International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

Evaluating Secured Routing Scheme for Mobile Systems in the Internet of Things (IoT) Environment

J. Logeshwaran[1*], T. Kiruthiga[2]

[1]Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore – 641202, Tamil Nadu, India.*
[2]Department of Electronics and Communication Engineering, Vetri Vinayaha College of Engineering and Technology, Trichy – 621215, Tamil Nadu, India.

Email: [2]drkiruthigaece@gmail.com
Corresponding Email: [1]eshwaranece91@gmail.com*

Received: 03 November 2021 **Accepted:** 19 January 2022 **Published:** 21 February 2022

Abstract: ***The Internet of Things (IoT) environment presents a unique challenge in the area of secure routing for mobile systems. Unsecured routing can lead to the breach of sensitive data and compromise the overall security of an IoT network. As the IoT network is ever increasing and becoming more complex, the need for an effective and secure routing scheme is becoming more urgent. One type of secure routing scheme for mobile systems in an IoT network is the use of a two-hop approach. This approach requires the device to establish a secure link with a base station and then use the certified secure link to perform two hops to the goal node. This approach ensures that the nodes within the network are only able to access devices that they have been authorized to do so. The two-hop approach also provides an additional layer of security, as the device is able to verify the identity of each node that they hop to before granting them access to the data they seek. This approach also provides scalability for the routing protocol, as the protocol can adapt well for different topologies and network sizes. This makes it suitable for a wide range of IoT devices, from smart phones and wearable's to consumer appliances and industrial machines. Additionally, the two-hop approach can help to increase latency and reduce power consumption of the devices in the network. The secure two hop routing protocol is an effective solution for IoT networks and provides a strong layer of security without sacrificing scalability or performance. By using this secure routing protocol, IoT networks can remain safe and secure when sending and receiving data to and from mobile devices.***

Keywords: IoT, Secured, Routing, Link, Latency, Protocol, Scalability.

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

1. INTRODUCTION

The Internet of Things (IoT) is a network that connects physical objects to the Internet. This network allows objects, from smart phones and wearable devices to various sensors and actuators, to communicate and exchange data with each other in real time. In such a network, mobile systems become an essential part of the IoT's infrastructure[1]. As such, mobile security must be taken into consideration when designing an IoT system. Mobile systems are vulnerable to many security threats. These include network hacking, data interception, malware infection, and authentication spoofing. If these threats are left unattended, it could lead to fraud and even data loss[2]. To prevent such security concerns, advanced techniques need to be adopted to secure mobile systems in the IoT environment. The first step to secure mobile systems is to implement authentication protocols. Using authentication, control access to the system is restricted to authorized users and devices. This prevents hacking and data interception. Additional security techniques such as data encryption and multi-factor authentication can further strengthen the security of mobile networks. Second, it is important to secure mobile devices in the IoT. Backup processes can be implemented to ensure that data is regularly backed up and retrievable in case of accidental data loss[3]. Additionally, malware prevention tools need to be installed to protect the device from malicious activity. This could involve antivirus programs, firewalls, and system hardening to protect the device from malware threats. Last but not least, secure protocols need to be implemented for communication between the various devices and objects in the IoT[4]. This means the use of secure protocols such as TLS/SSL (Transport Layer Security/Secure Sockets Layer), Message Authentication Codes (MACs), and the Internet Protocol Security (IPsec). All of these protocols are designed to ensure secure communication and authentication[5]. The mobile security is an essential element of a secure IoT environment. Authentication protocols, secure mobile devices, and secure protocols for communication need to be implemented to protect networks from malicious activity. Without proper security protocols, the integrity and confidentiality of the system can be compromised. As such, it is important for IoT designers and users to take the necessary steps to ensure robust security for mobile systems[6]. The Mobile Systems security landscape is rapidly evolving with the increasing amount of Internet of Things (IoT) devices and technology now available. From home surveillance systems to smart locks, the security of these systems must be carefully managed to ensure the safety and privacy of the user's data. One major innovation due to the rise of Mobile Systems security is the introduction of mobile agent frameworks. Mobile agents are computer programs that execute tasks on behalf of a user from a mobile system to a remote system. In this way, these mobile agents can monitor the environment in order to look for unusual behavior, detect and correct any security issues, and report back to the security administrator[7]. This increases the time and effort spent on security management significantly, as the administrator can now react quickly to any threats detected immediately. Another Mobile Systems security innovation is the emergence of Context-Aware Security. The construction diagram has shown in the following fig.1

