International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 3, May.-June, 2024 pp: 203-208 ISSN: 2584-2145
www.ijemh.com

Implementation of A Multi-Factor Authentication Protocol for Iot Based E-Health Applications Using FGPA

NEVEDHAGAYATHRIKS,NANDHINI S
DepartmentofElectronicsandCommunicationEngineering
Dr NGP Institute of Technology,Coimbatore,TamilNadu,India

Date of Submission: 12-06-2024 Date of Acceptance: 25-06-2024

ABSTRACT:
The IoT platform presents promising opportunities to enhance daily life, making it more intelligent and comfortable. In the realm of e-healthcare, IoT holds significant potential to improve service quality within constrained timeframes. However, the connectivity offered by e-healthcare devices raises significant concerns regarding security and privacy. To address these issues, this study employs Multi-Factor Authentication (MFA) between entities, enhancing security. Authentication utilizes Truncated Multiplier (TM), chosen for its cost-effectiveness and improved randomness. The research introduces a three-factor authentication protocol for IoT-based e-health devices. The architecture is implemented using Verilog HDL, synthesized with Xilinx Synthesis Technology (XST), and deployed on a Zynq FPGA device (XC7Z020CLG484-1). Results demonstrate that the proposed protocol achieves enhanced security measures at a minimal cost.

Keywords:E-Health, Truncated multiplier, FPGA, , MultifactorAuthentication, IoT.

I. INTRODUCTION

The Internet of Things (IoT) represents the integration of internet connectivity into everyday objects. In our daily lives, even small gadgets analyse their surroundings to operate intelligently. Globally, billions of physical devices connect to the internet, independently sharing information without human intervention. IoT enhances smart living by enabling devices to autonomously transmit gathered data to a central hub. Its impact spans various fields such as healthcare, smart homes, cities, environmental automation, weather forecasting, and transportation. In healthcare, IoT reduces unnecessary doctor visits, hospital stays, and readmissions, enhancing e-health systems with smart devices.

Biosensors continuously monitor vital signs and health-related data, transmitting them to medical servers anytime, anywhere. Integrated IoT capabilities in medical devices facilitate tasks like remote patient monitoring, treatment progress tracking, and health issue detection. Benefits of IoT in healthcare include streamlined treatment processes, cost and time savings, adaptable hospitality models, and improved health decisions.

Authentication plays a crucial role in IoT to ensure the trustworthiness of connected devices. It verifies individuals based on possession (something they have), knowledge (something they know), and inherence (something they are). Authentication occurs from account login to device connection to the cloud, assigning unique identities for tracking and analysis throughout their lifecycle. Access to protected resources like network databases and service applications is restricted to authenticated users. Multi-Factor Authentication (MFA) is employed in e-health for secure data transmission between patients and healthcare providers, enhancing security by employing multiple authentication methods.

Traditional authentication methods using only usernames and passwords face security risks such as password database breaches. MFA addresses these issues by requiring multiple authentication factors, offering greater security than single-factor methods. Truncated multiplication-based authentication is proposed to further enhance security in authentication processes. This paper outlines the protocol design, algorithm analysis, Finite State Machine (FSM), and simulation results of the proposed authentication protocol.

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 3, May.-June, 2024 pp: 203-208 ISSN: 2584-2145
www.ijemh.com

