EDUZONE: International Peer Reviewed/Refereed Multidisciplinary Journal (EIPRMJ), ISSN: 2319-5045
Volume 11, Issue 2, July-December, 2022, Available online at: www.eduzonejournal.com

IoT: Emerging technologies-challenges and countermeasures

Vibhuti Mishra

Gyan Jyoti Institute, India

ABSTRACT

The primary challenge facing the Internet of Things (IoT) is security. Due to the sheer number and diversity of IoT devices, devices may be vulnerable to a range of cyber-attacks. This includes man-in-the-middle attacks, in which unauthorized devices can intercept communications, as well as malicious code injection attacks, in which malicious code is inserted into a device's firmware or software. These threats can lead to a range of serious issues, including financial losses, confidential data disclosure, and the disruption of critical services.In order to address the security challenges posed by IoT, a number of measures can be taken. These include the use of strong authentication systems, encryption measures, and secure protocols and development guidelines. Additionally, organizations should set up a comprehensive security policy and regularly assess the security of their IoT devices. Furthermore, network segmentation can be used to minimize the risks posed by malicious actors to connected systems, and data must be securely transmitted and stored. Finally, organizations should conduct regular testing of their systems and incorporate a proactive security monitoring system.

Keywords: IoT, Machine Learning, Blockchain, Security Threats, Security Solutions.

INTRODUCTION

The internet of things (IoT) is a network of physical objects that are connected to the internet and are able to collect, share and exchange data. As the number of connected devices and sensors increases exponentially, so does the amount of data being generated, creating an immense amount of opportunities for businesses and organizations, but also a number of challenges and potential risks that must be addressed [1].The most prominent challenge in the field of IoT is the massive amount of data generated. As such, the traditional storage and data analysis approaches used in the past may not be suitable for such large datasets. Therefore, organizations need to invest in scalable storage solutions that are capable of handling high volumes of data. Organizations also need to develop new and more effective ways of analyzing and interpreting such large amounts of data in real-time [2].

Another challenge associated with IoT is the issue of security and privacy. As IoT networks are made up of numerous devices and sensors, all of which are connected to the internet, they are vulnerable to cyberattacks [3]. Therefore, organizations must ensure that they put adequate security measures in place in order to protect their IoT networks. This includes investing in secure networking hardware, encrypting data sent across the network and regularly monitoring the network for suspicious activity.The third challenge associated with IoT is the complication of managing large numbers of interconnected devices. This can be a difficult task, especially when the number of connected devices increases exponentially. As such, organizations need to develop effective strategies and procedures for efficiently managing large numbers of interconnected devices [4].

One potential countermeasure for addressing the challenges posed by IoT is the implementation of cloud computing solutions. Cloud computing solutions can help to reduce the complexity of managing large numbers of interconnected devices, as well as providing scalability and cost-effectiveness for data storage and analysis [5]. Additionally, cloud computing solutions can also provide better security for IoT networks, as data can be stored and encrypted in the cloud, making it more difficult for attackers to gain access to the data.Overall, organizations looking to capitalize on the opportunities offered by the internet of things need to be aware of the various challenges associated with it, including the complexity associated with managing large numbers of interconnected devices, the massive amount of data generated, and the security and privacy issues associated with IoT networks [6]. By investing in secure networking hardware, employing cloud-based solutions and encrypting data sent across their networks, organizations can ensure that their IoT networks are safe and secure and can help them to better take advantage of the opportunities offered by the internet of things.In addition to the challenges and countermeasures outlined above, organizations should also focus on developing effective standards that all IoT devices should adhere to in order to ensure interoperability between different devices [7]. This will help to make sure that data is exchanged without any errors or security risks. Additionally, organizations should also look into utilizing advanced technologies, such as blockchain, to further secure and protect their data, while also providing improved analytics. Finally, organizations should focus on developing effective and secure protocols that can be used to communicate between IoT devices when exchanging data. By doing

so, organizations can ensure that data is kept secure, while also making sure that all devices connected to the network are performing their intended tasks securely [8].