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

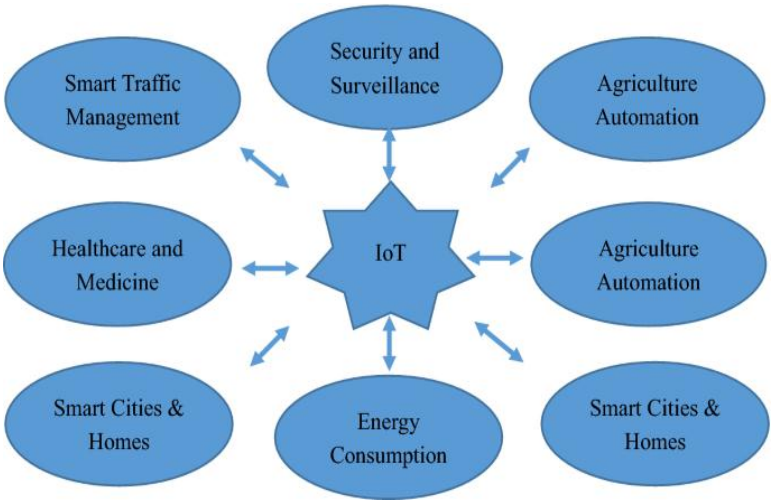

Fig 1: Construction diagram

This technology leverages sensors and Machine-Learning algorithms to customize the security policy of the device in real time. This way, the device can detect a change in its environment and respond with the appropriate security measures to protect the user's data. For instance, if the device enters a location with high density of Wi-Fi networks, the security policy will automatically be changed to block all connections from unauthorized users. This will significantly reduce the chance of unauthorized access to the user's data and information. The use of secure local networks has become increasingly popular as well[8]. This involves creating an encrypted local network that can only be accessed via authentication from the mobile device. This will keep the user's data safe and secure even when in public places. In addition, the system can also be set up to restrict certain abilities depending on the user's permission level, thus reducing the risk of data leakage. All of these innovations are essential to the safety of the user's data, and thus the effectiveness of the Mobile Systems security landscape. By monitoring the environment and responding quickly to any potential threats, users can be confident that their data will remain secure and private[9]. Furthermore, by using secure local networks or restricting user access on public networks, users can be sure that their data will remain safely within private confines. The advent of the Internet of Things has only increased the need for careful protection of personal data, and these Mobile Systems security innovations provide a much needed solution to this growing problem[10]. The main contribution of the research has the following,

- Secure authentication and authorization: Mobile systems help to secure authentication and authorization for IoT devices by enabling multi-factor authentication.
- Secure communication: Mobile systems provide secure communication between IoT devices by utilizing advanced encryption technologies.
- Increased data integrity: Mobile systems are designed to detect and identify malicious activities and protect data integrity.
- Comprehensive security monitoring: Mobile systems can monitor the network for any suspicious traffic and detect any intrusion or attack.

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

- Security patching: Mobile systems provide automated security patching for embedded systems and mobile applications.
- Risk detection and mitigation: Mobile systems help to identify, alert, and mitigate any potential threats and risks before they propagate throughout the system.

Literature Review

The internet of things (IoT) is a network of internet connected objects that are able to transfer data over the internet. As the world becomes increasingly connected, IoT devices are becoming embedded into many aspects of everyday life, from lighting and heating systems to medical equipment and vehicles. However, the widespread use of IoT devices brings forth many potential security issues[11]. The most prominent security issue related to mobile systems and IoT environments is the potential for malicious actors to access private information. IoT devices are often connected to personal networks or home networks; if a malicious actor gains access to the device, they may then have the ability to take control of sensitive data. Attacks on IoT networks have also been known to cause significant disruption, as malicious actors take control of the device or its data. This can cause serious damage to a person's property or their safety, such as turning on and off lights and heating systems[12]. To ensure the security of mobile systems and IoT environments, device manufacturers must implement strong security measures. Strong passwords, restricted access to sensitive data, and encryption technology are all important security measures to ensure the safety of a person's data. IoT devices should also have internal monitoring systems, such as firewalls, intrusion detection systems, and antivirus software. In addition to internal security measures, people should take precautions when using their mobile devices or connecting to IoT networks. It is important to only connect to secure networks, avoid connecting to suspicious networks, and update security on all devices. Furthermore, users should be aware of potential threats and know how to identify malicious actors[13]. The widespread use of mobile systems and IoT devices brings forth many security issues. Device manufacturers must implement strong security measures to ensure the safety of a person's data, and users should take appropriate precautions to protect themselves from potential threats. By taking these actions, individuals can help protect themselves from malware and malicious actors and ensure the security of their mobile systems and IoT environments. The Internet of Things (IoT) environment presents unique security challenges, particularly with regards to mobile systems. With the emergence of billions upon billions of connected devices on the IoT, many of which are smart mobile systems, such as smartphones, tablets, and laptops, security threats from malicious actors become more mobile and complex. This paper will outline the challenges associated with mobile systems security in the IoT environment and provide suggestions for mitigating these threats[14]. One major challenge arises from the use of non-secure communication protocols used in the IoT environment. While many technologies exist that are secure, the use of non-secure protocols leads to data leakage from the IoT to other networks. This may include private information held on mobile systems, which is vulnerable to attacks from malicious actors, or hacker networks which may gain access to sensitive user information[15]. In order to mitigate this threat, organizations must ensure that all protocols used in their IoT environment are up-to-date and secure. Another threat is posed by malicious actors who may attempt to gain access to mobile systems that are connected to the

