AIRO JOURNALS
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

INTEGRATED METHODS FOR ENHANCING SECURITY AND EFFICIENCY IN IOT SYSTEMS

Bharath GG
Research Scholar
Computer Science
Dr. Kamal Kumar Srivastava
Guide name & Deginastion:
[Professor]
Computer Science,
School of Computer Science,
Sun Rise University, Alwar

Abstract

This study investigates integrated approaches that use traffic filtering, packet compression, and cryptography to improve the security and performance of Internet of Things (IoT) systems. Conventional techniques, such packet filtering, encryption, and port forwarding, have drawbacks, especially in terms of overall security and performance. According to the study, cryptography stops hackers from accessing data without authorization, but it does not handle the discovery of hackers or illicit data transfers. Furthermore, there is a noticeable decrease in speed when cryptographic procedures and packet filtering are carried out simultaneously. This research suggests using data filtering, user filtering, IP and port filtering, user-defined ports, and an integrated firewall method to address these problems. Because it is more effective than more conventional techniques like AES and RSA at enabling quicker and more secure data transfer, XOR-based encryption is used. The suggested approach also highlights how crucial it is to update often in order to preserve IoT performance and security. The findings show that when compared to conventional approaches, the integrated approach decreases time consumption, error rates, and packet sizes, enhancing overall system security and efficiency.

Keywords: *Integrated Methods, Enhancing Security and Efficiency, Internet of Things (IoT) Systems, Compression Technology, Integrated Approach.*

1. INTRODUCTION

The majority of research has focused on protecting Internet of Things (IOT) systems through the use of user-defined ports, packet compression, and packet filtering. It has been found that a

ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

considerable amount of research projects has employed techniques based on cryptography to provide a security concern. Regretfully, neither hacking nor the transfer of illegal data is checked using this approach. Its only goal is to keep unauthorized parties from accessing private information. It has the ability to prevent data corruption and alteration, but it is unable to prevent data being incomprehensible to unauthorized individuals. Nevertheless, cryptography has gotten less attention while IP and packet filtering have proven successful in discouraging these invaders. Although some researchers did use the strategies previously mentioned, overall performance suffered as a result.

Data transmission is slow when packet filtering and cryptography processes are done simultaneously. This is one of the primary causes of the performance decrease; the other significant factor is the performance decrease brought on by carrying out these processes all at once. As a result, packet compression technologies, traffic filtering, and cryptography approaches are all used in this work. The proposed work used user-defined ports in place of preset ports as preset ports may have been the source of dangerous communications. This added even more security to the work.

Network security has become a worry as IOT needs become more and more important. Consequently, several security protocols have been implemented to protect Internet of Things systems from a variety of threats, including denial of service attacks, SQL injection, and brute force assaults. One of the most important aspects of technology is the necessity of frequent upgrades to guarantee the security of Internet of Things devices. This necessitates prompt modifications to the previously mentioned mechanisms, which will eventually improve performance while maintaining integrity. Figure 1 describes the techniques used in the recommended approach to increase security. Additionally, it is how the ongoing inquiry is proceeding.

