International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

Tackling the Security Challenges of IoT using Forensic Perspective

Karlapalem Sujitha
Department of Cybersecurity
CMR College of Engineering & Technology
Hyderabad, Telangana

A. Mounika Rajeswari
Department of Computer Science & Engineering
CMR College of Engineering & Technology
Hyderabad, Telangana

***Abstract*— From home automation to business control systems, the Internet of Things (IoT) has transformed how we interact with the environment. But as the quantity of IoT devices increases, so do the forensic and security concerns. The problems and prospects in IoT security and forensics are briefly discussed in this paper. The first issue is that IoT devices lack security, leaving them open to threats like denial-of-service attacks, data theft, and hacking. This is brought on by the lack of a uniform security protocol for IoT devices. The lack of forensic tools and methods to look into crimes involving IoT is the second problem. The third difficulty is gathering and analysing massive amounts of data produced by IoT devices. The paper also discusses ways to address these issues, including the creation of a standardised security protocol for IoT devices, advancements in forensic methods and tools for the investigation of crimes involving IoT, and the use of AI and machine learning to process and interpret massive amounts of IoT data. The report also looks at the part stakeholders play in assuring IoT security and forensics, including manufacturers, regulators, and end users. This paper's conclusion emphasises the urgent need for forensic and IoT security solutions to resolve the issues brought on by the vulnerabilities of IoT devices. The possibilities discussed in this paper offer stakeholders a road map for taking proactive steps in safeguarding IoT devices and looking into IoT-related crimes.**

Keywords*— *Internet of Things, Cyber Security, Digital Forensic

1. INTRODUCTION

The Internet of Things (IoT) combines a variety of smart nodes, items, and sensors that can communicate with one another without the need for human involvement. The items operate on their own while interacting with other things. IoT nodes may access and authorize cloud-based resources for collecting and extracting data, distribute lightweight data, and make decisions by analyzing acquired data. IoT has made it commonplace for people, services, sensors, and objects to be connected. IoT devices are currently being used in a variety of applications, including intelligent transportation systems, smart grids, and healthcare. IoT networks now offer a much higher number of smart devices and intelligent, autonomous services thanks to the enormous commercial potential within the IoT area. Additionally, the development of cloud-enabled IoT networks was influenced by the reliance of IoT devices on cloud infrastructure for data transport, storage, and analysis.

In the IoT ecosystem, security difficulties such privacy, access control, secure communication, and safe data storage are growing in importance. Additionally, every new sensor we install, every device we design, and every byte that is synchronized in an IoT system may at some point be the subject of an investigation. Numerous weak and insecure nodes were deployed as a result of the IoT's rapid growth in both devices and services. Furthermore, object-driven IoT networks do not benefit much from standard user-driven security architectures. As a result, we need specialized equipment, methods, and procedures for protecting IoT networks as well as gathering, conserving, and examining leftover traces of IoT settings.

2. LITERATURE REVIEW

The literature review focuses on the topic of IoT security and forensics and analyzes the following papers:

Ambrosin et al. (n.d.) investigate the feasibility of attribute-based encryption (ABE) on IoT devices. The authors explore the use of ABE to provide data confidentiality and access control in IoT devices. The study highlights the benefits of ABE in protecting sensitive data on IoT devices and discusses the challenges of implementing ABE on resource-constrained devices.

Giaretta et al. (n.d.) examine security vulnerabilities and countermeasures for target localization in Bio-Nano Things communication networks. The authors present a framework for securing Bio-Nano Things communication networks against various attacks, such as data injection and node compromise. The paper discusses the use of trust-based approaches and cryptography to secure the network against these attacks.

Yang et al. (2016) propose a lightweight anonymous entity authentication scheme for IoT applications. The authors present a scheme that provides mutual authentication between IoT devices and servers without revealing their identities. The paper discusses the benefits of the proposed scheme in terms of efficiency, privacy, and security.

Bertino et al. (n.d.) analyze the security and privacy challenges of IoT devices and propose a framework for securing IoT devices against various attacks. The authors discuss the importance of privacy-preserving techniques and access control mechanisms in securing IoT devices. The paper also highlights the role of regulations and standards in ensuring the security and privacy of IoT devices.

Haddad Pajouh et al. (n.d.) propose a two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. The authors present a model that reduces the dimensionality of the data and classifies it into normal and anomalous traffic. The paper discusses the effectiveness of the proposed model in detecting anomalous traffic in IoT backbone networks.