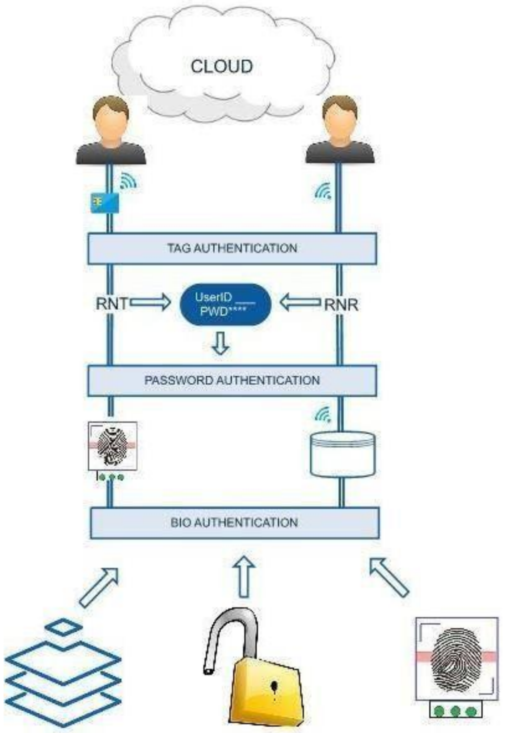

Figure1-Internet of Things

II. LITERATURESURVEY

This section explores various security challenges and solutions in the medical field. In recent years, several security protocols have been proposed to address issues such as key sharing among users. However, only a few protocols have been implemented in hardware using FPGAs and embedded microcontrollers, with some evaluated using simulators like AVISPA. Most mutual authentication protocols remain theoretical, focusing on qualitative analysis. Examples of hardware-implemented protocols can be found in references [1-7], specifically for e-health applications in references [7, 13], and IoT cloud-based environments discussed in references [4, 8, 9].In their work, Zhang et al. [12] propose a three-factor authentication scheme for e-health systems aimed at protecting user privacy in real-time applications. Despite its strengths, this protocol is susceptible to attacks such as de-synchronization, denial-of-service (DoS), and insider threats. Another approach presented in [13] introduces a lightweight authentication bio hash function with five phases (setup, registration, login, authentication, key agreement, and ownership transfer) and utilizes three factors (password, smart card, biometric) tailored for e-health Internet of Medical Things (IoMT) applications. This method mitigates insider attacks, DoS attacks, de-synchronization attacks, and offline password guessing attacks.[14] discusses a remote authentication scheme combining passwords and smart cards without detailed robustness explanation, prompting the integration of biometric data (e.g., fingerprints, iris scans) with traditional authentication schemes. Generally, three-factor authentication schemes have been introduced to enhance patient information security [15, 16]. A comprehensive study in [17] addresses recent topics and challenges in e-health applications, proposing effective solutions to mitigate risks. Future considerations regarding security and privacy issues are also discussed.Furthermore, reference [18] reviews authentication schemes based on Elliptic-curve cryptography (ECC), noting security vulnerabilities that make it unsuitable for IoMT systems. Consequently, there is a growing need for protocols that balance both area overhead and security to address these challenges effectively.

III. PROPOSEDWORK

This section outlines the design of the proposed protocol utilizing the truncated multiplier architecture, chosen for its capability to generate output values according to the specified design requirements. The protocol is presented with a detailed, step-by-step procedure as follows:

PROPOSEDPROTOCOL:

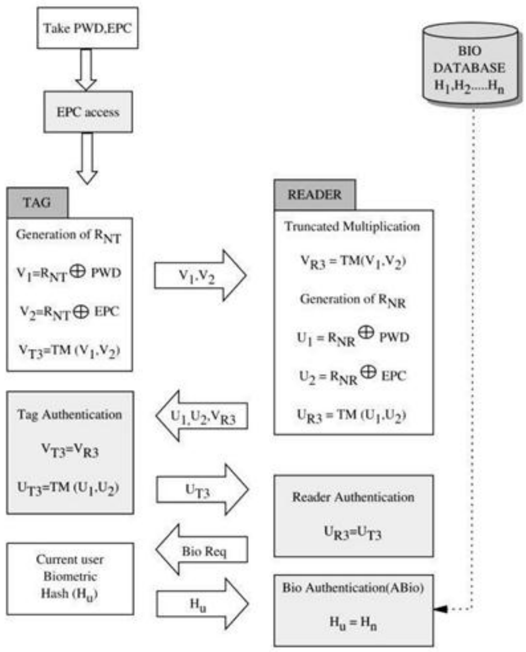

Figure2-Three-FactorAuthentication

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 3, May.-June, 2024 pp: 203-208 ISSN: 2584-2145
www.ijemh.com

