An Algorithm to Increase the Attached Complexity and Time Consumption for Iot Healthcare Applications Based on the Truncated Quantum Hashed Method

Bharathi Malakreddy A.[1], Vani G.[2]

[a]*Computer Science, BMS Institute of Technology and Management, Bangalore, Karnataka, India*

[b]*Computer Science, Sonata-Software.com, Bangalore, Karnataka, India*

Karnataka, India

Abstract:- Internet of Things (IoT) implementations have been used in numerous healthcare domains. The majority of smart devices are connected, including the automatic environment in which such systems operate. Security and privacy have emerged as major challenges for IoT management. Recently published research has revealed the effectiveness of Elliptic Curve Cryptography (ECC) techniques are very useful for undertaking security research and evaluation of IoT applications and have numerous advantages over further techniques. The objective of this research paper is to suggest options for where to improve the encryption system in the ECC technique, with numerous optimization techniques to prepare the best enhancement of the light-weight algorithm. Our primary focus is on enhancing the Truncated Quantum Hashed Signature (TQHS) methods to increase the complexity of the adaptation and reduce the time utilization of the ECC encryption model. A hybrid data encryption architecture model integrating an ECC model with a TQHS-based architecture design to develop a lightweight encryption technology and the proposed Truncated Quantum Hashed Signature method integrates a random Hashed Signature methodology with a key generation model to improve security complexity. Second, from the standpoint of IoT security systems, Comparison and estimation of memory consumption and time complexity analyses to increase privacy and security. Lastly, we enhance the encryption system parameters in the ECC method. In the proposed work, we present a novel model of random key formation for the ECC to improve the model as a lightweight architecture.

Keywords:*Truncated Quantum Hashed method, IoT, healthcare, Internet of Things, Elliptic Curve Cryptography, mutual authentication, efficient authenticated key, MQTT, ROC curve, Confusion Matrix, memory consumption*

1. Introduction

The (IoT) Internet of Things has become a reality, and this is now being used for a variety of essential areas such as healthcare, smart buildings, cybercrime tracking systems, and smart vehicles. This has presented unique privacy, security, and integrity challenges to IoT users. Privacy, integrity and security are extremely challenging issues to solve, due to heterogeneous environments with IoT devices and computational restrictions. Nevertheless, privacy, integrity and security are precarious for several additional IoT applications in domains such as intelligence gathering, healthcare, and transportation.

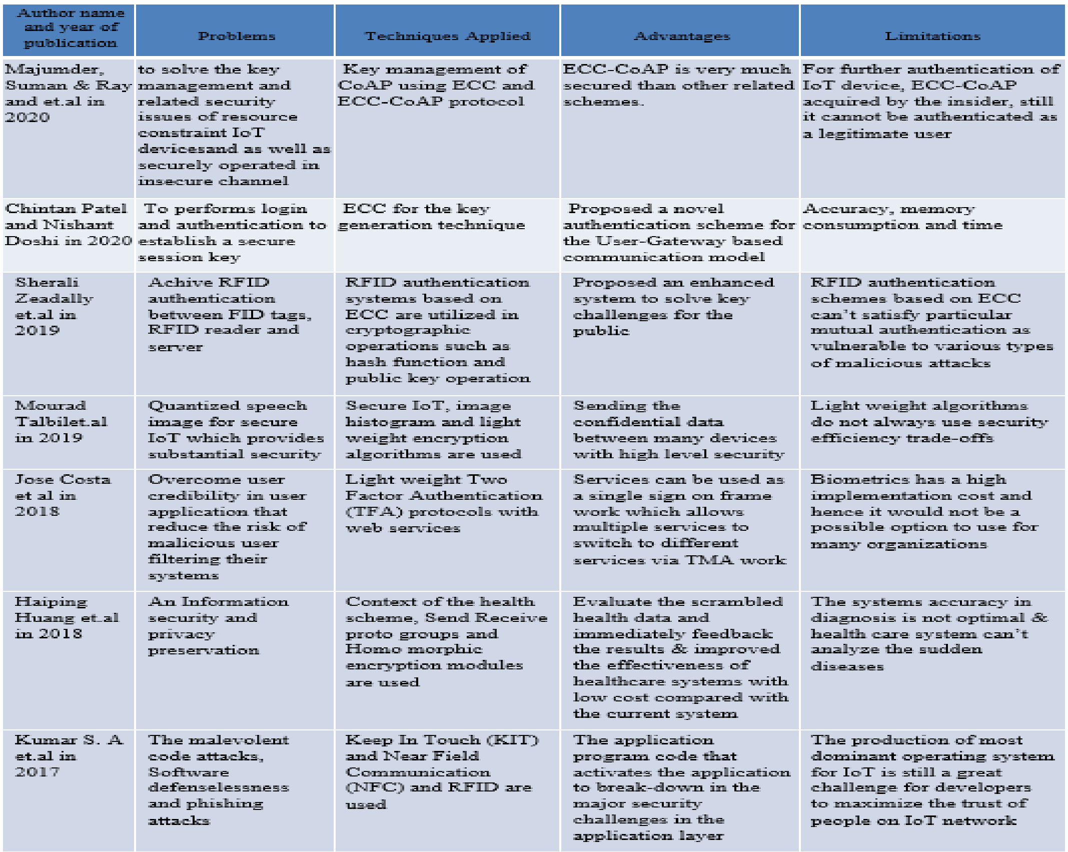
Privacy, security, integrity, and security are critical for most IoT applications for example environmental, medicinal treatment, confidentiality, infrastructure for transportation, manufacturing, logistic and operation management, and food and nutrition security. Without effective privacy, safety, and integrity solutions, accurate information hybridization and extraction, effectively managed by narrative cleverness and improved customer approvals and involvement are impossible to achieve.