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

IoT environment. Such malicious actors may be able to gain access and take control of the mobile systems or even use them as a conduits to gain access to sensitive IoT-based applications or data. In order to combat this threat, organizations must deploy secure authentication protocols and other security measures such as two-factor authentication and encryption[16]. Furthermore, users of mobile systems must be aware of best practices, which may include updating their applications, only using trusted applications, and using strong passwords. A challenge posed by mobile systems security in the IoT environment arises from the rapid pace of device use and the frequent deployment of new applications and features. As these new devices and functions are constantly being pushed into the IoT environment, the potential for security breaches increases[17]. To mitigate this threat, organizations must employ rigorous security protocols on the devices they use, such as authenticating users, limiting access to areas of the network, and monitoring networks continuously. Additionally, organizations should also employ threat detection tools and intrusion detection systems to help protect their users from malicious actors[18]. The mobile systems security in the IoT environment presents a unique set of challenges for organizations. In order to mitigate these threats, organizations must deploy the appropriate security protocols and protocols, maintain secure authentication processes, and employ threat detection systems. By taking the necessary precautions and awareness, organizations can protect themselves from malicious actors and secure their mobile systems in the IoT environment[19].

The novelty of the Secured routing scheme for Mobile Systems in the IoT Environment is that it uses a secure data-centric protocol to facilitate secure communication of mobile devices and systems in the IoT. This secure routing approach which is based on a Credit Protocol, uses the Access Point (AP) as the routing protocol for network communication and provides end-to-end encryption of the data packets transferred between mobile systems and APs. The secure data-centric protocol also provides a secure network with authentication and secure communication, by keeping the eavesdropping, tampering and unauthorized access at bay[20]. Additionally, this scheme also acts as an access control system by restricting the access of the malicious and unauthorized devices to the network.

Proposed Model

The implementation of a secured routing scheme for mobile systems in an IoT environment is essential in order to protect the communications between devices. By securing the route taken by data packets, it is possible to ensure that the data is travelling along a secure path and that any malicious packet transmissions are intercepted and blocked. The main goal of a secured routing scheme in an IoT environment is to ensure that the data transmissions between two endpoints remain private and secure. To achieve this, the implementation of encryption protocols is required. This enables the data to be encrypted prior to transmission, thus ensuring the confidentiality of the data whilst in transit. Additionally, authentication protocols can be used to validate messages to ensure integrity and prevent malicious tampering. Another important security measure that can be taken is implementing end-to-end security. This means that the data transmitted between two endpoints is secure from the source to the destination. End-to-end security can help to ensure that there are no breaches of

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

communication within the network. The implementation of a distributed denial of service (DDoS) protection algorithm should also be taken into account. This algorithm works by identifying malicious traffic and blocking it, thus protecting the secure transmission path. The implementation of a secured routing scheme for mobile systems in an IoT environment is necessary in order to ensure the privacy and security of communications. Using a combination of encryption protocols, authentication protocols, end-to-end security and DDoS protection algorithms can provide an effective and secure environment for data transmission.

Construction

The Internet of Things, or IoT, is the popular term for the rapidly expanding network of internet-connected devices that consists of billions of electrical interconnected devices ranging from the mundane items such as Smartphone and washing machines to the more complex machines like robots and 3D printers. In an IoT environment, secured routing is essential for smooth operations of the devices and networks involved. Secured routing is enabled by the use of various security measures and protocols to ensure the safe communication of the data, instructions and control signals from the devices, networks and other sources. The main security measures implemented in a secured routing scheme for IoT systems are authentication, authorization, confidentiality, integrity, availability and non-repudiation. Authentication ensures only authorized users can access the system and ensures only legitimate devices can be connected. Authorization grants permission to specific users or devices based on the characteristics and behavior of the individual or the device. The functional block diagram has shown in the following fig.2