AIRO JOURNALS
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

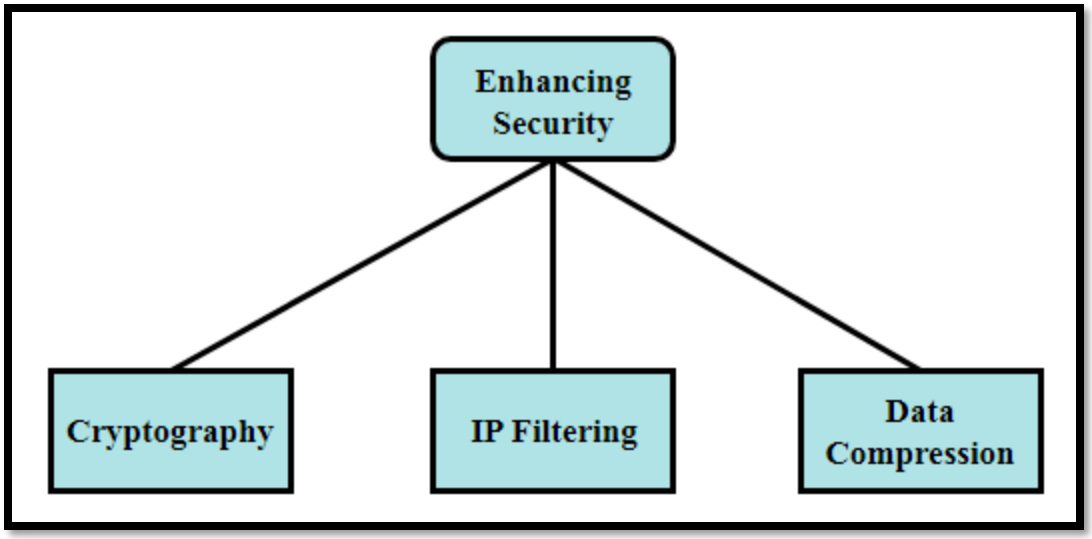

Figure 1: Techniques to Boost Security

2. LITERATURE REVIEW

Ahmed, A. W., Khan, O. A., Mian, M. A., and Shah, M. A. (2017) The phrase "Internet of Things" refers to a ubiquitous organizational engineering that provides information handling and analysis services to provide administrations to the real climate. This engineering has a lot of applications. Today, the Internet of Things has become increasingly important and is expanding quickly thanks to the most popular method of linking a variety of devices with different kinds of innovation. The multitude of electronic devices that are networked and linked to the Internet of Things increases the danger to privacy and information security. This article examines a variety of security issues, considers potential solutions, and projects the future of Internet of Things (IoT) security. Additionally, in light of the most recent analysis, this article examines crucial security measures, such as encryption, in relation to the Internet of Things (IoT) in an effort to thwart potentially dangerous attacks.

Al-Turjman, F., Zahmatkesh, H., &Shahroze, R. (2022) Smart urban communities have improved resident happiness and services. They are ideal for managing things gradually and providing smart data to people in transportation, medical services, smart structures, public health, smart stopping and traffic systems, smart farming, and other fields. Smart urban communities use programs that collect sensitive data. However, many security and protection issues may develop

ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

at various design stages. Thus, while creating and launching apps, security and protection concerns must be considered. This article covers the primary applications of smart urban communities and their security and safety concerns. It also looks at some of the current measures taken to ensure the classification and safety of data-focused applications in smart cities and suggests potential research gains that could improve performance.

Patil, S. S., and Sunitha, N. R. (2018) Since the introduction of the Internet of Things (IoT), communication has expanded, enabling faster reaction times and meeting the requirements of applications that are simply necessary. However, the security measures that are now in place are insufficient to ensure that it is safe from enemies. A few attempts have been made to outline safe, specialized methods that provide enhanced security features to a wide range of crucial Internet of Things applications (IoT). This might be attributed to the fact that the Internet of Things is relatively new. Within the context of the Internet of Things (IoT), this study commits to the discourse of the current research trend toward secure communication between devices. It is believed that the discussion that is recalled for the article will assist in providing an illustration of flow methodologies and strategies for handling research-based methodology in the context of the Internet of Things (IoT).

Dhanda, S. S., et.al., (2020) Security has become a major concern as the Internet of Things (IoT) grows. The internet has expanded to include the entire world. Due to the Internet of Things (IoT), the internet may move, making security more difficult. Security has always been the priority while arranging. Organizational size and security breach likelihood are related. Since the advent of IoT, the organization has grown beyond all previous bounds. It is everywhere on Earth. Remote sensor networks (WSN) and implanted devices with limited asset utilization recognize the discernment layer, the lowest layer in the Internet of Things design. These devices have limited memory, figure, power, and energy. They cannot resist a significant number of strikes. Since Internet of Things (IoT) devices automate traffic control and other duties, data security is crucial. Specialists and scientists have created blockchains, interruption recognition systems, lightweight cryptography, and protocols.

AIRO JOURNALS
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

Kim, T., et.al., (2024) decentralized Identifiers have expanded into IoT devices. These IDs protect user data and digital identities. Decentralized Identifiers overcome obstacles in situations requiring authority appointment and obscurity, such as lawful guardianship for children, device damage or injury, and concentrated healthcare environments with patient data. These challenges demand anonymity and power. Using a protected power designation and namelessness plot, this study aims to increase information sway in the Decentralized Identifier framework. Clear introductions should use a sequential total signature, a Non-Intuitive Zero-Information Proof, and a Merkle tree to prevent linking and Sybil attacks and allow designation. This method reduces assignment and obscurity security problems, computational and confirmation requirements for marks, and the number of unquestionable introductions by 1.2 to twice.