Quant cryptography is the science of using quantum automated features to perform cryptographic operations. The most well-known application of quantum cryptography is quantum key supply, which offers a relevant data-protected resolution to key exchange problems. Quantum cryptography utilizes evolution's quantum mechanical behavior in the development and evaluation of cryptographic techniques of cryptography. Its objective is to create cryptographic systems whose security is guaranteed uniquely by natural rules. These are in marked contradiction to many of the typical cryptographic systems, since throughout theory may be broken if enough data processing power is applied. From a theoretical standpoint, Quantum cryptography provides a lovely combination of adversarial behavior mathematics and quantum data or information theory. Many approaches have been suggested to improve customer's rights to data control. For proactive security and confidentiality, for instance, a novel security protecting Naive Bayes education system with numerous data sources methods is proposed. Private information huge data applications in a hybrid cloud were projected, which was a scalable e-health record sharing system. In this research paper, propose a quick and secure authentication system with establishment keys for remote IoT applications. The proposed technique is based on ECC (Elliptic Curve Cryptography), specifically, an Elliptic Curve Digital Signature System and it is used to allow the proposed module to be faster and more efficient, in both terms of processing time and as well volume of data exchanged in the system. Eventually, the methodology outlined in this article provides a private session key between both the IoT structure and the customer's smartphone.

2. Related work and motivation

With the regular evolution of IoT systems, multiple surveys and novel research works have been carried out over ongoing enhancement across the various efficiency and security challenges faced by the IoT ecosystem. An overview of the literature review is mentioned in table 1.

Table 1: Summary of the Literature Review



Author name and year of publication	Problems	Techniques Applied	Advantages	Limitations
Majumder, Suman & Ray and et.al in 2020	to solve the key management and related security issues of resource constraint IoT devicesand as well as securely operated in insecure channel	Key management of CoAP using ECC and ECC-CoAP protocol	ECC-CoAP is very much secured than other related schemes.	For further authentication of IoT device, ECC-CoAP acquired by the insider, still it cannot be authenticated as a legitimate user
Chintan Patel and Nishant Doshi in 2020	To performs login and authentication to establish a secure session key	ECC for the key generation technique	Proposed a novel authentication scheme for the User-Gateway based communication model	Accuracy, memory consumption and time
Sherali Zeadally et.al in 2019	Achive RFID authentication between FID tags, RFID reader and server	RFID authentication systems based on ECC are utilized in cryptographic operations such as hash function and public key operation	Proposed an enhanced system to solve key challenges for the public	RFID authentication schemes based on ECC can't satisfy particular mutual authentication as vulnerable to various types of malicious attacks
Mourad Talbilet.al in 2019	Quantized speech image for secure IoT which provides substantial security	Secure IoT, image histogram and light weight encryption algorithms are used	Sending the confidential data between many devices with high level security	Light weight algorithms do not always use security efficiency trade-offs
Jose Costa et al in 2018	Overcome user credibility in user application that reduce the risk of malicious user filtering their systems	Light weight Two Factor Authentication (TFA) protocols with web services	Services can be used as a single sign on frame work which allows multiple services to switch to different services via TMA work	Biometrics has a high implementation cost and hence it would not be a possible option to use for many organizations
Haiping Huang et.al in 2018	An Information security and privacy preservation	Context of the health scheme, Send Receive proto groups and Homo morphic encryption modules are used	Evaluate the scrambled health data and immediately feedback the results & improved the effectiveness of healthcare systems with low cost compared with the current system	The systems accuracy in diagnosis is not optimal & health care system can't analyze the sudden diseases
Kumar S. A et.al in 2017	The malevolent code attacks, Software defenselessness and phishing attacks	Keep In Touch (KIT) and Near Field Communication (NFC) and RFID are used	The application program code that activates the application to break-down in the major security challenges in the application layer	The production of most dominant operating system for IoT is still a great challenge for developers to maximize the trust of people on IoT network