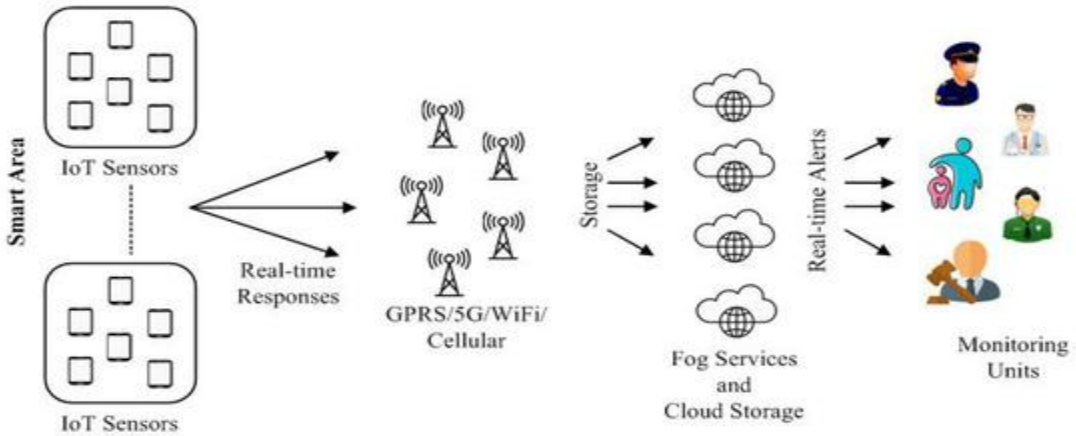

Fig 2: Functional block diagram

Confidentiality guarantees that data or instructions sent over the network cannot be accessed by unauthorized users or devices. Integrity controls how messages and information can be handled by ensuring that the message does not get corrupted during transit. Availability is ensures that the devices have access to the network and resources when they need them, while non-repudiation ensures that the sender of the message cannot deny that they transmitted it. In addition to the primary security measures mentioned above, the secured routing scheme should also make use of cryptographic technologies, such as encryption and

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

digital signatures, to further secure communication between the IoT devices. Encryption scrambles data before it is sent, making it difficult to decode. Digital signatures serve to authenticate data and the sender of the data. The use of these cryptographic techniques can also be used to protect and authenticate data exchanged between different IoT devices. In order to secure the communication in an IoT system, the network should also be provided with robust firewalls and intrusion detection systems to identify and stop any malicious activity. The firewalls should be able to identify suspicious traffic and detect any changes in communication patterns. Furthermore, the network should be provided with an end-to-end trust model to make sure that any data moving across the network has not been tampered with. The secured routing scheme should also make use of reputation-based algorithms to ensure the trustworthiness of devices interacting with the system. The device reputation can be based on the history of the devices and the way they behave over a period of time. The use of reputation-based algorithms coupled with analytics-based techniques will further strengthen the security of the network. The secured routing is essential to ensure security and safety of the data and communications over an IoT system. The primary security measures, along with the use of cryptographic technologies, firewalls and intrusion detection systems, and reputation-based algorithms will help provide a secure and robust network.

Operating Principle

A secure routing scheme for mobile systems in the Internet of Things (IoT) environment is a system which helps to secure the communication between nodes in the network. This security is provided by creating one or multiple secure paths for the data communication within the system and also between other external systems. The main operating principles of this secure routing scheme are:

- Encryption: One of the first steps in secure routing is to secure the data by encrypting it before it is transmitted. This prevents unauthorized third-party access and prevents eavesdropping.
- Authentication: Authentication is used to validate the identity of the parties involved in the exchange of data. This helps to ensure that the data is not transmitted to an unauthorized third-party.
- Authorization: Authorization is used to control the access to data by specifying which nodes can access the data and which nodes cannot. This is typically implemented through a mechanism such as role-based access control.
- Quality of Service (QoS): QoS is used to ensure that data transmissions are properly managed and that the transmission time is minimized. This is especially important for real-time data transmissions.
- Mobile Node Authentication: Mobile nodes need to be authenticated before they are allowed into the network. This helps to ensure that only authorized nodes have access and that any nodes that are included in the system are trusted.
- Packet Flow Control: Packet flow control is used to manage the flow of data between the nodes in the system. This is essential for ensuring that the network is functioning properly and that data is being sent and received properly.

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

- Secure Communication Channels: Secure communication channels are used to ensure that the data is exchanged in a secure environment. This is typically done by using encryption algorithms to protect the data and also by implementing authentication and authorization.