3. FIREWALL'S FUNCTION IN AN INTEGRATED APPROACH

An integrated strategy to firewalls is being examined for this project. Data, port, IP, and user filters are all taken into consideration by this strategy. The data connection originating from an actual infrastructure is considered by the Internet Protocol (IP) filter. When an incoming request originates from an illegitimate machine, the IP filter ignores it. Because the firewall has an IP filter built in, it is therefore possible to connect to a legitimate computer. The port filter achieves this by taking into account the actual port. The port numbers that come before 1024 have been reserved in case they are needed later. The total number of ports that the user defines is greater than 1024. The port that is present on the receiving end is the one that is utilized to start the process of initializing a connection. The port that has been initialized is the only one on which the sender is permitted to send data. Data will not be correctly communicated if it is transferred to a port that has not been initialized. A data filter will only limit the scope of the data if the specific kind, size, and author of the data are known. These files could be harmful, or they might be an attempt to carry out an attack. This means that the study that has been proposed must look at the systems that make up data filters in order to prevent the transmission of bogus data items. Users that are invalid can be restricted thanks to User Filter's functionality. When a user-filter-based firewall is activated, users with lower rights than other users are subject to limitations. Only users who have not yet finished the authentication procedure are able to transmit and receive packets.

AIRO JOURNALS
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

4. CRYPTOGRAPHY'S PLACE IN THE INTEGRATED APPROACH

The goal of the current study is to determine whether or not an encryption approach may be used to increase the security of data during transmission. XOR-based encryption is taken into consideration in the proposed study. In order to perform XOR operations, this kind of encryption requires recovering characters one at a time. To perform XOR-based encryption, a key is taken into consideration. Throughout this process, characters that are extracted from the data that will be sent from the sender's end are XORed with the binary version of the key. In order to recover the original data while the receiver is on the receiving end, the identical binary equivalent of the key is used with encrypted characters, or XOR. Considering this, a new method has been put into practice that takes a lot less time than DES, AES, and RSA together.

It has been shown that conventional data encryption techniques like AES and RSA need much more time due to the complexity of the algorithm. The suggested technique uses the XOR operation to achieve the purpose of data encryption, and content substitution comes next. After the data has been first compressed, it is further processed using the XOR technique to enable translation. The information that was included in the work that was suggested has also been encrypted using the XOR approach. The XOR method's functioning will be a key topic of study in this section. The outcome of the XOR operation will be 15, which is the sum of 9 and 6, if the user wants to submit the data with a value of 9. However, the XOR token is 6.

9 → 1001

15 → 1111

6 → 0110

After the data are received, they undergo further processing using the XOR method to produce the information that is really utilized.

15 → 1111

6 → 0110

9 → 1001

AIRO JOURNALS
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

An XOR operation yields a value of 1 if the bits being operated on are different from one another, and 0 otherwise. The data is then sent to the recipient when the XOR step is finished. If the receiver needs to decrypt the data, the replacement table is used to get the actual contents of the data after the XOR operation has been used to decode the data once again.

5. OUTCOME AND EFFICIENCY EVALUATION

The error rate is assessed in both the old model and the new strategy, and simulations of the processing time and packet size are given.

➢ Time Consumption

The simulation shows how much faster the suggested security solution would be implemented by contrasting it with the current security system. Figure 2 shows a comparison of the time spent on data transfers between the old method and the integrated scheme. The solution that has been proposed requires a far less time investment than the work that was done previously, which involved data transfer across the network without compression.

