International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5730
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

An Implementing A Continuous Authentication Protocol To Improve Robustness Security Threats On IoT Using ESP8266

P. Ramadevi[1], B.Manikandan[2], T.Jayasankar[3]
[1]Associate Professor,
Department of Electronics and Communication Engineering, University College of Engineering , BIT Campus, Anna University, Tiruchirapalli, 620025, India
ramadevi.mohan@gmail.com
[2]Assistant Professor,
Department of Electronics and Communication Engineering, University College of Engineering ,BIT Campus, Anna University, Tiruchirapalli, 620025, India
profmani.ece@gmail.com
[3]Assistant Professor,
Department of Electronics and Communication Engineering, University College of Engineering, BIT Campus, Anna University, Tiruchirapalli, 620025, India
jayasankar27681@gmail.com

Abstract
The Internet of Things (IoT) is a network of physical things that are outfitted with sensors, software, and other technologies that are able to communicate and exchange data with other devices and systems over the Internet. Because of the diversity of their surroundings, IoT systems are sensitive to network attacks. The IoT could be the source of these dangers and attacks. There are a lot of devices that communicate with each other via the IoT, and one of the most critical components of this is to maintain IoT security. IoT devices are a prime target for attackers and pose a serious risk of impersonation during a call. Proposals to prevent session hijacking in device-to-device communication are made in this research study. User-to-device authentication relies on usernames and passwords, but continuous authentication doesn't. This protocol relies on device features and contextual information. Moreover, this protocol reduces the synchronization losses using shadow IDs and emergency key. In addition, the protocol's robustness will be tested by providing security and performance analysis.

1. INTRODUCTION

Since the invention of writing, people have attempted to hide information in written form. There are examples of cryptographic systems in papyrus and inscriptions in stone that suggest that many ancient cultures established cryptographic systems. Scale was the earliest cypher device used by Spartans to communicate discreetly between military commanders in the early 400s BC. Today's cryptography is far more complicated than its predecessors because, in addition to military consequences, it has been developed to protect electronic data stored and transmitted through unsecure networks all over the world. Secrets2. of business, the military, and higher learning and research institutions, amongst others. With the Internet of Things, for example, everyday objects will be equipped with microcontrollers, digital transceivers, and protocol stacks that will allow them to communicate with one another and with users, thereby becoming part of the internet. Concepts like IoT are designed to broaden the Internet's reach and make it more omnipresent. By making various devices, such as home appliances, security cameras, monitoring sensors, actuators, displays, vehicles, and so on easily accessible and interoperable, the Internet of Things will also encourage the development of new applications that utilise the potentially enormous amounts of data generated by these and other objects. A wide range of industries can benefit from this paradigm, from home automation and industrial automation to medical assistance and mobility for the elderly to intelligent energy management and smart grids and autos. All Internet-connected devices are at risk of cyberattacks. There are two types of parties, one that has been hacked and the other that does not know it has been hacked, according to the saying. This sentence illustrates how vulnerable we are at all times. It all boils down to who is the least at risk. We can't safeguard our computers from online attacks unless we know what they are and how to spot them. Each and every threat on the Internet of Things has a reason for

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5730
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

existing. Depending on who the invader is trying to get to, the goal may be different.

One of the most important concerns facing the IoT business is the ease with which devices can be exposed to the public. Open invitations to troublemakers are provided by any equipment left unattended or in plain sight. IoT devices, in the vast majority of circumstances, are not vulnerable to third-party vulnerability. As a result, an intruder might easily grab the device and use it to connect to another device that contains damaging data. In this way, they are able to extract and modify cryptographic keys, alter programming, and install harmful devices. Privacy and security could be in jeopardy with all those sensors monitoring your every move. You can tell when you wake up because your smart coffee maker is on, and how well you brush your teeth because your smart toothbrush is on, and what radio station you're listening to because your smart speaker is on, what you're eating because of your smart oven or fridge, and who is visiting you because of your smart toys (thanks to your smart doorbell). Despite the fact that corporations will make money by selling you the smart item initially, their IoT business model almost certainly includes selling at least some of the data generated by that smart thing. Many fields, such as information technology, healthcare, data analytics, and agriculture, are being challenged by the Internet of Things. As the primary driver of many other issues, including government involvement, privacy is a top priority. Government, civic society, and business sector efforts will play a critical role in ensuring that the following values are protected: When a massive network of internet-enabled devices grows to include billions of nodes, massive amounts of data must be processed. Scalability is required for the system that stores and analyses the data from these IoT devices. In today's Internet of Things (IoT) era, everything is connected to the Internet. Big data analytics and cloud storage are needed to make sense of the raw data generated by these devices.

