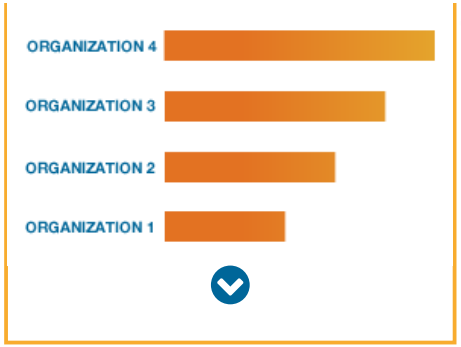
Ransomware: A Framework for Security Challenges in Internet of Things

Publisher: IEEE

Soobia Saeed; NZ Jhanjhi; Mehmood Naqvi; Mamoona Humayun; Shakeel Ahmed **All Authors**



Downl
PDF

Abstract: With the increasing volume of smartphones, computers, and sensors in the Internet of Things (IoT) model, enhancing security and preventing ransom attacks have become a ma...**View more**

Metadata

Abstract:
With the increasing volume of smartphones, computers, and sensors in the Internet of Things (IoT) model, enhancing security and preventing ransom attacks have become a major concern. Traditional security mechanisms are no longer applicable due to the involvement of devices with limited resources, which require more computing power and resources. Ransomware is comparatively a new and cruel malware in cyberspace with higher rates of attacks around the world. Ransomware could encrypt entire data to make users unable to access their files and important information. In some cases, the system has been hostage completely by the hackers, and the user may receive a demand for ransom money using different resources o access of his/her own data/system. One of the problems associated with the Internet of Things is how to keep your smartphones secure and keep your data safe as most of the antivirus solutions are not useful in this case. This research concludes the impact of ransomware on the IoT, malware processes, and work on detecting and monitoring smartphone infections. The paper also discusses ransomware awareness to end-user with strategy to defeat it.

Published in: 2020 2nd International Conference on Computer and Information Sciences (ICCIS)

Date of Conference: 13-15 Oct. 2020 **DOI:** 10.1109/ICCIS49240.2020.9257660

Date Added to IEEE *Xplore*: 24 November 2020 **Publisher:** IEEE

ISBN Information:

Conference Location: Sakaka, Saudi Arabia, Saudi Arabia

Funding Agency:

Citation Map

1.L. Atzori, A. Iera and G. Morabito, "The internet of things: A survey", *Computer networks*, vol. 54, no. 15, pp. 2787-2805, 2010.
Show Context CrossRef Google Scholar

2.S. Andreev and Y. Koucheryavy, "Internet of things smart spaces and next-generation networking" in LNCS, Springer, vol. 7469, pp. 464, 2012.
Show Context CrossRef Google Scholar

3.J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues" in International Journal of Computer Applications, New York, USA:Foundation of Computer Science, vol. 90, no. 11, pp. 20-26, March 2014.
Show Context CrossRef Google Scholar

4.A. Stango, N. R. Prasad and D. M. Kyriazanos, "A threat analysis methodology for security evaluation and enhancement planning", *Emerging Security Information Systems and Technologies 2009. SECUR WARE' 09. Third International Conference on*, pp. 262-267, 2009.
Show Context View Article Full Text: PDF (337KB) Google Scholar

5.D. Jiang and C. ShiWei, "A study of information security for m2m of iot", *Advanced Computer Theory and Engineering (ICACTE) 2010 3rd International Conference on*, vol. 3, pp. 83, 2010.
Show Context Google Scholar

6.B. Schneier, Secrets and lies: digital security in a networked world, new york:John Wiley & Sons, vol. 51, pp. 304-306, 2011.
Show Context Google Scholar

7.S. Balamurugan, A. Ayyasamy and K. S. Joseph, "A Review on Privacy and Security Challenges in the Internet of Things (IoT) to protect the Device and Communication Networks", *Journal of Computer Science IJCSIS*, vol. 16, no. 6, pp. 57-62, 2018.
Show Context Google Scholar

8.M. Taneja, "An analytics framework to detect compromised IoT devices using mobility behaviour", *ICT Convergence (ICTC) 2013 International Conference on*, pp. 38-43, 2013.
Show Context View Article Full Text: PDF (918KB) Google Scholar

9.G. M. Koien and V. A. Oleshchuk, "Aspects of Personal Privacy in Communications-Problems", *Technology and Solutions. River Publishers*, vol. 22, 2013.
Show Context Google Scholar

10.N. R. Prasad, "Threat model framework and methodology for personal networks (pns)", *Communication Systems Software and Middleware 2007. COMSWARE 2007. 2nd International Conference on*, pp. 1-6, 2007.
Show Context View Article Full Text: PDF (5150KB) Google Scholar