Harbawi and Varol (n.d.) propose an improved digital evidence acquisition model for IoT forensic investigation. The

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

authors present a theoretical framework for acquiring digital evidence from IoT devices, highlighting the importance of preserving the integrity and authenticity of the evidence. The paper also discusses the challenges of acquiring digital evidence from IoT devices and proposes solutions to overcome them.

Dehghantanha and Franke (n.d.) investigate data exfiltration from IoT devices, using iOS devices as case studies. The authors demonstrate how attackers can extract sensitive data from iOS devices through various attack vectors. The paper discusses the importance of protecting IoT devices against data exfiltration attacks and proposes countermeasures to prevent them.

In conclusion, the papers that have been evaluated show the prospects and challenges in IoT security and forensics. They go over several methods and frameworks for protecting IoT devices from threats and looking into crimes involving IoT. In the literature study, it is emphasised how critical it is to create standardized security protocols, enhance forensic tools and methods, and use AI and ML to analyses and understand IoT data.

3. IOT ENVIRONMENT SECURITY CHALLENGES

Security has become a significant concern because to the widespread dispersion of IoT nodes and the private nature of the data that IoT devices collect and transport. We're taking a quick look at the main security issues that affect IoT setups in this section.

3.1 Authentication

Authentication in the IoT sector enables the integration of various IoT devices that are deployed in various situations. Both the source of the data route (the data origin node) and the routing peers involved in data transmission must be authenticated as part of the authentication procedure.

The authentication of IoT devices faces a barrier with efficient key deployment and key management. The production and exchange of cryptographic keys shouldn't significantly increase the burden on IoT nodes. Additionally, other techniques are needed for validating cryptographic keys and guaranteeing key transfer integrity in the absence of a certified Certificate Authority (CA).

3.2 Access Control and Authorization

While access control techniques should ensure that only resources that have been authorized are accessible, authorization entails specifying access permissions to various resources. Every IoT node might only support a few number of access verification procedures, which might vary from other connected objects to the same node. Therefore, in a heterogeneous IoT network, it can be difficult to deploy and manage a range of authorization and access control techniques that are customized to distinct nodes' capabilities.

3.3 Privacy

The deployment of autonomous IoT equipment that can sense personal information about people (such health data) poses a new kind of threat to people's privacy. IoT nodes are secretly gathering people's private data, in contrast to traditional instances where users must perform some actions (such as searching for a keyword or uploading some material) to jeopardize their privacy.

User-centric privacy, content-oriented privacy, or context-oriented privacy are all provided through existing techniques. IoT networks, on the other hand, come naturally with autonomous nodes that gather data and demand object-oriented privacy models. Additionally, the majority of privacy laws require that consumers be kept aware about how their personal data is handled and managed. In heterogeneous IoT networks, identifying nodes that might have access to users' private information that has been passively collected is extremely difficult.

4. FORENSICS IN IOT ENVIRONMENTS

IoT would soon permeate every part of our lives, from controlling the temperature in our homes to intelligent cars and smart city administration. Therefore, it won't be long until we witness individuals suing one another for abusing their smart devices, such as cars that have accidents or attackers who have penetrated smart sensors. Identification, gathering, preservation, and reporting of evidences, as well as attack or deficiency attribution, would be difficult in this context. The Internet of Everything is developing into a haystack that holds many interesting forensics artefacts. We quickly discuss the primary forensics difficulties in IoT setups in this section.

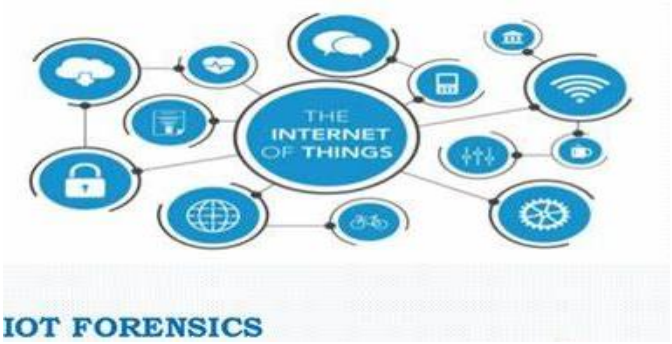

Figure: Forensics in IoT Environments

4.1 Identification, gathering, and preservation of evidence

The process of search and seizure is crucial to any forensic investigation. The fact that IoT solutions are made to operate discreetly and automatically makes detecting their presence rather difficult. Even when an IoT device is discovered, there is typically no established procedure or trustworthy instrument to gather any remaining evidence from the device in a forensically sound manner. Additionally, there are relatively few ways to capture forensic images of a specific IoT device while disregarding ethical issues when gathering proof from devices operating in a multi-tenancy setting.