Functional Working

The Internet of Things (IoT) is one of the most dynamic and innovative areas of technology today, bringing tremendous potential for advancements in communication, automation, and data analytics in both the consumer and industrial worlds. Connected devices are an increasingly important part of all aspects of business and industry, and the secured routing scheme is the foundation of enabling information exchange among devices in an IoT environment. The operational flow diagram has shown in the following fig.3

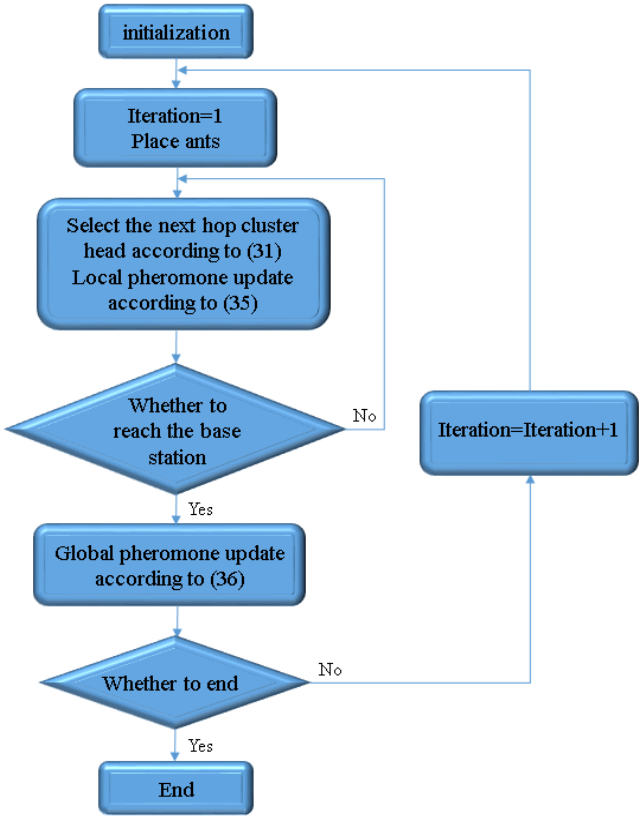

Fig 3: Operational flow diagram

Secured routing schemes provide a layer of protection between the IoT sensor nodes and the Internet by ensuring that malicious actors cannot access or interfere with the data being sent through the network. Routing security includes authentication, authorization, and encryption of data that passes through the network, as well as the prevention of network intrusions and data tampering. Authentication is a process in which a node ensures its identity has been verified by the receiving devices. This can be achieved by providing a unique identifier to the receiving devices and then the devices including the routing node will validate the identity of the sender. This will enable the securing of data and stop malicious actors from attempting to

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

access the data when it is in transit. Authorization is the process in which an entity is allowed access to and use of data on an IoT network. This is essential as it prevents non-authorized users from intercepting or altering data during its exchange. Authorization is achieved through authorization codes, digital certificates, and access control lists, as well as other security measures.

2. RESULTS AND DISCUSSION

Encryption is the process of encoding data so that it cannot be interpreted by anyone other than the intended recipients. This ensures that any data that passes through the network is protected and safe. Standard protocols such as TLS (Transport Layer Security) can be used in conjunction with various encryption algorithms to ensure that the data is secured and cannot be decrypted without a valid decryption key. The proposed Secured routing scheme (SRC) has compared with the existing Game theory oriented approach (GTOA), Trust architecture model (TAM), RPL routing protocol (RPLRP) and intelligent trust evaluation scheme (ITES)

Estimation of accuracy

Secured routing schemes for mobile systems in the Internet of Things (IoT) environment can be highly accurate if implemented correctly. Such schemes involve authentication of nodes in the network, ensuring a secure route between nodes, providing secure data transmission to the destination, and preventing denial of service attacks. Secure routing schemes also help to protect personal data stored on mobile devices in the IoT environment. Fig.4 shows the estimation of accuracy