3. Experimental results and discussion

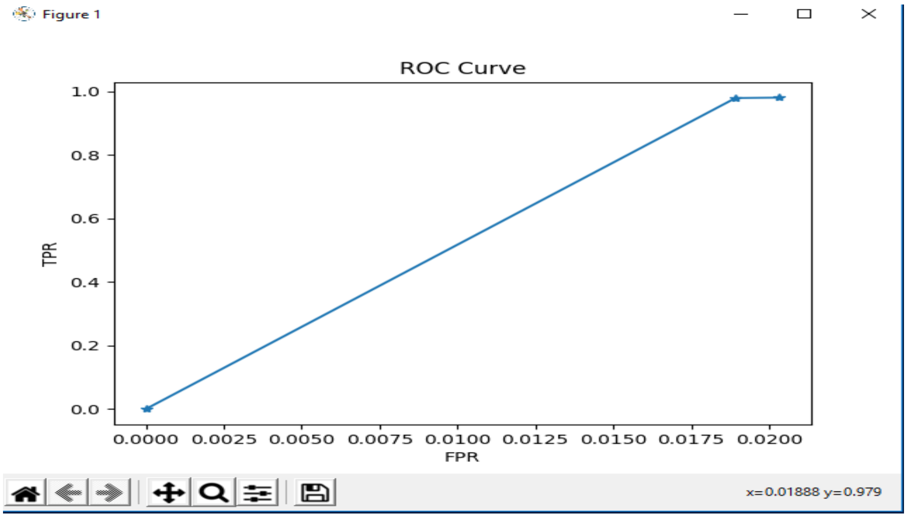
In this segment, we go through the specific details of the proposed method. The requirements of the IoT ecosystem along with the assumptions and notations employed, are discussed including the core design concept.

3.1 Methodology

The proposed Internet of Things Healthcare application solution consists of interaction between three different systems. Each system interface is protected by authentication at its entry point. In the lightweight encryption system, the implementation process includes the architecture design of the ECC encryption model. Since, for a better secure data transmission process the ECC concept can be enhanced generation of random keys. In that enhancement work, we propose a model of hybrid encryption architecture by the combination of the ECC model with a Truncated Quantum Hashed Signature (TQHS) based architecture design to develop a lightweight encryption system. This architecture mainly focused on the random key generation system to reduce the time complexity than to the traditional model of the ECC encryption system. Here, the proposed Truncated Quantum Hashed Signature (TQHS) method integrates the Hashed signature technique for the random key generation model for better security complexity. The Hashing models are designed by the Quantum model of architecture that truncates the looping design with appropriate components that can achieve a reduced amount of components and device utilizations. This results in the lightweight architecture of the encryption system in the IoT application.

In Graph 1, Receiver Operator Characteristic (ROC) curves in graph 1 show the exchange of TRP (True positive rate) and FRP. classification algorithm that give curves closer to the top left-hand corner indicate an improved performance. The test becomes less accurate as the angle approaches the diagonal of the ROC space.

