AYYA NADAR JANAKI AMMAL COLLEGE

(Autonomous, affiliated to Madurai Kamaraj University, Re-accredited with 'A+' Grade by NAAC (4th Cycle with CGPA of 3.48 out of 4), College of Excellence by UGC, STAR College by DBT, Ranked 83rd at National Level in NIRF 2022 & An ISO 9001 : 2015 Certified Institution)

SIVAKASI - 626 124, TAMIL NADU

ANJAC

PRO DEO ET PATRIA

1963 - 2022

DIAMOND JUBILEE YEAR

"KNOWLEDGE PARTNER"

ICTACADEMY®

DEPARTMENT OF COMPUTER APPLICATIONS

INTERNATIONAL CONFERENCE ON SMART INNOVATIVE TECHNOLOGIES ON DATA ANALYTICS (ICSITDA '23)

Certificate

This is certify to Dr./~~Mr./Mrs./Ms.~~ P. Raajan, Associate professor, PG & Research Department of C.S, Muslim Arts college has presented a paper entitled Detection Fiddle using elliptic Deflection Diffie Hellman (EDDH) method based Authorization in Blockchain for securing IoMT Data in the International Conference on "Smart Innovative Technologies on Data Analytics" (ICSITDA '23) organized by Department of Computer Applications on 26th May, 2023.

Director
Dr. R. LAWRANCE

Principal
Dr. C. ASHOK

Organizing Secretaries
Dr. T. MARIMUTHU
Dr. B. VINOTH KUMAR

Proceedings of

INTERNATIONAL CONFERENCE ON SMART INNOVATIVE TECHNOLOGIES ON DATA ANALYTICS

ICSITDA '23

26th MAY 2023

organized by

Department of Computer Applications

AYYA NADAR JANAKI AMMAL COLLEGE

(Autonomous, affiliated to Madurai Kamaraj University, Re-accredited with 'A+' Grade by NAAC (4th Cycle with CGPA of 3.48 out of 4), College of Excellence by UGC, STAR College by DBT, Ranked 83rd at National Level in NIRF 2022 & An ISO 9001 : 2015 Certified Institution)

SIVAKASI - 626 124, TAMIL NADU

ISBN: 978-93-83191-92-5

AJ188	**A HYBRID CNN, LSTM, AND STACKING ENSEMBLE APPROACH FOR IMPROVED SENTIMENT ANALYSIS** *Kanimozhi.J & Dr.R.Manicka Chezian*	**786**
AJ189	**STUDENT ADMISSION PREDICTION USING LOGISTIC REGRESSION** *V.MADUBALA , M.AKILA & Mr. A.SELVA KUMAR*	**485**
AJ190	**A STUDY ON DIGITAL TRANSFORMATION AND ITS IMPACT ON EMPLOYEE ENGAGEMENT IN THE INSURANCE SECTOR** *Dr. K. Jegatheesan & I. Seema*	**492**
AJ191	**CUSTOMER BEHAVIOUR ANALYSIS USING ASSOCIATION RULE MINING** *Kannan .K , Mahesh .A , Alagukumar.S & Lawrance. R*	**497**
AJ192	**APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN THE REAL WORLD** *Dr. R. Ushadevi & Mr.M. Viswanathan*	**501**
AJ193	**USING SOCIAL MEDIA FOR LEARNING: OPPORTUNITIES AND CHALLENGES** *Ananthi N & Devi Arockia Vanitha C*	**506**
AJ194	**MINING WEAKLY LABELED WEB FACIAL IMAGES FOR SEARCH-BASED FACE ANNOTATION** *R.Sutha Abirami & S.Jasmila*	**512**
AJ195	**DETECTING FIDDLE USING ELLIPTIC DEFLECTION DIFFIE HELLMAN (EDDH) METHOD BASED AUTHORIZATION IN BLOCKCHAIN FOR SECURING IOMT DATA** *Y. JANI & Dr. P. RAAJAN*	**796**
AJ196	**IMPLEMENTATION OF E - VOTING SYSTEM BASED ON ETHEREUM BLOCK CHAIN TECHNOLOGY** *Ananthavalli R & Muniyappan,K*	**518**
AJ197	**AN EFFICIENT DENOISING METHOD OF SALT AND PEPPER NOISE FROM FINGER VEIN USING TRIMMED MEDIAN FILTER** *Anusha S.K. & Dr. A. Yesu Raja*	**810**
AJ198	**ROLE OF ARTIFICIAL INTELLIGENCE IN WOMEN ENTREPRENEURSHIP BUSINESS** *S. Thanga Keerthana and Dr. K. Jegatheesan*	**524**
AJ199	**RCNNLSTM: HYBRID DEEP LEARNING CLASSIFIER FOR SENTIMENT ANALYSIS IN IMBALANCED UNSTRUCTURED TWEET DATA** *Dr.J.Arunadevi & M.Ramesh Raja*	**531**
AJ200	**A COMPREHENSIVE REVIEW ON CYBER CRIME DETECTION TECHNOLOGIES** *P. Aruljeyanthi & Dr. T. Balaji*	**549**
AJ201	**ANALYSIS AND PREDICTION OF STOCK PRICE BY TUNING THE HYPERPARAMETER OF LSTM MODEL** *Geetha M & Devi Arockia Vanitha C*	**564**
AJ202	**ENHANCED FEATURE EXTRACTION TODETECT LEAF DISEASES IN CROPS** *Raji N & Dr. S.N.Geethalakshmi*	**571**
AJ204	**DEEP LEARNING BASED USER AUTHENTICATION AND ALERT SYSTEM IN LIBRARY TRANSACTION** *K. Nivetha , M. Bava Atchaya , K. Devipriya & T. Manikandan*	**581**
AJ205	**PERFORMANCE ANALYSIS OF LOAN STATUS PREDICTION USING SVM, KNN, NAIVE BAYES AND DECISION TREE ALGORITHMS** *P. Bamarukmani, G. Mareeshwari & A. Vennila*	**815**
AJ206	**IMPLEMENTATION OF STUDENT PLACEMENT PREDICTION USING MACHINE LEARNING** *Indira Devi C, Thanga Aadharshana T.P. & R. Lawrance*	**599**
AJ207	**SWITCHING BEHAVIOUR OF CUSTOMERS OF BANKS IN SIVAKASI** *Dr. K. Ganesha Moorthy & Dr. M. Rifaya Meera*	**603**
AJ208	**AN ADAPTIVE METHODOLOGY FOR VARIOUS PREDICTIONS ON SUN SPOTS WITH MULTIPLE FACTORS USING SVM AND ARTIFICIAL NEURAL NETWORK** *Beena G P*	**820**