Security Risks related to Machine Learning for IoT

Machine learning can present some unique security risks for Internet of Things (IoT) devices. Generally, machine learning algorithms require access to large amounts of data to learn from in order to create insights, which can expose an IoT system to malicious access or attack [9]. If an IoT-based machine learning model is not robust and fails to detect malicious input or output, attackers could take advantage of the vulnerabilities.In addition, machine learning models that use IoT data must be properly secured to prevent malicious actors from extracting any future insights generated by the model. If the models are not sufficiently secured, attackers could use the data to gain insight into sensitive systems and even manipulate the model to generate their own results [10].

AI-based systems can also be vulnerable to adversarial perturbations, which are maliciously generated inputs or data points that can destabilize a model due to its unexpected nature. This can lead to incorrect or dangerous decisions based on the model's incorrect insights, or even shutdown the system.Finally, IoT machine learning models may be vulnerable to different types of inference attacks, which are attempts to extract confidential information about data used for training the model [11]. This can be done, for example, through analyzing the responses of the model when presented with different inputs. This type of attack could potentially allow malicious actors to gain insight into the system's data, even though the model has not been shared.Overall, the potential risks of using machine learning for IoT-based systems can be substantial, and organizations should take the necessary steps to ensure robust security protocols in order to prevent any potential malicious use of their models [12].

In addition to the aforementioned security risks, IoT machine learning models can also be subject to model inversion attacks, which are attempts by attackers to obtain information about the training data of a model by reverse-engineering the model. This can involve analyzing the structure or weights of a model to obtain information or insights into what types of data it was trained on [13].Another potential security risk with machine learning for IoT-based systems is the increase in attack surface related to using Machine Learning-as-a-service (MLaaS). With MLaaS, organizations can outsource all the components of a machine learning model, from data labeling to training and hosting, to an external provider. This process can make an organization's system more vulnerable to attack if the provider does not take sufficient security measures to protect the system from malicious actors [14].Finally, implementing machine learning models into an IoT system can also create a scenario where machine learning models and neural networks are more naïve to attacks because of the lack of security protocols and attack detection measures. This can potentially lead to attacks being successful against an IoT system with a machine learning model even if the attacks wouldn't have been successful against a system not utilizing machine learning [15].

Security Risks related to Blockchain Technology for IoT

Blockchain technology has become increasingly popular due to its decentralized nature and increased security. This technology is often used to secure data and transactions and can provide a layer of trust and security in areas like the Internet of Things (IoT) [16]. However, like any other technology, blockchain technology comes with its own set of security risks.One of the biggest risks is the risk of 51% attack. This kind of attack is most likely to occur in a distributed network of blockchain nodes, where more than half of them are compromised. An attacker can then gain control of the entire chain and reverse or delete transactions [17].

Another risk related to blockchain and IoT is the potential for manipulation of transaction data. This could be done through someone finding a vulnerability in the code that allows the attacker to manipulate the data stored on the chain. This could lead to issues of trust, which is one of the primary benefits of using blockchain technology [18].The security of any network ultimately depends on the security of the underlying hardware and software. Therefore, issues in the hardware or software used to support the blockchain can also create security risks. This includes malicious actors targeting hardware devices on the network and any other parts of the system that could be vulnerable [19].

Finally, fraud is another risk related to blockchain and IoT. For example, someone can create a fraudulent transaction on the blockchain, making it difficult to detect and resolve. This could result in an inability to access funds or other financial losses [20].Overall, blockchain technology can provide greater security for many areas, including the IoT. However, like any other technology, there are still security risks associated with it. Therefore, it is important to understand and address these risks in order to protect the data and transactions that occur on the blockchain [21].

Security Solutions for IoT

The security of an Internet of Things (IoT) system depends on the particular system and its components. However, most of the proposed security solutions for IoT systems fall into a few different categories [22].