11.J. E. Thomas, "Improving Backup System Evaluations in Information Security Risk Assessments to Combat Rans omware", *Published by Canadian Center of Science and Education*, vol. 11, pp. 1-12, 2018.
Show Context Google Scholar

12.J. Allen, "Surviving ransomware", *American Journal of Family Law*, vol. 31, no. 2, pp. 65-68, 2017.
Show Context Google Scholar

13.A. K. Maurya, N. Kumar, A. Agrawal and R. A. Khan, "Ransomware: Evolution Target and Safety Measures", *IET Faizabad India*, vol. 6, no. 1, pp. 80-85, 2018.
Show Context CrossRef Google Scholar

14.N. Agnihotri, "Ransomware Classifier using Extreme Gradient Boosting", *(IJCSIT) International Journal of Computer Science and Information Technologies*, vol. 9, no. 2, pp. 45-47, 2018.
Show Context Google Scholar

15.M. Paquet-Clouston, "Ransomware Payments in the Bitcoin Ecosystem", *Austrian Institute of Technology Vienna IEEE Symposium on Security and Privacy and Information Security Management Conference*, pp. 1-9, 2018.
Show Context Google Scholar

16.K. Cabaj and W. Mazurczyk, "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall", *IEEE Network*, vol. 30, no. 6, 2016.
Show Context View Article Full Text: PDF (231KB) Google Scholar

17.N. Shah and M. Farik, "Ransomware - Threats Vulnerabilities and Recommendations", *International Journal of Scientific & Technology*, vol. 6, no. 6, pp. 307-309, 2017.
Show Context Google Scholar

18.R. Richardson, "Ransomware: Evolution Mitigation and Prevention", *Management & Entrepreneurship Department Information Systems Department Coles College of Business Kennesaw State University GA USA*, vol. 13, pp. 25-32, 2017.
Show Context Google Scholar

19.S. H. Kok, A. Abdullah, N. Z. Jhanjhi and M. Supramaniam, "A Review of Intrusion Detection System using Machine Learning Approach", *International Journal of Engineering Research and Technology*, vol. 12, no. 1, pp. 8-15, 2019, ISSN 0974-3154.
Show Context Google Scholar

20.S. H. Kok, A. Abdullah, N. Z. Jhanjhi and M. Supramaniam, "Ransomware Threat and Detection Techniques: A Review", *IJCSNS International Journal of Computer Science and Network Security*, vol. 19, no. 2, February 2019.
Show Context Google Scholar

21.S. H. Kok, A. Abdullah, N. Z. Jhanjhi and M. Supramaniam, "Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm", *Computers*, vol. 8, no. 4, pp. 79-80, 2019.
Show Context CrossRef Google Scholar

22.H. U. Salvi, "Ransomware: A Cyber Extortion", *Asian Journal of Convergence in Technology*, vol. 2, pp. 1-9, 2017.
Show Context Google Scholar

23.S. B. Surati, "A Review on Ransomware Detection & Prevention", *International Journal of Research and Scientific Innovation (IJRSI)*, vol. 4, pp. 38-39, 2017.
Show Context Google Scholar

24.P. B. Pathak, "A Dangerous Trend of Cybercrime: Ransomware Growing Challenge", *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 5, no. 2, pp. 371-373, 2016.
Show Context Google Scholar

25.S. Mohurle and M. R. Patil, "A brief study of WannaCry Threat: Ransomware Attack 2017", *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1938-1940, 2017.
Show Context Google Scholar

26.M. M. Ahmadian, H. R. Shahriari and S. M. Ghaffarian, "Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable Ransomware", *Information Security and Cryptology (ISCISC) 2015 12th International Conference on Iranian Society of Cryptology*, pp. 79-84, 2015.
Show Context View Article Full Text: PDF (874KB) Google Scholar

27.K. Fischer and J. Gesner, "Security architecture elements for IoT enabled automation networks normally-off computing for IoT systems", *2015 International SoC Design Conference (ISOCC)*, pp. 1-8.