An assault on a cryptographic system by exploiting flaws in a code, cypher, cryptographic protocol, or key management technique is known as a cryptographic attack. The actions of the attacker are often used to characterise attacks. Passive or active attacks are thus possible. The primary objective of a passive attack is to gain access to confidential data. Passive attacks include, for example, listening in on a communication channel and intercepting and eavesdropping. These are passive activities since they don't interfere with the flow of information or interrupt conversation. A passive attack is typically interpreted as stealing data. By definition, an active attack is one in which the information is being altered in some way. Making unlawful changes to the data, for example. Sending out information that was not meant to be sent. Changing information connected with authentication, such as the name of the originator or the timestamp, Inappropriately erasing files. In a user impersonation attack, an attacker pretends to be an employee of a company in order to steal money or other confidential information. These types of attacks are frequently perpetrated by assailants who have their sights set on business leaders. For the bad guys, it's all about getting money into a bogus account, disclosing confidential information, or gaining access to a company's network. Cyber-attacks that try to disable a computer or other device from serving its intended users by interfering with its normal operation are known as denial-of-service (DoS) attacks. Typical DoS assaults are designed to overwhelm or flood a target computer with requests until normal traffic is unable to be handled, resulting in denial-of-service to additional users. A DoS attack is defined by the fact that it is launched from a single computer. In a DDoS assault, several distributed sources, such as a Mirai botnet, Hajime, and Reaper DDoS attack, are used to disrupt service. If the communication has been received by the correct person or if it was sent by the correct person, verifying the identity of the receiver or sender. During network contacts, a user's authenticity can be verified by allowing a human-to-machine transfer of credentials, a process known as "user authentication."

2. IoT Security Threats

Communication is no longer a one-way street in an Industry 4.0 environment. Increasing interconnectivity of systems is expected to continue in the years to come. Managers and workers on the ground who operate and repair machines will both expect readily available information at all levels. Systems that were originally intended to be completely self-contained may eventually be linked to other systems in order to make better use of their resources on a global scale. For example, connecting well-tested but isolated legacy systems to new and expanding services over the Internet can help keep these useful legacy systems rather than making them obsolete. IoT systems in particular should be developed from the start to allow for seamless integration with other systems at any moment in a controlled and relatively simple and seamless manner. To assist the notion of Cyber-Physical Systems (CPS), which opens up new business prospects via the Internet of Services, Industry 4.0 technology uses the Internet of Things. Cloud Manufacturing is another name for Internet of Services in the manufacturing industry. New business practises are introduced by the notion of Servitization, which focuses on delivering a service to a consumer rather than selling a product, although the product itself remains the property of the maker. It is important to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5730
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

note that this strategy presents new difficulties for manufacturers, as it leaves them responsible for all the tasks associated with providing Through-Life service, which includes everything from the creation of the product to the eventual recycling or disposal of it after its useful life has ended. For example, the Internet of Things can be useful in many ways in this situation. For example, real-time data can be acquired for the monitoring of products and processes.

Paper organisation

The remaining thing of this paper present that the Literature Survey in the third section. The proposed part is signified in proposed methodology. The result and discussion sectioned also presented. Finally the conclusion of the paper is represented in last section.

3. Literature Survey

Smart card authentication in a wide range of services, including e-commerce, e-learning, and more, has made our lives easier. Multidimensional fields including transportation, access control and logistics, manufacturing, inventory management and asset management can all benefit from technological advancements as well as e-health. If an intruder gets into the authentication process, it will be expensive and dangerous for society, thus there is an increasing need for secure and private authentication techniques to ensure that service seekers and low-cost tags are both legal and legitimate.

One-way hash chains were pioneered by Lamport [1] in 1981, but his approach depends exclusively on passwords and verification tables to authenticate distant users via an insecure means of communication. In the early days of remote user authentication, passwords were the only means of verifying identity. After that, the method of a dynamic identity-based remote user authentication system was created to safeguard the anonymity of users. To prevent ID thefts, Das et al.[2] first proposed a dynamic identity-based remote user authentication technique employing smart cards, but the protocol fails to establish user anonymity and is vulnerable to insider assault, masquerade attack, or server spoofing.