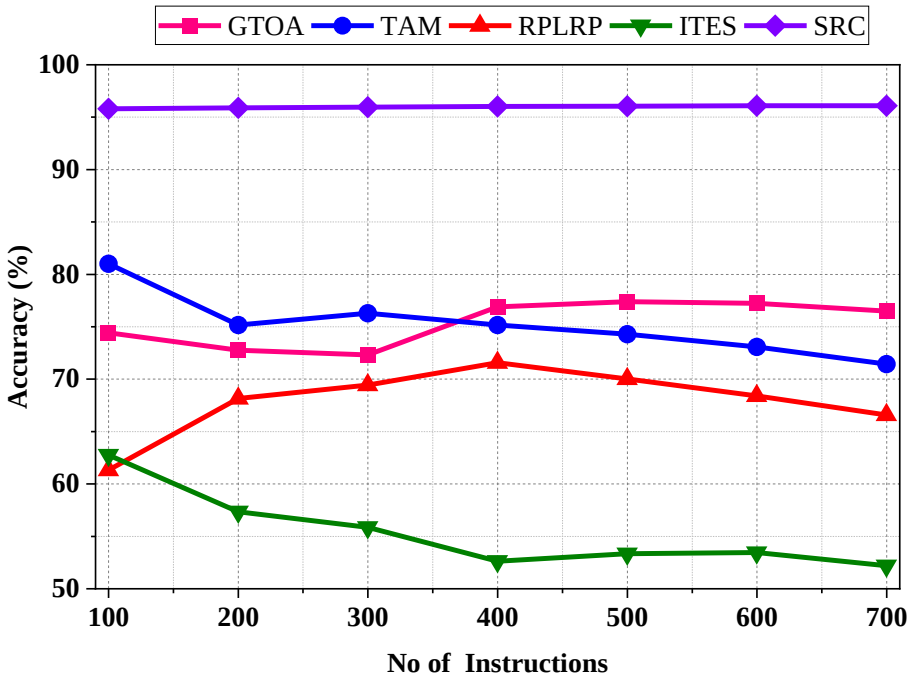

Fig.4: Estimation of accuracy

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

These schemes can provide high levels of accuracy by using cryptographic techniques and algorithms to provide authentication, authorization, and data integrity checks. Additionally, various methods such as link-level encryption, IPSEC, TLS, and SSH can be used to increase the accuracy of the secure routing scheme. Additionally, regular monitoring and updating of security features on the network can help to ensure the accuracy of the secure routing scheme.

Estimation of Precision

The precision of a secured routing scheme for mobile systems in the Internet of Things (IoT) environment largely depends on the implementation of the particular system being used. Generally speaking, a secured routing scheme includes measures to detect and prevent various types of attacks, such as man-in-the-middle attacks, denial of service attacks, and eavesdropping. It also ensures the secure transport of data between two or more points and provides authentication for different nodes involved in the communication. Fig.5 shows the estimation of precision

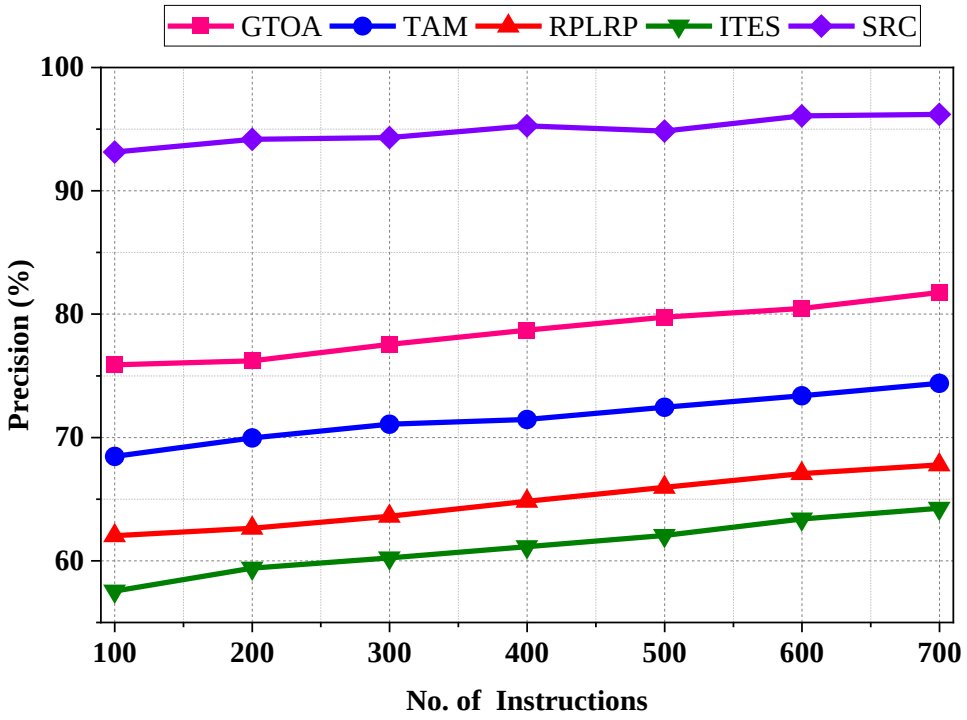

Fig.5: Estimation of precision

The precision of a secured routing scheme is determined by various factors, including the cryptographic algorithms used for the encryption of transmitted data, the implementation of authentication methods, the use of routing protocols for dynamic path selection, and the data verification methods. Additionally, precision is influenced by the security policies in place and the level of security recommended by the scheme itself. To achieve the highest level of precision, these components must all be configured correctly and regularly assessed for

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

vulnerabilities. Additionally, the adoption of real-time monitoring systems and an efficient incident response plan further reinforces the security of the system.

Estimation of Recall

The recall of the Secured Routing Scheme for Mobile Systems in the Internet of Things (IoT) Environment is a proposed system that would enable security and privacy in the routing of data between devices connected to the Internet of Things. The system would use an agent-based approach that would secure the data being sent and received by each device. The proposed routing protocol would authenticate each connection request sent from a device and verify the credentials of each connected device. The system would also facilitate the exchange of cryptographic keys between devices, which would be used to encrypt data for transmission. Fig.6 shows the Estimation of Recall.