 ISBN: 978-93-83191-92-5

DETECTING FIDDLE USING ELLIPTIC DEFLECTION DIFFIE HELLMAN (EDDH) METHOD BASED AUTHORIZATION IN BLOCKCHAIN FOR SECURING IoMT DATA

Y. JANI
Research Scholar,
Reg. No:**21213092342009**,
PG and Research Department of computer science,MuslimArtscollege,Thiruvithancode
AffiliatedtoManonmaniamSundaranar University, Abishekapatti,
Tirunelveli -627012, Tamil Nadu, India
E-mail: janijaanu05@gmail.com

Dr. P. RAAJAN
Associate Professor,
PG and Research Department of Computer Science,MuslimArtscollege,Thiruvithancode,
AffiliatedtoManonmaniamSundaranar University, Abishekapatti,
Tirunelveli- 627012, Tamil Nadu, India
E-mail: raajanp99@gmail.com

Abstract:

Internet of Medical Things (IoMT) is playing vital role in providing medical services instantaneously. In IoMT, sensitive data are shared via centralized service providers, which arises security concerns. Several works have been developed with blockchain to solve security issues, yet less focus was given tofiddle detection in shared IoMT data. Hence, in this paper, an OLES-LWT-based watermark for fiddle detection is proposed. Initially,a patient login into hospital website with credential information provided during registration and booksan appointment with doctor. Online consultation happens atthe scheduled time, and the IoT-sensed image will be shared. To detect fiddlinginIoT Image, watermark image by fusion of hospital icon, department icon, and signature with a time stamp image is embedded in the IoTImage and stored in the cloud. Meanwhile, for user authorization, FYS-Tiger hashing and role-based access policy with a digital signature in blockchain is introduced. On the other hand, the doctor downloads data after successful login, signature verification, and hash code matching processes. Then,the watermark will be removed at the doctor's side for fiddling detection. The performance of the proposed model is proven with better outcomes of experimental results.

Keywords: *Internet of Medical Things (IoMT), Blockchain, authorization, Watermarking, Wavelet transform, scaling.*

1. INTRODUCTION

The advancement of IoT is projected towards transforming the medical sector as well as compel the growth of IoMT[12].IoMT is an assortment of health care systems to

 ISBN: 978-93-8

provide secure transmission of health-related data between smart devices, which help remotely located doctors, and healthcare-providers, to collect and analyze health data electronically[5]. Although IoMT provides more services, it is also equally important to protect patient's data that is generated from various healthcare systems[13]as healthcare data requires a high-level of security and privacy[15]. To solve security and privacy issues, symmetric and asymmetric cryptographic techniques were developed[6]. Still, cryptographic techniques failed to give security to patients' data due to exploitation of public key parameters. One possible solution to solve this issue relies on Blockchain technology-based authentication of users.