Attacks such as offline password guessing, impersonation, server masquerade, and insider threats can all be carried out with Chang et alprotocol's help. There are weaknesses in the password-changing process, and no way to transmit session keys in the future, according to them. This was followed by the development of an enhanced remote user authentication system with key agreement, which claimed to be more secure, efficient, and suitable for real-world applications. Security Enhancement of Improved Remote User Authentication Scheme With Key Agreement demonstrated that their proposed mechanism was completely collapsed as an adversary can easily obtain not only the security parameters of protocol but also the common session key for future communication between user and server. Aside from that, the attacker possesses a copy of the password used by the registered user and the secret key stored on the server.

According to Sarma et al., the shortage of tag resources in 2003 was a major issue to providing security and privacy for low-cost RFID systems. [4 They recommended the use of simple cryptographic primitives and protocols that take into consideration the resource limitations of RFID tags as a way to improve security. To address the security concerns of restricted devices, several authentication methods [150] known as lightweight or low cost devices have been created specifically for this market niche. To begin the first step toward privacy, Juels et al. [5] suggested that the tag should be destroyed at the point of sale. But it's not practical because all previous communication details have been erased from the database. To further secure the tag, in 2004, Weis et al. [6] suggested an access control method based on a random key's hash as its metaID. However, the tag may be monitored because the same metaID is used several times [7]. Randomized access control (RAC) was also proposed by Weis et al., which encrypts the ID of the tag with a random number. Although it can be replayed, it still does not enable backward tracing due to the fixed ID of the tag. In accordance with the EPC global framework, Lopez et al. [8] proposed an authentication mechanism for low-cost RFID tags. For low-cost RFID tags, EPCglobal and the International Organization for Standardization (ISO) established worldwide specifications in 2006. The most pressing issue with these requirements was the lack of attention paid to security concerns. This problem was addressed by Konidala et al. [9] in their scheme. If numerous sessions are available, Lim and Li [10] demonstrated that passive eavesdropping might be used to obtain passwords from their approach.

In compliance with the EPC Class 1 Generation 2 standards, Chen and Deng [11] introduced a new RFID authentication and encryption mechanism in 2009. A pseudo-random number generator and cyclic redundancy code function assure user privacy and RFID security between tags and readers. An opponent can successfully trace the tag in by mimicking either the tag or the reader, as Lopez et al. [12] discovered in 2011. They are also vulnerable to denial of service attacks. Finally, a new EPC-friendly protocol has been proposed to provide high security for Gen-2 compliant tags in order to overcome these observed weaknesses.

The GPS-enabled mobile sensor nodes are offered as a location strategy for three-dimensional wireless sensor networks (Vibha Yadav et al., 2009). A three-dimensional

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5730
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

space is used by a WSN localization process that does not require a range. Static and mobile sensors should make up the sensor network. Sinalgo is used to model this strategy. It is compared to the current chord selection method based on the simulation results. The average localization error, average localization time, and beacon overhead are the performance measures used to evaluate the localization system.

In wireless sensor networks, a cooperative localization approach has been developed (Hongyang Chen et al., 2009). It takes into account the presence of obstacles in wireless sensor networks with mobility assistance. Static sensor nodes work with a Mobile Anchor (MA) node, which actively moves to improve location performance. By adjusting the mobile anchor node's transmission range, the localization accuracy can be further improved. MAs and static sensors work together in this approach to maximise the utilisation of beacon signals by considering the availability of relay nodes.

4. Symmetric and Asymmetric Cryptography

In order to increase the computational hardness of algorithms and to enable the confidentiality of communication, cryptographic techniques will be categorized into following main classes based on nature of the keys.

Symmetric Cryptography In symmetric cryptography, there is a single ecret key which is shared between sender and the receiver. Symmetric key algorithms generate a secret symmetric key $k \in K$ in a polynomial time which will be used for encryption as well as for decryption. Encryption algorithm $ek \in E$ encrypt the message $m \in P$ to a ciphertext $c \in C$ by using key k.

Asymmetric Cryptography In every participating entity has its own key pair, made up of a publickey (which is distributed freely to public) and private key. Public key algorithms generate a key pair $(pk, sk) \in K$ in a polynomial time in which public key pk is used for encryption while private secret key sk is used for decryption.