ALGORITHM:

Step1a: GenerateaRandomnumber(RNT)

Step1b:XORRNTwithPWDandEPC

V_1=(RNT)⊕(PWD) (1)

V_2=(RNT)⊕(EPC) (2)

Step2a: Truncated multiplication

V_{R3}=TM(V_1,V_2) (3)

Step2b: GenerateaRandomnumber(RNR)

U_1=(RNR)⊕(PWD) (4)

U_2=(RNR)⊕(EPC) (5)

Step3a: Truncated multiplication

V_{T3}=TM(V_1,V_2) (6)

Step3b:TagAuthentication

A_T ={1,ifV_{T3}=V_{R3}0,i fV_{T3}≠V_{R3} (7)

Step4a: Truncationmultiplication

U_{T3}=TM(U_1,U_2) (8)

Step5a: Truncated multiplication

U_{R3}=TM(U_1,U_2) (9)

Step5b:ReaderAuthentication

A_R= {1,ifU_{T3}=U_{R3} 0,ifU_{T3}≠U_{R3} (10)

Step6a: The reader sends a biometric request to the tag

Step6b: The tag generates a hash function (Hu) and sends it to the reader.

Step6c:BiometricAuthentication

A_{Bio} ={1, ifH_u= H_n0, ifH_u≠ H_n (11)

where Hn represents the total number of users in the database

WhereC_2=9913

U_{R3}=U_3−C_2=151191552

FSM:

FSM DIAGRAM:

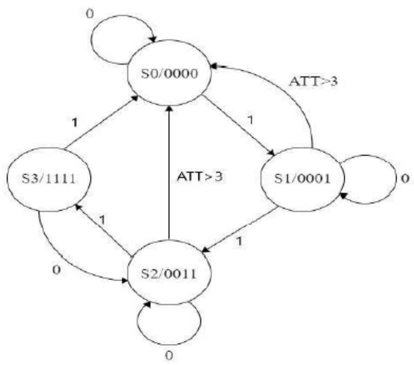

Figure 3-State diagram

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 3, May.-June, 2024 pp: 203-208 ISSN: 2584-2145
www.ijemh.com

EXAMPLECALCULATION:

Table1-SampleCalculation

Password(PWD) =27914 EPC=32178	
TAG	**READER**
RNT=48165	RNR=21837
V_1=53551 V_2=49559	U_1= 14407 U_2=10495
Truncated Multiplication	Truncated Multiplication
V_{T3}=2653880320	V_{R3}= 2653880320
TAGAuthentication	Truncated Multiplication
$AT=VT3=VR3$	U_{R3}=151191552
Truncated Multiplication	**ReaderAuthentication**
U_{T3}=151191552	$AR=UR3=UT3$

ILLUSTRATION:

Password(PWD)=27917
Electronic Product Code (EPC)=32178
Tag'sRandomnumber(RNT)= 48165
V_1=48165⊕27914 =53551
V_2=48165⊕32178=49559
TruncatedMultiplication
$V_3=V_1\times V_2$=53551×49559
V_3=2653934009
Binaryformof
V_3=1001111000101111|10100011011100
WhereC_1=53689

$V_{T3} = V_3 - C_1$=2653880320
Reader'srandomnumber(RNR)=21837
U_1=21837⊕27914=14407
U_2=21837⊕32178=10495
TruncatedMultiplication
$U_3=U_1\times U_2$=14407× 10495
U_3=151201465
Binaryformof
U_3=0000100100000011|0010011010111001

Table2-Bitexplanation

Output	Authentication	Biometric	Password	EPC
Bits	X	X	X	X

Table3-FSMStates

STATE	INPUT	NEXT STATE	OUTPUT
S0	0	S0	0000
	1	S1	0001
S1	0	S1	0001
	1	S2	0011
S2	0	S2	0011
	1	S3	1111
S3	0	S2	0011
	1	S0	0000

IV. ATTACKS

1) ReplayAttack

A new session key is generated to prevent replay attacks once the tag and reader identities are successfully verified.