While maintaining collected data using conventional methods like hashing is not difficult, maintaining the scene in an IoT setting is really challenging. Identification of a compromise's scope and the perimeter of a crime scene would be highly challenging, if not impossible, due to real-time and autonomous interactions between various nodes.

4.2 Analysis and Correlation of the Evidence

A hurdle for an investigator is determining the provenance of evidence because the majority of IoT nodes don't store any metadata, including time information. Correlation of evidence received from various IoT devices is nearly impossible without temporal information like modified, accessed, and generated

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 05, May-2023

times. Beyond technological difficulties, privacy is a crucial problem to take into account while analyzing and correlating obtained data, particularly as the bulk of IoT sensors are gathering inherently personal data. Additionally, it is very impossible to perform an end-to-end analysis of residual evidences due to the vast volume of data that is generated in heterogeneous IoT systems.

4.3 Attribution of Attack or Deficit

Finding criminal actors or the liable parties in the case of an occurrence is a regular result of any forensics investigation. Finding out who is responsible for an accident, whether it be a human driver or an autonomous vehicle, may soon provide a difficulty for cyber forensics because of the industry's rapid development. Without defined methodologies and forensically sound tools for the gathering, preservation, and analysis of data from cyber physical systems, it would be impossible to respond to such inquiries. Additionally, it would be difficult to determine the activities and liabilities of various parties with access to an IoT node in the absence of a reliable authentication method. Lastly, the identification of malicious even with proof, it can be difficult to discover behaviors in an IoT context because there isn't a safe and dependable architecture that ensures forensically sound logging and a mechanism for monitoring.

5. CONCLUSION

In conclusion, the Internet of Things (IoT) is a fast expanding technology that offers opportunities and difficulties for forensic analysis and security. IoT devices are susceptible to a variety of security risks due to their immense quantity and diversity as well as their constrained compute and storage capacities. Researchers have suggested a number of methods and approaches to deal with these problems, including attribute-based encryption, light authentication, and anomaly-based intrusion detection. Additionally, specialized tools and methods like data recovery and the capture of digital evidence are needed for IoT forensic investigations. IoT presents substantial security and forensic concerns, but it also offers enormous potential for new tools and methodologies to be created. We can strengthen the security of IoT environments and our capacity to analyses cybercrimes using IoT devices with sustained research and development.

REFERENCES

[1] Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S. R., Rahmani, A. M., & Liljeberg, P.On the Feasibility of Attribute-Based Encryption on Internet of Things Devices. (n.d.). On The Feasibility of Attribute-Based Encryption on Internet of Things Devices | IEEE Journals & Magazine | IEEE Xplore. http://doi.org/10.1109/MM.2016.101.

[2] Giaretta, A., Balasubramaniam, S., & Conti, M. Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks. (n.d.). Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks | IEEE Journals & Magazine | IEEE Xplore. http://doi.org/10.1109/TIFS.2015.2505632

[3] Yang, Y., Cai, H., Wei, Z., Lu, H., & Choo, K. K. R. (2016, June 30). Towards Lightweight Anonymous Entity Authentication for IoT Applications. Towards Lightweight Anonymous Entity Authentication for IoT Applications | SpringerLink. https://doi.org/10.1007/978-3-319-40253-6_16

[4] Bertino, E., Choo, K.-K. R., Georgakopolous, D., & Nepal, S. ACM Digital Library. (n.d.). ACM Digital Library. http://doi.org/10.1145/3013520

[5] Haddad Pajouh, H., Javidan, R., Khayami, R., Ali, D., & Choo, K.-K. R. A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks. (n.d.). A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks | IEEE Journals & Magazine | IEEE Xplore. http://doi.org/10.1109/TETC.2016.2633228

[6] Harbawi, M., & Varol, A.An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. (n.d.). An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I: A Theoretical Framework | IEEE Conference Publication | IEEE Xplore. http://doi.org/10.1109/ISDFS.2017.7916508

[7] Dehghantanha, A., & Franke, K. Data Exfiltration From Internet of Things Devices: iOS Devices as Case Studies. (n.d.). Data Exfiltration From Internet of Things Devices: iOS Devices as Case Studies | IEEE Journals & Magazine | IEEE Xplore. http://doi.org/10.1109/JIOT.2016.2569094

[8] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/comst.2015.2444095

[9] Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2013, June 10). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728–2742. https://doi.org/10.1002/sec.795

[10] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep Learning for IoT Big Data and Streaming Analytics: A Survey. IEEE Communications Surveys & Tutorials, 20(4), 2923–2960. https://doi.org/10.1109/comst.2018.2844341