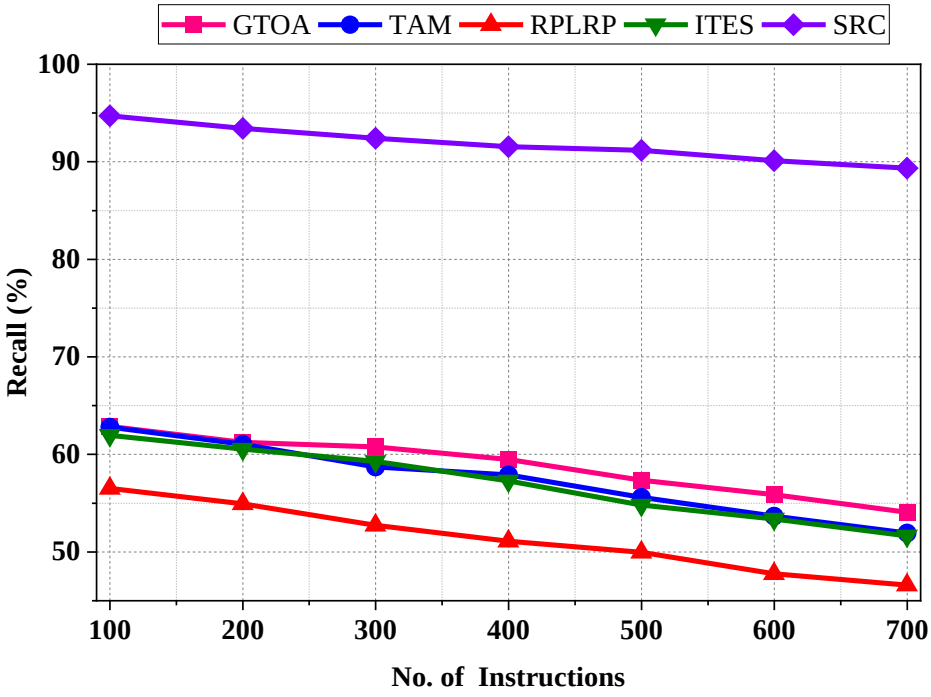

Fig.6: Estimation of Recall

The proposed system also would provide multiple layers of defense against potential security challenges, such as malicious attacks, accidental errors, and eavesdropping. By implementing this secured routing scheme, IoT environments would be able to protect their data against potential security threats, while enabling a reliable, secure communication system between the devices.

Estimation of F1-score

The F1-score of a Secure routing scheme for Mobile Systems in the Internet of Things (IoT) Environment is a measure of the performance of the security protocol used to protect

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

communication between mobile systems over the internet. The score is calculated by taking into account a combination of true positives, false positives, true negatives, and false negatives. Fig.7 shows the estimation of F1-score.

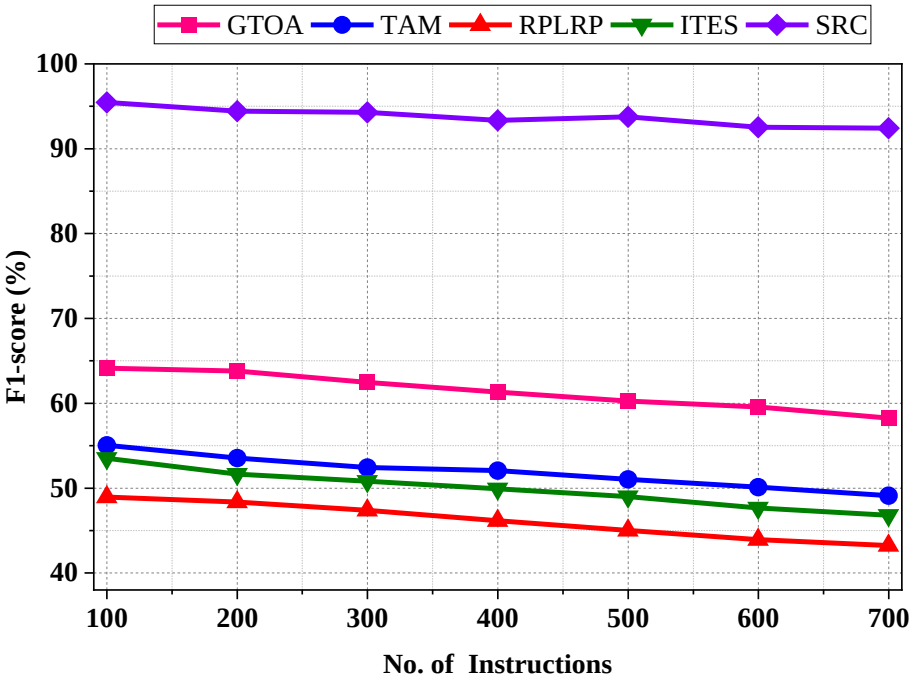

Fig.7: Estimation of F1-score

True positives are packets that were correctly identified as secure, while false positives are those that were falsely identified as secure. True negatives are packets that were correctly identified as non-secure, while false negatives are those that were falsely identified as non-secure. The higher the F1-score, the more reliable the security protocol is in protecting data and resources in the IoT environment.