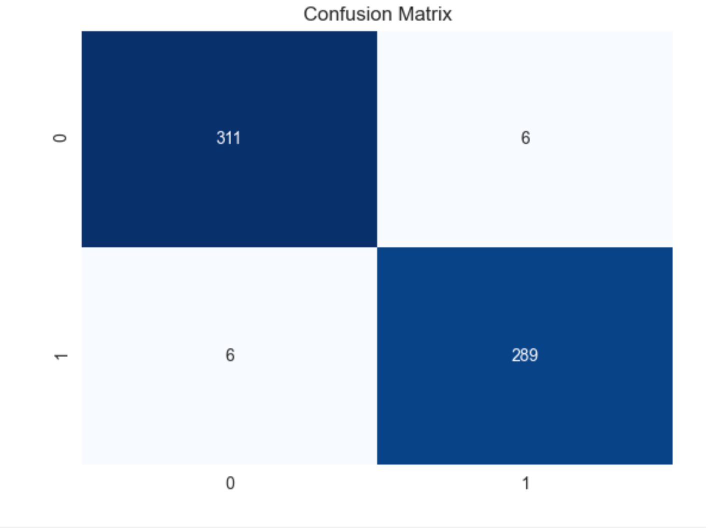
Graph 1: ROC Curve FPR



A Receiver Operator Characteristic (ROC**) curve is** created by plotting True Positive Rate (TPR) compared against the False Positive Rate (FPR). The percentage of all the True positive rate (TP/ (TP + FN)) is observations that are predicted to be positive properly. The false positive rate is the percentage of negative observed that are mistakenly assumed to be positive.

A confusion table is a matrix that displays how well a grouping model operates on test data sets with given true values. The matrix of confusion is simple to understand, but the terminology used to describe it can be confusing.

Graph 3: Confusion Matrix

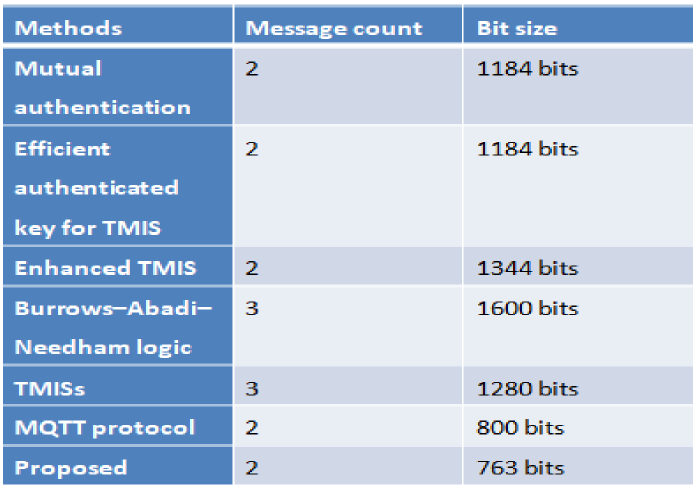


We can compute a Confusion Matrix with the following steps. To begin, you must test the dataset using the predicted outcome standards. Second, predict entirely of the rows in the test dataset, and then compute the expected outcomes and predictions.

3.2 Comparison Evaluation of memory consumption and time taken

The following tables 2 and 3 describe about the evaluation of memory consumption and time analysis in milliseconds with the recommended work of secure light-weight key exchange technique for the user gateways by means of elliptic curve cryptography technique and existing work.

Table 2: Comparison Evaluation of Memory Consumption



Methods	Message count	Bit size
Mutual authentication	2	1184 bits
Efficient authenticated key for TMIS	2	1184 bits
Enhanced TMIS	2	1344 bits
Burrows–Abadi–Needham logic	3	1600 bits
TMISs	3	1280 bits
MQTT protocol	2	800 bits
Proposed	2	763 bits

Table 3: Comparison Evaluation of time taken in ms

Methods	Time taken (ms)
Mutual authentication	13.38 ms
Efficient authenticated key for TMIS	13.4 ms
Enhanced TMIS	15.6 ms
Burrows–Abadi–Needham logic	11.17 ms
TMISs	8.9 ms
MQTT protocol	8.9 ms
Proposed	7.4 ms

3.4 Comparison with ECC-CoAP: ECC-based Limitation Application Protocol for an IoT

The following tables four and five describe about the Comparative Evaluation of ECC-based constraint application protocol for an IoT with existing work and proposed work.