5. Problem Statement and Rectification

It's becoming increasingly difficult for businesses to maintain physical boundaries, and as a result, the risk environment is becoming more perilous. Cyber-Physical Systems (CPS) that are enabled by the Internet of Things (IoT) are vulnerable and at risk. This heterogeneous ecosystem, where billions of devices are interconnected, can be used in very sensitive and protected environments. The Internet of Things (IoT) Prior to encrypting the data, we need to verify that the node is permitted to do so. The entire network is at risk if an unauthorised node enters the network, or if one device in the network is compromised. it will result catastrophic damage so every node enters into the network should be authenticated and end device and gateway should also be authenticated mutually. When considering device to device, a more concern need to secure the communication where the static authentication is used to authenticate the device at the beginning of the session but it happens once at the beginning. Intruders can takes place on the ongoing session and can interrupt the communication or perform some attack. Suppose advisory node impersonate and enters into the network as legitimate user at the beginning of the session they can perform attacks on network or can steal the information about the session so it is necessary to authenticate the ongoing session. On considering the above challenges, there is a highly demand for a protocol which is robust on preventing the IoT network from impersonation, session hijacking and some of other attacks. IoT consists of different types of sensor nodes which has to sense different types of environment and the important factor considered the most is enable those end devices to communicate over the internet. With the rapid proliferation of IoT devices comes a accumulation of data – data that offers a host of insights while also posing a host of security and privacy risks. The volume of sensor data can also be used by both attackers and legitimate users to compromise user's security and privacy. While processing a large amount of data, Memory dump attack will happen. It is impossible for IoT devices to protect themselves from attacks since they are confined in terms of memory, CPU, battery, and power. As a result, IoT characteristics necessitate the development of specific techniques. It is common for many solutions to use static authentication, which only checks the user or device once in the course of the entire session. Because it only validates the user at the start of each session, this method of authentication is vulnerable to attacks like Session Hijacking. To put it another way, an attacker can hijack a genuine session by masquerading as one. This is called an Impersonation Attack. With this in mind, let's imagine a smart house equipped with sensors that collect data about the home's condition and send it to the gateway for storage in a cloud service. Sensors are validated by the gateway for each session, but if an attacker steals this legal session and impersonates a real user, there is a major problem that needs to be addressed. The attacker can then gain access to all of the system's data and privileged services. Since they'll have to get inside your home, the attacker may attempt a variety of destructive things, such as gaining entry, spying on you using a camera or changing your electricity usage.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5730
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

6. IoT Stack Security Issues

Consider the security of the entire Internet protocol down to the Edge when thinking about IoT. Tier 3 and higher would entail ignoring any possible IoT security vulnerabilities that arise directly from the data creation and preprocessing stages. Tier 3 and higher security tiers often use well-developed Internet technology. At this level, security technology and dangers are well-understood, supported by consensus standards, and strictly regulated. There are a number of IoT standards being developed by several consortia, including AllJoyn, Thread, OCI, and the Industrial Internet Consortium (IIC).

7. Proposed methodology

Determining how devices can be authenticated during a session using their unique attributes, and how this may be done continuously. Between security and IoT, the limitations of restricted software and hardware capabilities can be circumvented by applying lightweight computations (HMAC, hash, XOR). Using a combination of a Shadow ID and an Emergency Key to ensure that data is not lost in transit. Additionally, a non-formal analysis of the protocol's security and resilience can be performed.

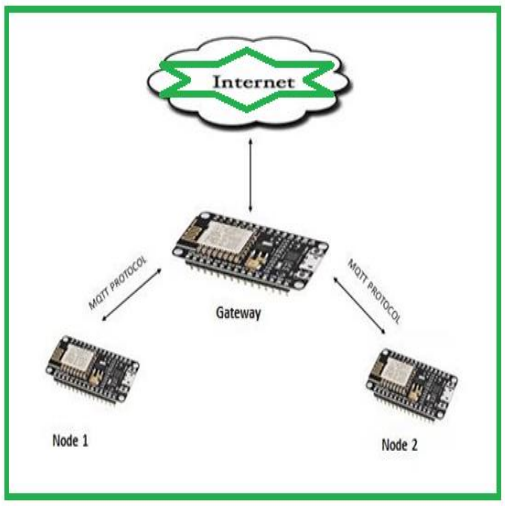

Figure 1: projected implementation ideal

As depicted in Figure 1, the proposed implementation model is depicted. One gateway and two end-node IoT devices are used to distribute an authentication system in order to achieve real-time response. In the initialization step, critical sensor and gateway parameters are set up. Authentication that is constant across time: Static authentication involves the gateway and sensors verifying each other's identities at the start of each session. Continual authentication is used while the device is re-launching new static authentication after the authentication period has expired. Constant authentication uses a token and the context of a user's device to authenticate a user throughout the session.