One of the most important security solutions for IoT systems is the use of authentication and encryption. Authentication ensures that requests from specific, trusted devices or users are handled, and encryption ensures that data shared between devices is kept secure, even if it is intercepted. Implementing strong authentication methods such as two-factor authentication and using encryption standards such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL) can go a long way in protecting the sensitive data in an IoT system [23].

Another important security measure for IoT systems is to install firewalls and use Network Access Control (NAC) systems. Firewalls and NAC systems can inspect IoT traffic, detect malicious traffic and block it before it can reach its intended target. Having a monitoring system in place is also important. This can involve using technologies such as Intrusion Prevention and Detection System (IPS/IDS) or Security Event and Incident Management (SEIM) systems. These systems can detect and respond to malicious activity within an IoT system.Finally, it is important to have periodic security audits to ensure that the security measures for an IoT system are always up to date. Security audits can include vulnerability scanning, system patching, and penetration testing. These security audits can help identify security weaknesses and allow for the necessary steps to be taken in order to fix any identified issues.Overall, implementing the mentioned security solutions for IoT systems, or developing custom solutions, can drastically increase the security of an IoT system, and help protect it from malicious actors [24].

I. Authentication and Encryption

One of the most important security solutions for IoT systems is the use of authentication and encryption. Authentication ensures that requests from specific, trusted devices or users are handled, and encryption ensures that data shared between devices is kept secure, even if it is intercepted. Implementing strong authentication methods such as two-factor authentication and using encryption standards such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL) can go a long way in protecting the sensitive data in an IoT system [25].

II. Firewalls and Network Access Control

Another important security measure for IoT systems is to install firewalls and use Network Access Control (NAC) systems. Firewalls and NAC systems can inspect IoT traffic, detect malicious traffic and block it before it can reach its intended target.

III. Monitoring

Having a monitoring system in place is also important. This can involve using technologies such as Intrusion Prevention and Detection System (IPS/IDS) or Security Event and Incident Management (SEIM) systems. These systems can detect and respond to malicious activity within an IoT system [26].

IV. Auditing

Finally, it is important to have periodic security audits to ensure that the security measures for an IoT system are always up to date. Security audits can include vulnerability scanning, system patching, and penetration testing. These security audits can help identify security weaknesses, and allow for the necessary steps to be taken in order to fix any identified issues.

In addition to the above security solutions for IoT systems, there are a few other measures that can be taken to protect an IoT system.One of these measures is to use technology that is specifically designed to be secure and reliable. This can include using operating systems such as Linux that are built with security in mind, as well as hardware components such as microcontrollers with hardware-based authentication to further secure communications[27-31]. Additionally, it is important to ensure that any devices used in an IoT system are properly updated and patched to prevent exploits of known vulnerabilities.Another measure that can be taken is to use virtualization technologies such as virtualized networks, containers, and operating systems. This can help add an extra layer of security by isolating resources and preventing malicious actors from gaining access to sensitive data. Additionally, segmenting networks in an IoT system can help ensure that any malicious actors are unable to move through the system without being detected. Having a secure platform for deploying IoT services and applications can also help keep systems safe.Overall, by implementing the mentioned security solutions for IoT systems and taking additional measures, it is possible to greatly increase the security of an IoT system and help protect it from malicious actors [32-35].

CONCLUSION

To ensure a truly secure and safe IoT system, companies need to consider all measures from authentication and encryption to firewalls, NAC systems, monitoring systems, security audits, secure technology, and virtualization. Authentication measures like multi-factor authentication and two-factor authentication should be used to protect user accounts. Encryption measures such as Transport Layer Security (TLS) should be used to keep data secure. Firewalls should be used to defend against malicious actors, by blocking access to unauthorized users and networks. NAC systems should also be used to segment networks and audit user data. A comprehensive monitoring system should be

used to detect and alert on potential security threats or breaches. Security audits should be conducted on a regular basis to make sure the system is operating in accordance with company policies and procedures. In addition, secure technology and virtualization should be used to isolate and secure the IoT system from the wider, unsecured network. By taking all of these measures into account, it is possible to secure and protect an IoT system and all its components from malicious intrusion.