2) ManintheMiddle Attack

In this context, the truncated multiplication algorithm is employed. Only residue values are accessible to attackers or potential interceptors in the channel. Attackers on an insecure channel are unable to recoverthe key or password.

3)Desynchronizationattack

The protocol structure is designed to ensure that the elements in the tag and reader operate independently of each other. Each entity has its own distinct feature, eliminating the need for time synchronization between them. Therefore, desynchronization attacks are not possible under this protocol.

3) Stolensmartcardattack

If a smart card is stolen, attackers may attempt to access the information stored within it. By employing biometrics as one of the authentication factors, any information contained in the smart card's hash values remains inaccessible to attackers.

4) Credentialstuffing

Credential stuffing is a type of cyberattack where attackers attempt to guess passwords using usernames and email addresses stored in a database. Biometric authentication is employed in this context to mitigate such attacks..

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 3, May.-June, 2024 pp: 203-208 ISSN: 2584-2145
www.ijemh.com

Table4Attacks

Attacks	Truncated Multiplication (3-Factor)
Maninthemiddleattack	Δ
Desynchronizationattack	✓
ReplayAttack	✓
Stolensmartcardattack	✓
Credentialstuffing	✓

✓ -Prevented,Δ-NotApplicable

V. RESULTANDANALYSIS SIMULATED RESULT:

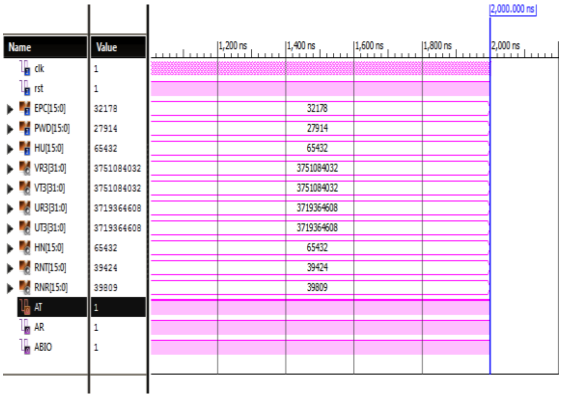

Figure4-Simulatedoutput SYNTHESIS RESULT

Table5-Synthesizedresult

Logicutilization&Delay	Proposed Protocol 16 bit
Numberofsliceregisters	32
NumberofSliceLUTs	69
Numberoffullyused LUT-FFpairs	10
Numberofbonded IOBs	181
Numberof BUFG/BUFGCTRLs	1
NumberofDSP48EIs	4
LogicDelay(ns)	0.353
RoutingDelay(ns)	0.655
Total Delay(ns)	1.008

VI. CONCLUSION

This paper proposes a three-factor authentication protocol for IoT-based E-health devices. Multi-factor authentication is utilized to enhance security between entities in healthcare environments. Password authentication is implemented using the Truncated Multiplier (TM), chosen for its cost-effectiveness and improved randomness. Smart card and biometric authentication are integrated with password authentication to further bolster security. The architecture for password authentication is developed using Verilog HDL and synthesized for the Zynq FPGA device (XC7Z020CLG484-1) using Xilinx Synthesis Technology (XST). This FPGA-based implementation of the three-factor authentication protocol maintains user security while providing enhanced service to patients at a reduced cost