Security Analysis

Additional security features include mutual authentication and tag anonymity as well as backward and forward traceability, man-in-the-middle and cloning-attack-resistant synchronisation, as well as de-synchronization attacks, impression attacks, and replay attacks.

8. Result and Discussion

To complete the Continuous Authentication between node and gateway, try to establish the one way communication by sending data from node to gateway. Try to establish a mutual communication between node and gateway by node sending a value to gateway after receiving the value, the gateway send a value with an acknowledgement to node and further they can mutually communicate. After mutual communication, set a parameters for Initialization phase. When setting the parameters, we faced a difficulties on storing and transmitting the data from node to gateway, then we choose JSON to resolve the above problem. In this project, Arduino IDE is used. Many of the Arduino IDE in build functions help us to perform computations much easier but there is a minimum libraries for cryptography, security and lightweight computations so we need libraries from outside of Arduino IDE.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5730
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

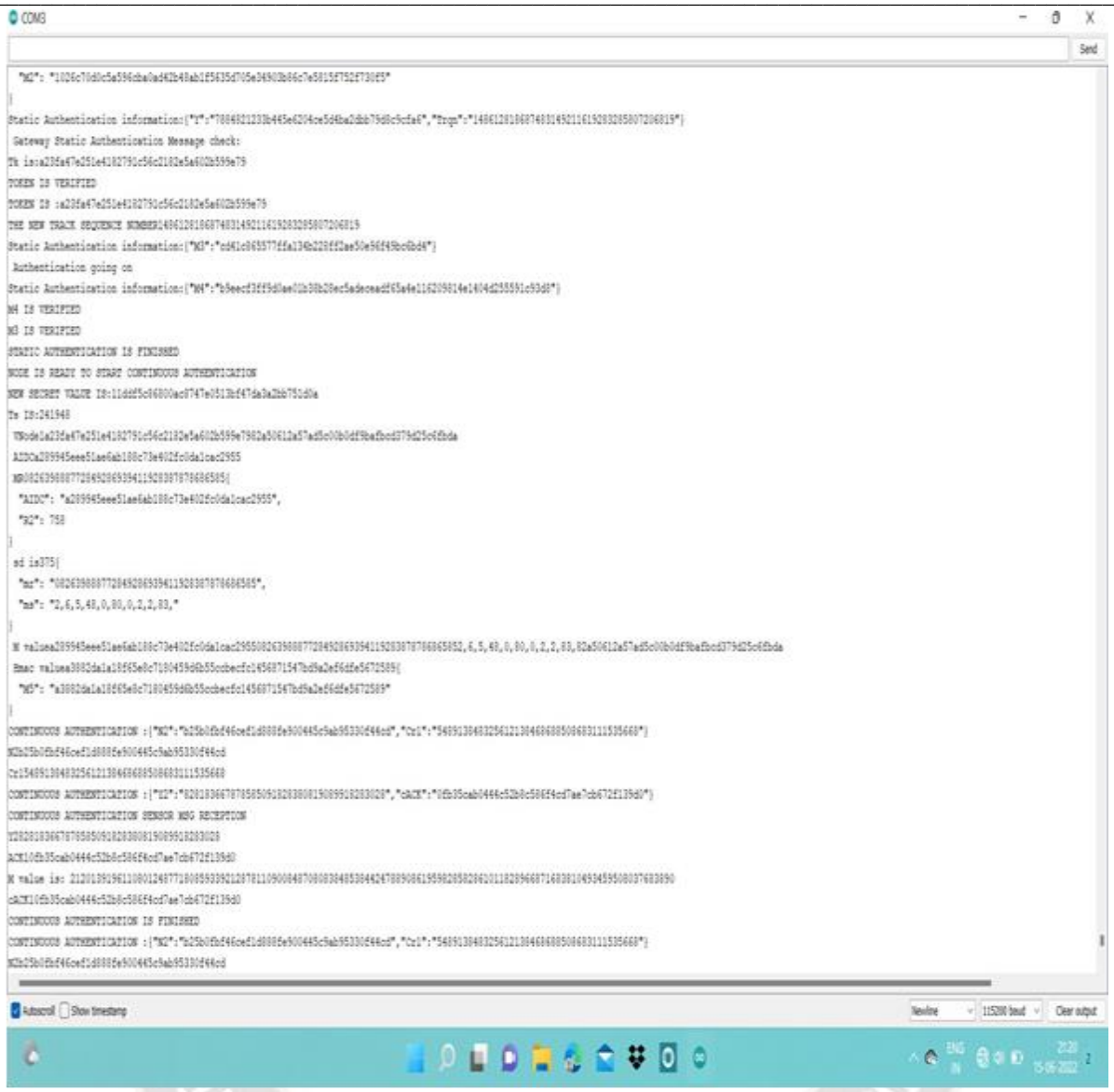

Figure 2: A verifying the gateway parameters and continuous authentication is finished Node authenticate the gateway

Table 1: Percentage wise Improvement at varying Range

Range	Delay (%)	Delivery Ratio (%)	Energy (%)
250	3.95161	10.3255	8.65161
300	3.9546	9.6532	10.6551
350	4.2549	11.6556	6.2515
400	4.2668	10.8949	7.6542
450	3.93154	11.8994	9.8221
500	4.35898	9.81616	10.3256

Table 1 presents the percentage wise improvement for varying the range.

Table 2: Percentage wise Development of SATL for varying Attackers

Attackers	Delay (%)	Delivery Ratio (%)	Energy (%)
1	3.251	3.6161	6.75
2	4.665	5.2145	5.42
3	5.985	6.9851	6.98
4	6.442	7.3651	5.78
5	8.521	8.5462	4.52

Table 2 shows the percentage wise improvement for varying the attackers.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5730
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

9. CONCLUSION