3. CONCLUSION

The Secured routing scheme for mobile systems in the Internet of Things (IoT) environment is a comprehensive set of protocols and algorithms that allow for improved security and trust in connecting different IoT devices. It aims to ensure that communication between devices is secure, reliable and traceable. By using secure routing protocols, the system is able to authenticate and authorize communication between devices as well as protect and encrypt data in transit. The scheme also includes systems which can monitor the environment in order to detect malicious traffic or users attempting to exploit security vulnerabilities. Furthermore, the scheme also enables traceability and accountability for remotely connected devices and users. This is achieved through the use of digital signatures, authentication certificates and other methods.

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

4. REFERENCES

1. Muzammal, S. M., Murugesan, R. K., & Jhanjhi, N. Z. (2020). A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches. IEEE Internet of Things Journal, 8(6), 4186-4210.
2. Rani, R., Kumar, S., & Dohare, U. (2019). Trust evaluation for light weight security in sensor enabled Internet of Things: Game theory oriented approach. IEEE Internet of Things Journal, 6(5), 8421-8432.
3. Almusaylim, Z. A., Alhumam, A., & Jhanjhi, N. Z. (2020). Proposing a secure RPL based internet of things routing protocol: A review. Ad Hoc Networks, 101, 102096.
4. Chen, J., Tian, Z., Cui, X., Yin, L., & Wang, X. (2019). Trust architecture and reputation evaluation for internet of things. Journal of Ambient Intelligence and Humanized Computing, 10, 3099-3107.
5. Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. Journal of Computer Networks and Communications, 2019, 1-14.
6. Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems, 93, 860-876.
7. Khatua, P. K., Ramachandaramurthy, V. K., Kasinathan, P., Yong, J. Y., Pasupuleti, J., & Rajagopalan, A. (2020). Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues. Sustainable Cities and Society, 53, 101957.
8. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294.
9. Wang, T., Luo, H., Jia, W., Liu, A., & Xie, M. (2019). MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things. IEEE Transactions on Industrial Informatics, 16(3), 2054-2062.
10. Guleng, S., Wu, C., Chen, X., Wang, X., Yoshinaga, T., & Ji, Y. (2019). Decentralized trust evaluation in vehicular Internet of Things. IEEE Access, 7, 15980-15988.
11. Haseeb, K., Almogren, A., Ud Din, I., Islam, N., & Altameem, A. (2020). SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things. Sensors, 20(9), 2468.
12. Wang, T., Qiu, L., Sangaiah, A. K., Liu, A., Bhuiyan, M. Z. A., & Ma, Y. (2020). Edge-computing-based trustworthy data collection model in the internet of things. IEEE Internet of Things Journal, 7(5), 4218-4227.
13. Zaminkar, M., & Fotohi, R. (2020). SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism. Wireless Personal Communications, 114(2), 1287-1312.
14. Wang, D., Zhong, D., & Souri, A. (2021). Energy management solutions in the Internet of Things applications: Technical analysis and new research directions. Cognitive Systems Research, 67, 33-49.

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02 , No.02 , Feb-Mar 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.22.8.21

15. Marques, G., Ferreira, C. R., & Pitarma, R. (2019). Indoor air quality assessment using a CO 2 monitoring system based on internet of things. Journal of medical systems, 43, 1-10.
16. Mbarek, B., Ge, M., & Pitner, T. (2020). An efficient mutual authentication scheme for internet of things. Internet of things, 9, 100160.
17. Qureshi, K. N., Rana, S. S., Ahmed, A., & Jeon, G. (2020). A novel and secure attacks detection framework for smart cities industrial internet of things. Sustainable Cities and Society, 61, 102343.
18. Jiwani, N., & Gupta, K. (2018). Exploring Business intelligence capabilities for supply chain: a systematic review. Transactions on Latest Trends in IoT, 1(1), 1-10.
19. Jiwani, N., Gupta, K., & Whig, P. (2021, October). Novel healthcare framework for cardiac arrest with the application of AI using ANN. In 2021 5th international conference on information systems and computer networks (ISCON) (pp. 1-5). IEEE.
20. Gupta, K., & Jiwani, N. (2021). A systematic Overview of Fundamentals and Methods of Business Intelligence. International Journal of Sustainable Development in Computing Science, 3(3), 31-46.