REFERENCES

[1]. Liu, D., et al. "Design and Implementation of An ECC-Based Digital Baseband Controller for RFID Tag Chip" IEEE Transactions on Industrial Electronics, Vol.62, No.7,pp.4365-4373, 2015.
[2]. Zilong, L., et al. "Implementation of a New RFID Authentication Protocol for EPC Gen2 Standard" IEEE Sensors Journal, Vol.15, No.2,pp.1003-1011, 2015.
[3]. Hatzivasilis, G., et al. "Lightweight authenticated encryption for embedded on-chip systems" Information Security Journal: A Global Perspective, Vol.25, No.4-6,pp.151-161, 2016.
[4]. Li, N., et al. "Lightweight Mutual Authentication for IoT and Its Applications" IEEE Transactions on Sustainable Computing, Vol.2, No.4,pp.359-370, 2017.
[5]. Mujahid, U., et al. "Efficient Hardware Implementation of KMAP+: An Ultralightweight Mutual Authentication Protocol" Journal of Circuits, Systemsand Computers, Vol.27, No.02, 2018.
[6]. Vijaykumar,V. R.,etal. "Implementationof $2^n - 2^k - 1$ Modulo Adder Based RFID Mutual Authentication Protocol" IEEE Transactions on Industrial Electronics, Vol.65, No.1,pp.626-635, 2018.
[7]. VenkatasamySureshkumar, Ruhul Amin, V. R. Vijaykumar, S. Rajasekar, Robust SecureCommunication Protocol for Smart Healthcare System with FPGA Implementation, Future

GenerationComputer Systems, Accepted Manuscript, 2019.

[8]. Dong, Q., et al. "Cloud-based radio frequency identification authentication protocol with location privacy protection" International Journal of Distributed Sensor Networks, Vol.14, No.1, 2018.

[9]. ProsantaGope, Ruhul Amin, S.K. Hafizul Islam, Neeraj Kumar, Vinod Kumar Bhalla, "Lightweightand privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for the smart city environment," FutureGenerationComputerSystems83629–637,2018.

[10]. Vijaykumar, V. R. and S. Elango. "Hardware implementation of tag-reader mutual authentication protocol for RFID systems" Integration, the VLSI Journal, Vol.47, No.1,pp.123-129, 2014.

[11]. Dr V. R. Vijaykumar, RoshnaReghunath, S.Rajasekar, S.Elango“A novel lightweight and low power tag-reader mutual authentication protocol for portableRFIDbasedsecuritysystems”IEACon2016
- 2016 IEEE Industrial Electronics and Applications Conference, DOI: 10.1109/IEACON.2016.8067405

[12]. L. Zhang, Y. Zhang, S. Tang, H. Luo, Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement, IEEE TransactionsonIndustrialElectronics65(3)2795–2805,2018.

[13]. SeyedFarhadAghili, Hamid Mala, Mohammad Shojafar, Pedro Peris-Lopez, LACO: Lightweight Three-Factor Authentication, Access Control and Ownership Transfer Scheme for E-Health Systems in IoT, Future Generation Computer Systems, Volume 96, Pages 410-424,2019.

[14]. H. Arshad and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for sessioninitiationprotocolusingECC,"Multimedia Tools Appl., vol. 75, no. 1, pp. 181–197, 2016, DOI: 10.1007/s11042-014-2282-x.

[15]. D. Guo, Q. Wen, W. Li, H. Zhang, and Z. Jin, ‘‘An improved biometrics-based authenticationscheme for telecare medical information systems," J. Med. Syst., vol. 39, no. 3, pp. 1–10, 2015.

[16]. K.Srivastava,A.K.Awasthi,S.D.Kaul,andR. C. Mittal, "A hash-based mutual RFID tag authentication protocol in telecare medicine informationsystem"J.Med.Syst.,vol.39,p. 153,Jan. 2015, DOI: 10.1007/s10916- 014-0153-7.

[17]. Suhardi, and AlfianRamadhan.“A Survey of SecurityAspectsforIoTinHealthcare"Lecture Notes in Electrical Engineering Information Science and Applications(ICISA)2016,2016,pp.1237–1247., DOI:10.1007/978-981-10-0557-2_11712.

[18]. D. He, S. Zeadally, An analysis of RFID authentication schemes for the internet of things in a healthcare environment using elliptic curve cryptography,IEEEinternetofthingsjournal2(1)72–83,2015