REFERENCES

[1]. Rathore, R.S., Sangwan, S., Kaiwartya, O. and Aggarwal, G., 2021. Green communication for next-generation wireless systems: optimization strategies, challenges, solutions, and future aspects. *Wireless Communications and Mobile Computing*, *2021*, pp.1-38.

[2]. Mohanta, B.K., Jena, D., Satapathy, U. and Patnaik, S., 2020. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*, p.100227.

[3]. Balaji, S., Nathani, K. and Santhakumar, R., 2019. IoT technology, applications and challenges: a contemporary survey. *Wireless personal communications*, *108*, pp.363-388.

[4]. Rathore, R.S., Sangwan, S., Mazumdar, S., Kaiwartya, O., Adhikari, K., Kharel, R. and Song, H., 2020. W-GUN: Whale optimization for energy and delay-centric green underwater networks. *Sensors*, *20*(5), p.1377.

[5]. Singh, U.P. and Rathore, R.S., 2013. Distributed Hierarchical Group Key Management using Elliptic Curve and Hash Function. *International Journal of Computer Applications*, *61*(19).

[6]. Singh, U.P. and Rathore, R.S., 2012. An efficient distributed group key management using hierarchical approach with ECDH and symmetric algorithm. *J. Comput. Eng. Intel. Syst*, *3*(7), pp.32-41.

[7]. Abdulkarem, M., Samsudin, K., Rokhani, F.Z. and A Rasid, M.F., 2020. Wireless sensor network for structural health monitoring: A contemporary review of technologies, challenges, and future direction. *Structural Health Monitoring*, *19*(3), pp.693-735.

[8]. Rathore, R.S., Sangwan, S. and Kaiwartya, O., 2021. Towards Trusted Green Computing for Wireless Sensor Networks: Multi Metric Optimization Approach. *Adhoc& Sensor Wireless Networks*, *49*.

[9]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Routing Protocol for MANETs: A Survey. *IUP Journal of Computer Sciences*, *4*(3).

[10]. Bali, V. and Rathore, R.S., 2010. A NEW HIERARCHICAL TRANSACTION MODEL FOR MOBILE ADHOC NETWORK ENVIRONMENT. *International Journal on Computer Science and Engineering*, *2*(3).

[11]. Singhal, S. and Rathore, R.S., 2015. Detailed Review of Image Based Steganographic Techniques. *IJCST*, *6*, pp.93-95.

[12]. Kumar, V. and Rathore, R.S., 2018, October. Security issues with virtualization in cloud computing. In *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 487-491). IEEE.

[13]. Rathore, R.S., Sangwan, S., Prakash, S., Adhikari, K., Kharel, R. and Cao, Y., 2020. Hybrid WGWO: whale grey wolf optimization-based novel energy-efficient clustering for EH-WSNs. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), pp.1-28.

[14]. Sharma, P. and Rathore, R.S., 2015. Three Level Cloud Computing Security Model. *International Journal of Computer Applications*, *119*(2).

[15]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, August. Information Technology Architectures for Grid Computing and Applications. In *2009 Fourth International Multi-Conference on Computing in the Global Information Technology* (pp. 52-56). IEEE.

[16]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Performance analysis of priority scheme in ATM network. *International Journal of Computer Applications*, *1*(13), pp.26-31.

[17]. Rathore, R.S., Sangwan, S., Adhikari, K. and Kharel, R., 2020. Modified echo state network enabled dynamic duty cycle for optimal opportunistic routing in EH-WSNs. *Electronics*, *9*(1), p.98.