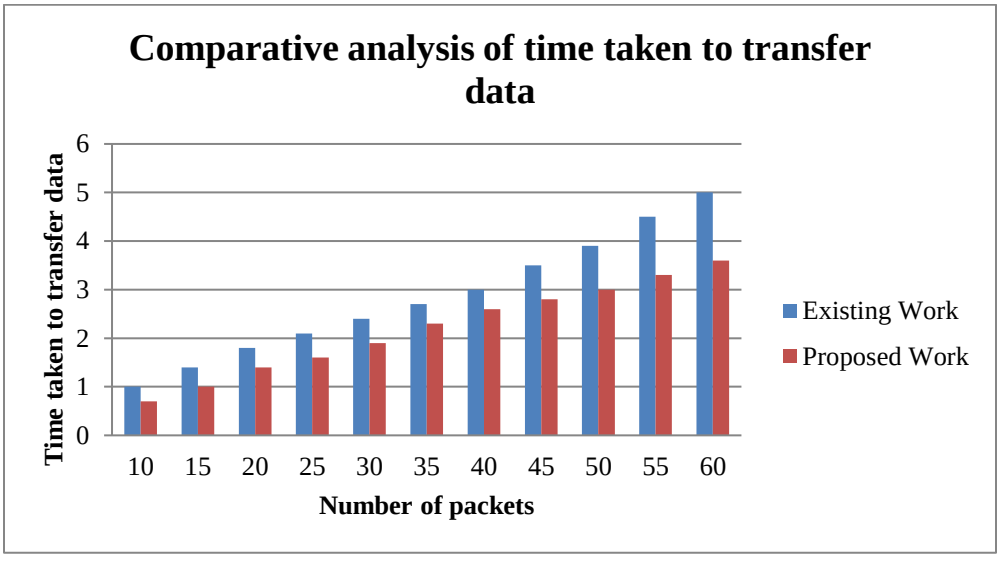

Figure 2: Analyzing the Transfer Time of Data

AIRO JOURNALS
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

- **Error Rate**

The packets are smaller than they would have been otherwise because the data is being compressed. This greatly lowers the possibility of errors happening. Given this, it is possible that, in comparison to labor that is already done, the suggested work will produce less errors. A comparison between the error rates that happened during the work that is now being done and the work that was done in the past is shown in Figure 3.

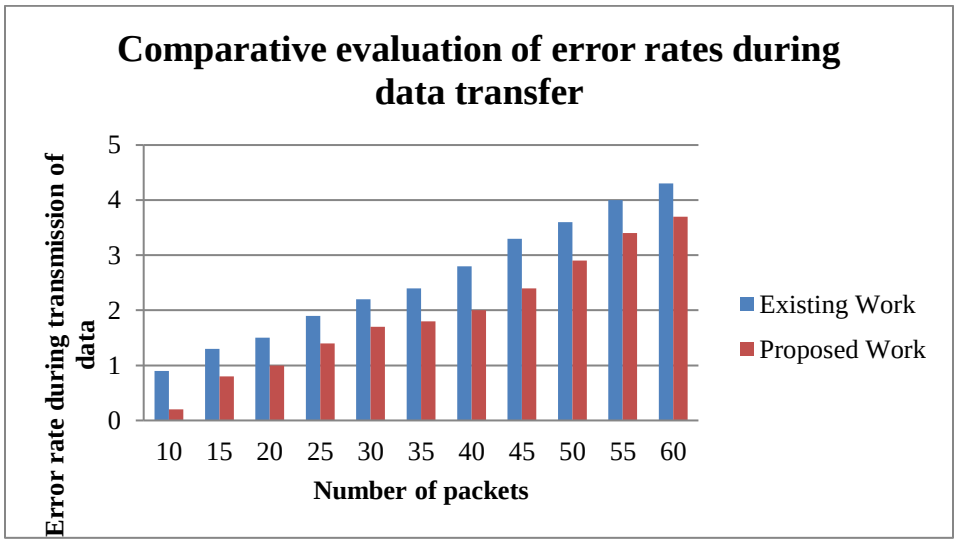

Figure 3: Analyzing the Error Rate in Data Transmission

- **Packet Size**

It is shown that in the work that is being given, if the amount of the data is decreased, the size of the packets will also be reduced. The technique that is recommended uses relatively little of the data contained in packets compared to more traditional sorts of mechanisms. Figure 4 shows how the proposed work and the existing work are similar to one other in terms of the size of the packets they create.