In this proposed model to reduce computational cost, we focus on utilising the device's single feature instead of using too many features. We implement a client-server 0continuous authentication protocol. The protocol utilise RSSI to continuously authenticate IoT devices. As IoT devices have limited software and hardware constraints, We focus lightweight cryptography computation function such as HASH, HMAC and XOR in this protocol. We use MQTT communication protocol which is one of the most commonly used protocols in IoT so that the proposed project can be applicable to all IoT networks. On implementing the protocol in very basic developer kit, Because of this, we can guarantee that the protocol can be used on lower-end devices with less processing power. i. Designing a D2D continuous authentication protocol, which exploits the capabilities of the devices to validate devices continuously during the session. The limitations of restricted software and hardware capabilities can be solved by leveraging lightweight computations such as HMAC, hash, and XOR between security and IoT. Using a combination of a Shadow ID and an Emergency Key to ensure that data is not lost in transit. Due to node movement, route breaking is common in wireless sensor networks, which makes mobility even more difficult. The need for frequent position updates from a mobile node to establish routing arises from the fact that mobile wireless sensor networks consume sensor nodes' battery supplies and cause collisions.

10. Reference

[1] Alladi T, Chamola V. HARCI: A two-way authentication protocol for three entity healthcare IoT networks. IEEE Journal on Selected Areas in Communications. 2020 Sep 1;39(2):361-9.

[2] Alladi T, Chamola V, Kumar N. PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks. Computer Communications. 2020 Jul 1;160:81-90.

[3] Bhaskaran, R., Ramamoorthy, K., Fancy, C., Jayasankar, T.(2022), "Replica Node Detection using Metaheuristic Algorithms in Wireless Sensor Networks", International Journal of Engineering Trends and Technology, 70(5), 339-345

[4] Awan KA, Ud Din I, Almogren A, Almajed H. AgriTrust—a trust management approach for smart agriculture in cloud-based internet of agriculture things. Sensors. 2020 Oct 29;20(21):6174.

[5] Sowah RA, Boahene DE, Owoh DC, Addo R, Mills GA, Owusu-Banahene W, Buah G, Sarkodie-Mensah B. Design of a secure wireless home automation system with an open home automation bus (OpenHAB 2) framework. Journal of Sensors. 2020 Oct 30;2020.

[6] Jaya NI, Hossain MF. A prototype air flow control system for home automation using mqtt over websocket in aws iot core. In2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) 2018 Oct 18 (pp. 111-1116). IEEE.