Table 4: Comparative Evaluation ECC based Limitation Application Protocol for an IoT

Methods	Message count	Bit size
Dey and Hossain scheme	5	1312 bits
ECC-CoAP	4	1024 bits
Proposed	4	926 bits

Table 5: Comparative analysis of Time taken in ms

Methods	Time Taken (ms)
Dey and Hossain scheme	38.5276
ECC-CoAP	28.779
Proposed	24.513

4. Possible Outcome

This proposal aims to improve the boundary conditions of the encryption method employed by the ECC technique, with numerous optimization techniques to prepare the best glossary of random key generation system. In this proposed work, I present a novel model of an important establishment for an ECC to optimize the model as a lightweight architecture. This can be executed using the Truncated Quantum Hashed Signature (TQHS) method to increase the complexity of the adaptation and reduce the time utilization of the ECC encryption model. A hybrid data encryption architecture model integrating an ECC model with a Truncated Quantum Hashed Signature (TQHS) based architecture design to develop a lightweight encryption technology. The proposed Truncated Quantum Hashed Signature (TQHS) method integrates a random Hashed Signature methodology with a key generation model to improve security complexity.

5. Acknowledgements

The research work published in this paper was made possible through the funding and support of the Vision Group on Science and Technology, Govt. of Karnataka (GRD No.782), within the Department of AI & ML at BMSIT & M, Bangalore. This grant enabled the acquisition of high-quality equipment essential for conducting research in Healthcare applications.

1. References

[1] Bharathi Malakreddy A, Vani G, 'ECC based multifactor authentication & key generation system for the Internet of Things Healthcare, in the "Turkish Journals of Computer and Mathematics Education", Published online on 10 May 2021, Vol.12 No.11 (2021), 5026-5032 Research Article

[2] Vani G, Bharathi Malakredd A, "Survey on Security challenges in IoT in Healthcare domain", in the ICNTET, 2018, ISBN- CFP18P34-PRT/978-1-5386-5629-7. 2

[3] Vani G, Bharathi Malakreddy A, "A review on identification & analysis of security issues & challenges of IoT based Healthcare", International Journal of innovative technology & Exploring Engineering (IJITEE) ISSN - 2278-3075, Vol. 8 Issue:4, February 2019, pp. 546-549. 3

[4] Vani G, Bharathi Malakreddy A, "Security challenge in an IoT", in the healthcare domain, September 2016, DOI No. IAECS IRAJ DOI 5592, pp.141-144

[5] Akashdeep Bhardwaj, Bharat Bhushan, "Model to enhance security posture of IoT devices and components with private APN" Published online 19 April 2021, https://doi.org/10.1504/IJISTA.2021.114645

[6] Yavari ali, Georgakopolous Dimitrios, "A Lightweight and Holistic IoT Security Based on IoT data contextualization and Homomorphic Encryption" published in 2021, ISSN 0302-9743, ISBN - 9783030732028, publisher URL https://doi.org/10.1007/978-3-030-73203-5_16

[7] Debiao He, an analysis of RFID authentication scheme for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography", in 'IEEE INTERNET OF THINGS JOURNAL, Vol. 2, No. 1, February 2015

[8] Mourad Talbi1et, "Application of the Lightweight encryption algorithm to the quantized speech image intended for Secure IoT, 2018, DOI: 10.20944/preprints 201802.0096. v2

[9] Jose Costa et al, "Middle Man: An Efficient Two-Factor Authentication Framework", Third IEEE International Conference going on Communication, Computing, Control and Automation, Pune, India 17th to 18 Aug 2017", IEEE

[10] Dylan Sey, "A survey on authentication methods for the IoT", Vol.2, 2018, pp. 537-567 8. Hafizah Che Hasan, "Comparison of authentication methods in IoT technology", Vol. 12, No. 3, 2018

[11] Lee T, 'Verifier Based three-party authentication schemes', Vol. 38, No. 5, in 2014, pp. 464 – 472.

[12] H. Zhou, X Lin et.al, "Patient Self controllable and Multi-Level Privacy preserving cooperative authentication in Distributed Healthcare Cloud CS", in 2014, pp.1693-1703

[13] Rehiman K, "A secure infrastructure for the Internet of Things supported smart mobile devices, in 2016, in Vol. 9, DOI: '10.17485/ijst/2016/v9i9/86791

[14] Lella A, Martin B, "The Mobile application report available in ww.comscore.com/Insights/Presentations and Whitepapers', in 2015