Show Context Google Scholar

28.Z. A. Almusaylim, N. Zaman and L. T. Jung, "Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment", *IEEE In 2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, pp. 1-5, August 2018.
Show Context View Article Full Text: PDF (1239KB) Google Scholar

29.Z. A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT)", *Journal of Wireless Networks*, pp. 1-12, 2018.
Show Context Google Scholar

30.Z. A. Almusaylim and N. Z. Jhanjhi, "Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing", *Wireless Pers Commun*, pp. 32-38, 2019.
Show Context Google Scholar

31.M. Alamri, N. Z. Jhanjhi and M. Humayun, "Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review", *International Journal of Computer Science and Network Security*, vol. 19, no. 5, pp. 244-258, 2019.
Show Context Google Scholar

32.K. Hussain, S. J. Hussain, N. Z. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", *2019 International Conference on Computer and Information Sciences (ICCIS)*, vol. 3, pp. 1-4, 2019.
Show Context View Article Full Text: PDF (1562KB) Google Scholar

Contents

I. Introduction

The recent rapid development in the Internet of Things (IoT) and its ability to provide different types of services have made it the one of the fastest-growing technologies with a major impact on social life and business environments [1]–[3]. The Internet of Things has increasingly entered all areas of modern human life, such as education, health care, and the business world, with storing confidential personal and business information, financial data transactions, brand development, and marketing. The widespread proliferation of connected devices in IoT has increased the demand for robust safety in response to the growing worldwide demand of connected devices and services [4]. The threats on IoT are increasing every day and there is a growth in the number and intensity of attacks. In addition to the increasing number of potential attackers and the size of networks, the tools available to potential attackers have become more advanced, efficient and effective [5]. Protection against threats and vulnerabilities is therefore necessary for the IoT to achieve its full potential [6]–[9]. Protection is characterized as a mechanism for protecting an object from physical damage, unauthorized access, theft or destruction, preserving high security and integrity of the object's data, and providing information about the object at any time [10]. Digital technology awareness and information techniques have helped cybercriminals to give constant and emerging threats to the computer users.

Authors

Figures

References

Citation Map

1. L. Atzori, A. Iera and G. Morabito, "The internet of things: A survey", *Computer*

networks, vol. 54, no. 15, pp. 2787-2805, 2010.
Show Context CrossRef Google Scholar

2.S. Andreev and Y. Koucheryavy, "Internet of things smart spaces and next-generation networking" in LNCS, Springer, vol. 7469, pp. 464, 2012.
Show Context CrossRef Google Scholar

3.J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues" in International Journal of Computer Applications, New York, USA:Foundation of Computer Science, vol. 90, no. 11, pp. 20-26, March 2014.
Show Context CrossRef Google Scholar

4.A. Stango, N. R. Prasad and D. M. Kyriazanos, "A threat analysis methodology for security evaluation and enhancement planning", *Emerging Security Information Systems and Technologies 2009. SECUR WARE' 09. Third International Conference on*, pp. 262-267, 2009.
Show Context View Article Full Text: PDF (337KB) Google Scholar

5.D. Jiang and C. ShiWei, "A study of information security for m2m of iot", *Advanced Computer Theory and Engineering (ICACTE) 2010 3rd International Conference on*, vol. 3, pp. 83, 2010.
Show Context Google Scholar

6.B. Schneier, Secrets and lies: digital security in a networked world, new york:John Wiley & Sons, vol. 51, pp. 304-306, 2011.
Show Context Google Scholar

7.S. Balamurugan, A. Ayyasamy and K. S. Joseph, "A Review on Privacy and Security Challenges in the Internet of Things (IoT) to protect the Device and Communication Networks", *Journal of Computer Science IJCSIS*, vol. 16, no. 6, pp. 57-62, 2018.
Show Context Google Scholar

8.M. Taneja, "An analytics framework to detect compromised IoT devices using mobility behaviour", *ICT Convergence (ICTC) 2013 International Conference on*, pp. 38-43, 2013.
Show Context View Article Full Text: PDF (918KB) Google Scholar

9.G. M. Koien and V. A. Oleshchuk, "Aspects of Personal Privacy in Communications-Problems", *Technology and Solutions. River Publishers*, vol. 22, 2013.
Show Context Google Scholar

10.N. R. Prasad, "Threat model framework and methodology for personal networks (pns)", *Communication Systems Software and Middleware 2007. COMSWARE 2007. 2nd International Conference on*, pp. 1-6, 2007.
Show Context View Article Full Text: PDF (5150KB) Google Scholar

11.J. E. Thomas, "Improving Backup System Evaluations in Information Security Risk Assessments to Combat Rans omware", *Published by Canadian Center of Science and Education*, vol. 11, pp. 1-12, 2018.
Show Context Google Scholar

12.J. Allen, "Surviving ransomware", *American Journal of Family Law*, vol. 31, no. 2, pp. 65-68, 2017.
Show Context Google Scholar