[7] J. V. Anchitaalagammai, T. Jayasankar, P. Selvaraj, Mohamed Yacin Sikkandar, M. Zakarya, Mohamed Elhoseny and K. Shankar, "Energy Efficient Cluster-Based Optimal Resource Management in IoT Environment", Computers, Materials & Continua, vol. 70, no.1, pp. 1248-1261, 2022, ISSN: 1752-1767 (Print) 1546-2226.

[8] Hayashi V, Ruggiero W. Non-invasive challenge response authentication for voice transactions with smart home behavior. Sensors. 2020 Nov 17;20(22):6563.

[9] Faid A, Sadik M, Sabir E. An agile AI and IoT-augmented smart farming: a cost-effective cognitive weather station. Agriculture. 2021 Dec 29;12(1):35.

[10] Hasan D, Ismaeel A. Designing ECG monitoring healthcare system based on internet of things blynk application. Journal of applied science and technology trends. 2020 Jul 31;1(3):106-11.

[11] M. L. Das, A. Saxena, and V. P. Gulati. A dynamic id-based remote user authentication scheme. IEEE Transactions on Consumer Electronics, 50(2):629–631, May 2004.

[12] . L. Das, A. Saxena, and V. P. Gulati. A dynamic id-based remote user authentication scheme. IEEE Transactions on Consumer Electronics, 50(2):629–631, May 2004

[13] Y.-F. Chang, W.-L. Tai, and H.-C. Chang. Untraceable dynamicidentity-based remote user authentication scheme with verifiable pass word update. International Journal of Communication Systems, 27(11):3430–3440, 2014

[14] S. Sarma, S. Weis, and D. Engles. Radio frequency identification: Security risks and challenges. Cryptobytes, 6(1):2–9, 2003.

[15] D. Molnar, A. Soppera, and D. Wagner. A scalable, delegatable pseudonym protocol enabling ownership transfer of rfid tags. Proc. Workshop on Selected Areas in Cyptography, LNCS Springer, SAC2005,3897, 2006.\

[16] Ruels, R. L. Rivest, and M. Szudlo. The blocker tag : selective blocking of rfid tags for consumer privacy. The 8th ACM Conference on Computer and Communications Security, pages 103–111, 2003.

[17] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. In Security in pervasive computing, pages 201–212. Springer, 2004.

[18] Juels. Rfid security and privacy: A research survey. Selected Areas in Communications, IEEE Journal on, 24(2):381–394, 2006.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5730
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

[19] P. Peris-Lopez, T.-L. Lim, and T. Li. Providing stronger authentication at a low cost to rfid tags operating under the epcglobal framework. In Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference on, volume 2, pages 159–166. IEEE, 2008.\D. M. Konidala and K. Kim. Rfid tag-reader mutual authentication scheme utilizing tags access password. Auto-ID Labs White Paper WP- HARDWARE-033, 2007.

[20] Louis Jestin, & Ibrahim Hamdan. (2022). Architecture Modelling of MOS Device for the Circuit simulation. Acta Energetica, (02), 21–27. Retrieved from http://actaenergetica.org/index.php/journal/article/view/465

[21] T.-L. Lim and T. Li. Addressing the weakness in a lightweight rfid tag-reader mutual authentication scheme. In Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE, pages 59–63. IEEE, 2007.

[22] C.-L. Chen and Y.-Y. Deng. Conformation of epc class 1 generation 2 standards rfid system with mutual authentication and privacy pro- tection. Engineering Applications of Artificial Intelligence, 22(8):1284–1291, 2009.

[23] Jakub Siemek, & Dr. Prakash Pise. (2022). Model Designing of Analog Integrated Circuits for the Physiological Signals. Acta Energetica, (03), 01–08. Retrieved from http://actaenergetica.org/index.php/journal/article/view/470

[24] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Tapiador, and J. C. Van der Lubbe. Cryptanalysis of an epc class-1 generation-2 standard compliant authentication protocol. Engineering Applications of Artificial Intelligence, 24(6):1061–1069, 2011.

[25] Vibha Yadav, Manas Kumar Mishra, Singh, AK & Gore, MM 2009, 'Localization Scheme for Three Dimensional Wireless Sensor Networks using GPS enabled Mobile Sensor Nodes', International Journal of Next-Generation Networks (IJNGN),vol. 1, no.1,pp. 60-72.

[26] Hongyang Chen, Qingjiang Shi, Pei Huang, Vincent Poor, H & Kaoru Sezaki 2009, 'Mobile Anchor Assisted Node Localization for Wireless Sensor Networks', IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, Tokyo,Japan, pp.87-91