasis of this paper was to highlight major security issues of IoT analytics particularly, focusing the security attacks and their countermeasures. Due to loss of safety mechanism in IoT gadgets, many IoT gadgets grow to be gentle objectives or even this isn't with inside the victim's expertise of being infected. In this paper, the safety necessities are mentioned including confidentiality, integrity, and authentication, etc. Considering the significance of safety in IoT applications, it's far surely essential to put in safety mechanism in IoT gadgets and verbal exchange networks. Moreover, to protect from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not used may decrease the chances of security attacks. Moreover, it's far crucial to have a look at distinctive safety protocols utilized in IoT gadgets and networks.

References

1. Kumar JS, Patel DR. A survey on internet of things: Security and privacy issues. Int J Comput Appl. 2014;90(11):1-9.
2. Abomhara M, Køien GM. Security and privacy in the internet of things: Current status and open issues. In: Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE; c2014. p. 1-8.
3. Chen S, Xu H, Liu D, Hu B, Wang H. A vision of iot: Applications, challenges, and opportunities with china perspective. IEEE Internet of Things J. 2014;1(4):349-59.
4. Atzori L, Iera A, Morabito G. The internet of things: A survey. Comput Netw. 2010;54(15):2787-805.
5. Hossain MM, Fotouhi M, Hasan R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In: Services (SERVICES), 2015 IEEE World Congress on. IEEE; c2015. p. 21-8.
6. Xu L, He W, Li S. Internet of things in industries: A survey. IEEE Trans Ind Inform. 2014;10(4):2233-43.
7. Tarouco LMR, Bertholdo LM, Granville LZ, Arbiza LMR, Carbone F, Marotta M, *et al*. Internet of things in healthcare: Interoperability and security issues. In: Communications (ICC), IEEE International Conference on. IEEE; c2012. p. 6121-5.
8. Mohan A. Cyber security for personal medical devices internet of things. In: Distributed Computing in Sensor Systems (DCOSS), IEEE International Conference on. IEEE; c2014, p. 372-4.
9. Yoon S, Park H, Yoo HS. Security issues on smarthome in iot environment. In: Computer Science and its Applications. Springer; c2015, p. 691-6.
10. Weber RH. Internet of things–new security and privacy challenges. Comput Law Security Rev. 2010;26(1):23-30.
11. Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the internet of things (IoT). In: International Conference on Network Security and Applications. Springer; c2010. 420-9.
12. Hwang YH. IoT security & privacy: Threats and challenges. In: Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security. ACM; c2015, 1-1.
13. Qureshi MA, Aziz A, Ahmed B, Khalid A, Munir H. Comparative analysis and implementation of efficient digital image watermarking schemes. Int J Comput Electr Eng. 2012;4(4):558.