13.A. K. Maurya, N. Kumar, A. Agrawal and R. A. Khan, "Ransomware: Evolution Target and Safety Measures", *IET Faizabad India*, vol. 6, no. 1, pp. 80-85, 2018.
Show Context CrossRef Google Scholar

14.N. Agnihotri, "Ransomware Classifier using Extreme Gradient Boosting", *(IJCSIT) International Journal of Computer Science and Information Technologies*, vol. 9, no. 2, pp. 45-47, 2018.
Show Context Google Scholar

15.M. Paquet-Clouston, "Ransomware Payments in the Bitcoin Ecosystem", *Austrian Institute of Technology Vienna IEEE Symposium on Security and Privacy and Information Security Management Conference*, pp. 1-9, 2018.
Show Context Google Scholar

16.K. Cabaj and W. Mazurczyk, "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall", *IEEE Network*, vol. 30, no. 6, 2016.
Show Context View Article Full Text: PDF (231KB) Google Scholar

17.N. Shah and M. Farik, "Ransomware - Threats Vulnerabilities and Recommendations", *International Journal of Scientific & Technology*, vol. 6, no. 6, pp. 307-309, 2017.
Show Context Google Scholar

18.R. Richardson, "Ransomware: Evolution Mitigation and Prevention", *Management & Entrepreneurship Department Information Systems Department Coles College of Business Kennesaw State University GA USA*, vol. 13, pp. 25-32, 2017.
Show Context Google Scholar

19.S. H. Kok, A. Abdullah, N. Z. Jhanjhi and M. Supramaniam, "A Review of Intrusion Detection System using Machine Learning Approach", *International Journal of Engineering Research and Technology*, vol. 12, no. 1, pp. 8-15, 2019, ISSN 0974-3154.
Show Context Google Scholar

20.S. H. Kok, A. Abdullah, N. Z. Jhanjhi and M. Supramaniam, "Ransomware Threat and Detection Techniques: A Review", *IJCSNS International Journal of Computer Science and Network Security*, vol. 19, no. 2, February 2019.
Show Context Google Scholar

21.S. H. Kok, A. Abdullah, N. Z. Jhanjhi and M. Supramaniam, "Prevention of Crypto- Ransomware Using a Pre-Encryption Detection Algorithm", *Computers*, vol. 8, no. 4, pp. 79-80, 2019.
Show Context CrossRef Google Scholar

22.H. U. Salvi, "Ransomware: A Cyber Extortion", *Asian Journal of Convergence in Technology*, vol. 2, pp. 1-9, 2017.
Show Context Google Scholar

23.S. B. Surati, "A Review on Ransomware Detection & Prevention", *International Journal of Research and Scientific Innovation (IJRSI)*, vol. 4, pp. 38-39, 2017.
Show Context Google Scholar

24.P. B. Pathak, "A Dangerous Trend of Cybercrime: Ransomware Growing Challenge", *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 5, no. 2, pp. 371-373, 2016.
Show Context Google Scholar

25.S. Mohurle and M. R. Patil, "A brief study of WannaCry Threat: Ransomware Attack 2017", *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1938-1940, 2017.
Show Context Google Scholar

26.M. M. Ahmadian, H. R. Shahriari and S. M. Ghaffarian, "Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable Ransomware", *Information Security and Cryptology (ISCISC) 2015 12th International Conference on Iranian Society of Cryptology*, pp. 79-84, 2015.
Show Context View Article Full Text: PDF (874KB) Google Scholar

27.K. Fischer and J. Gesner, "Security architecture elements for IoT enabled automation networks normally-off computing for IoT systems", *2015 International SoC Design Conference (ISOCC)*, pp. 1-8.
Show Context Google Scholar

28.Z. A. Almusaylim, N. Zaman and L. T. Jung, "Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment", *IEEE In 2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, pp. 1-5, August 2018.
Show Context View Article Full Text: PDF (1239KB) Google Scholar

29.Z. A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT)", *Journal of Wireless Networks*, pp. 1-12, 2018.
Show Context Google Scholar

30.Z. A. Almusaylim and N. Z. Jhanjhi, "Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing", *Wireless Pers Commun*, pp. 32-38, 2019.
Show Context Google Scholar

31.M. Alamri, N. Z. Jhanjhi and M. Humayun, "Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review", *International Journal of Computer Science and Network Security*, vol. 19, no. 5, pp. 244-258, 2019.
Show Context Google Scholar

32.K. Hussain, S. J. Hussain, N. Z. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", *2019 International Conference on Computer and Information Sciences (ICCIS)*, vol. 3, pp. 1-4, 2019.
Show Context View Article Full Text: PDF (1562KB) Google Scholar

Keywords