[18]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, December. A Framework to Provide a Bidirectional Abstraction of the Asymmetric Network to Routing Protocols. In *2009 Second International Conference on Emerging Trends in Engineering & Technology* (pp. 1143-1150). IEEE.

[19]. Dixit, R., Gupta, S., Rathore, R.S. and Gupta, S., 2015. A novel approach to priority based focused crawler. *International Journal of Computer Applications*, *116*(19).

[20]. Tomar, R. and Rathore, R.S., 2016. Privacy Preserving in TPA using Secured Encryption Technique for Secure Cloud. *International Journal of Computer Applications*, *138*(8).

[21]. Tomar, R. and Rathore, R.S., 2016. A Survey on Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud. *International Advanced Research Journal in Science, Engineering and Technology*, *3*(4), pp.83-86.

[22]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Clustering Technique Approach to Detect the Special Patterns for Medical Video Mining. *Advances in Data Management*, p.140.

[23]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Architectural Options and Challenges for Broadband Satellite ATM networks. *Recent Developments in Computing and Its Applications*, p.155.

[24]. Srivastava, S.N., Kshatriya, S. and Rathore, R.S., 2017. Search Engine Optimization in E-Commerce Sites. *International Research Journal of Engineering and Technology (IRJET)*, *4*(5), pp.153-155.
[25]. Rattan, V., Sinha, E.M., Bali, V. and Rathore, R.S., 2010. E-Commerce Security using PKI approach. *International Journal on Computer Science and Engineering*, *2*(5), pp.1439-1444.
[26]. Bali, V., Rathore, R.S. and Sirohi, A.,2010. Adaptive Analysis of Throughput in Mobile Admhoc Network (IEEEm802. 11).*International Journal of Computer Science & Communication*, *1*(1), pp.25-28.
[27]. Kumar, V. and Singh Rathore, R., 2016. A Review on Natural Language Processing. *International Journal Of Engineering Development And Research*.
[28]. Bhatnagar, D. and Rathore, R.S.,2015. CLOUD COMPUTING: SECURITY ISSUES AND SECURITY MEASURES. *International Journal of Advance Research in Science And Engineering*, *4*(01), pp.683-690.
[29]. Rathore, R.S., Hewage, C., Kaiwartya, O. and Lloret, J., 2022. In-vehicle communication cyber security: challenges and solutions. *Sensors*, *22*(17), p.6679.
[30]. D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in Proc. Int. Conf. Mobile Computing and Networking (MOBICOM), 1999, pp. 263–270.
[31]. Rathore, R.S., Kaiwartya, O., Qureshi, K.N., Javed, I.T., Nagmeldin, W., Abdelmaboud, A. and Crespi, N., 2022. Towards enabling fault tolerance and reliable green communications in next-generation wireless systems. *Applied Sciences*, *12*(17), p.8870.
[32]. Khasawneh, A.M., Singh, P., Aggarwal, G., Rathore, R.S. and Kaiwartya, O., 2022. E-Mobility Advisor for Connected and Autonomous Vehicles Environments. *Adhoc& Sensor Wireless Networks*, *53*.
[33]. Kumar, S., Rathore, R.S., Mahmud, M., Kaiwartya, O. and Lloret, J., 2022. BEST—Blockchain-Enabled Secure and Trusted Public Emergency Services for Smart Cities Environment. *Sensors*, *22*(15), p.5733.
[34]. Jha, S.K., Prakash, S., Rathore, R.S., Mahmud, M., Kaiwartya, O. and Lloret, J., 2022. Quality-of-service-centric design and analysis of unmanned aerial vehicles. *Sensors*, *22*(15), p.5477.
[35]. Kumar, M., Kumar, S., Kashyap, P.K., Aggarwal, G., Rathore, R.S., Kaiwartya, O. and Lloret, J., 2022. Green communication in internet of things: A hybrid bio-inspired intelligent approach. *Sensors*, *22*(10), p.3910.