AIRO JOURNALS
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

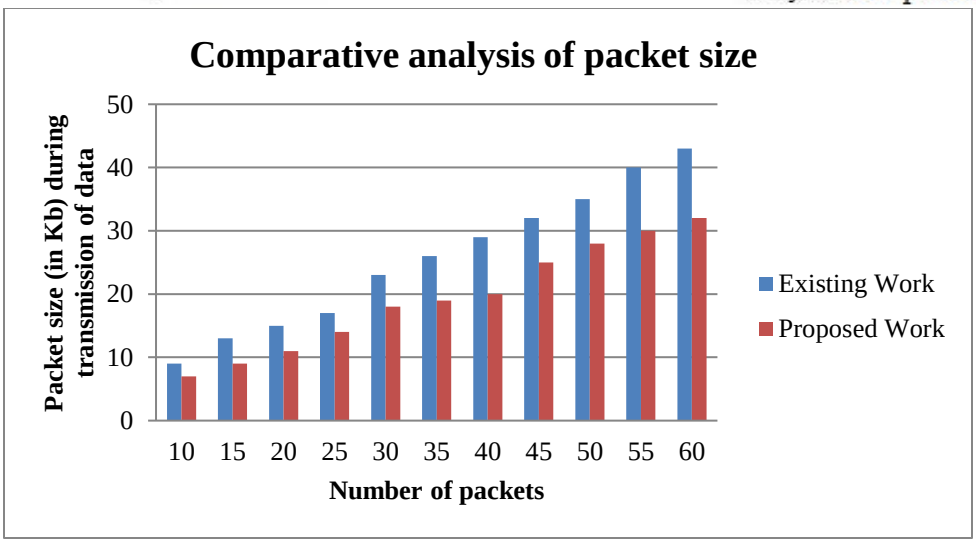

Figure 4: Analyzing the size of the packet

6. CONCLUSION

The proposed study shows how the integration of cryptographic algorithms, traffic filtering, and packet compression technologies may significantly improve security and efficiency in Internet of Things systems. Utilizing user-defined ports and applying an XOR-based encryption technique, the study overcomes the drawbacks of conventional cryptography and packet filtering techniques that frequently lead to inadequate security measures and performance drops. IP, port, data, and user filtering are all included in the integrated firewall method, which offers a complete security solution that is reliable and effective. An analysis of the suggested approach shows significant gains over the conventional approaches in terms of time consumption, error rates, and packet size. These results emphasize the integrated approach's potential to provide a more effective and safer framework for Internet of Things (IoT) systems, emphasizing the significance of regular updates and cutting-edge encryption methods in preserving the integrity and functionality of these systems.

REFERNCES

1. *Adat, V., & Gupta, B. B. (2018). Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems, 67, 423-441.*
2. *Ahanger, T. A., &Aljumah, A. (2018). Internet of Things: A comprehensive study of security issues and defense mechanisms. IEEE Access, 7, 11020-11028*

ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

3. *Ahmed, A. W., Khan, O. A., Mian, M. A., & Shah, M. A. (2017). A comprehensive analysis on the security threats and their countermeasures of IoT. International Journal of Advanced Computer Science and Applications, 8(7).*

4. *Al-Turjman, F., Zahmatkesh, H., &Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, 33(3), e3677*

5. *Dhanda, S. S., Singh, B., & Jindal, P. (2020). IoT security: A comprehensive view. Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, 467-494.*

6. *Kim, T., Seo, D., Kim, S. H., & Lee, I. Y. (2024). A Comprehensive Approach to User Delegation and Anonymity within Decentralized Identifiers for IoT. Sensors, 24(7), 2215.*

7. *Li, C., Wang, J., Wang, S., & Zhang, Y. (2023). A review of IoT applications in healthcare. Neurocomputing, 127017.*

8. *Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. Information, 7(3), 44.*

9. *Nebbione, G., &Calzarossa, M. C. (2020). Security of IoT application layer protocols: Challenges and findings. Future Internet, 12(3), 55.*

10. *Nguyen, H. H. (2023). A Comprehensive Approach to Secure and Effective Fall Detection in IOT Healthcare Systems.*

11. *Patil, S. S., &Sunitha, N. R. (2018). Review of Research Approaches for Securing Communication in Internet of Things. Communications on Applied Electronics, 7(13), 7-14.*

12. *Skwarek, V. (2017). Blockchains as security-enabler for industrial IoT-applications. Asia Pacific Journal of Innovation and Entrepreneurship, 11(3), 301-311.*

13. *Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975*

14. *Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., &Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.*

ISSN:2320-3714
Volume:3 Issue:1
July 2024
Impact Factor:10.2
Subject: Computer & Science

15. *Zaki, H. (2024). Addressing IoT Security: Understanding Challenges, Threats, and Countermeasures (No. 12019). EasyChair.*

Author's Declaration

I as an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher then my paper maybe rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds Any complication or error or anything hidden or implemented otherwise, my paper maybe removed from the website or the watermark of remark/actuality maybe mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me

Bharath GG
Dr. Kamal Kumar Srivastava