Blockchain technology is a fiddle-proof digital ledger with secure Peer-to-Peer communication feature[3]. Blockchain is extremely secure as it is immune to modification of data. One of the most important properties of blockchain is that it is a distributed ledger[14]. Also, blockchain is a decentralized technology that solves setbacks of centralized architectures' such as network users do not clearly view how the information they generated will be used[2]. More research was developed based on blockchain technology to preserve privacy of patient's data. However, these schemes often use interplanetary file system, which relies on Hash Table for data storage and sharing, leading to high data retrieval latency[10]. Moreover, various Attribute-based authentication techniques were developed to create access policies in block chain. Although various authentication mechanisms have been developed to protect patients' data, most of them are cost-ineffective, or face scalability issues[4]. Also, less importance was given to detection of fiddling in received patients' data. Hence, to solve these problems, an OLES-LWT watermarked image-based IoMT-data fiddle detection is proposed in this research.

1.1 Problem definition

The securing of healthcare data with existing works in IoMT environment has certain limitations such as,

- In existing works, no importance was given to prevent malicious modifications to the shared medical image.
- In existing system, confidentiality is low in distributed healthcare networks.
- In existing system, attribute-based access policy relied on centralized authorities which caused privacy issues.

By considering the above problems, the contributions of proposed model are,

- The OLES-LWT watermark image-based fiddle detection is

 ISBN: 978-93-83191-92-5

proposed to detect the modifications on shared IoT images.

- To solve confidentiality and privacy problems, the EDDH-DSA with FYS-Tiger-based user authorization in blockchain is introduced.

The rest of this paper is organized as follows; Section 2 describes related works of proposed model. Section 3 describes proposed methodologies. Section 5 discusses experimental results. Section 5 concludes the paper.

2. RELATED WORKS

[11]presented a framework for electronic healthcare data security with blockchain and smart contracts. The presented framework utilized Etherium network to store patient data. The framework revealed that the developed system facilitated secure transfer of patient medical records. However, Etherium needed more resources, which create scalability issues in IoMT. [1]suggested a Blockchain-assisted Secure Data Management Framework (BSDMF) for health information on IoMT. In BSDMF, blockchain guaranteed data transmission security between linked nodes. Experimental results revealed a high accuracy ratio, which proved efficacy of the suggested framework. Still, with less than 20 patients, the BSDMF could not provide sufficient trust.

[17] demonstrated a framework for the adaptive security of healthcare IoTs. The framework was developed based on fuzzy logic and Hyperledger blockchain to achieve Authentication, Authorization, and Audit logs. Defined comparison unveiled reliability of the demonstrated model. Yet, fuzzy rules created with human knowledge make the model less reliable.[16] implemented a secure healthcare framework with Optimal Deep Learning-based Secure Blockchain (ODLSB) model. ODLSB leveraged orthogonal particle swarm optimization algorithm for secret sharing of medical images. Presented approach attained the highest accuracy during model validation. Yet, with compression technique in ODLSB model, quality of data could deteriorate when decompressed at the receiver end. [9] developed blockchain for secure data handling in IoMT. Data confidentiality was ensured via a double-encryption mechanism. Experimental outcomes revealed that the developed model performed well with minimum transaction speed. However, double encryption and Proof of Work consensus algorithm could make time inefficient in IoMT.

[7]Investigated a secure data-sharing scheme in cloud-assisted IoMT. The

 ISBN: 978-93-8319

sharing scheme was developed with proxy re-encryption and key blinding techniques. Performance evaluation demonstrated security of the scheme. But, with communication overhead problem, the scheme could not be applicable to larger distributed network.[8] deployed robust authentication protocol for IoMT-based Cloud-Healthcare Infrastructure (CHI). To ensure the security of CHI, an authentication and key agreement were formed. The comparative analysis revealed that deployed scheme was lightweight in terms of computation. But they relied on third-party services and centralized architecture, which caused security threats.

3. PROPOSED IOMT DATA FIDDLE DETECTION AND USER AUTHENTICATION METHODOLOGIES

Medical image watermarking is considered as one of the possible solutions to detect fiddling with received file. Thus, OLES-LWT watermarked image-based IoMT data fiddle detection with FYS-TIGER hashing for user authorization is proposed. The framework of the proposed approach is given in figure 1,

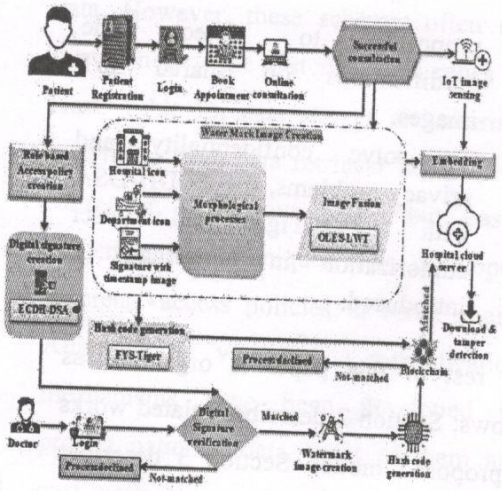

Figure 1: Block representation of the proposed model

3.1 Registration and login

Initially, patient registers their details such as user ID, password on hospital website. After successful registration, patient (P) logs into the hospital website using user ID, and password. If the user ID, and password of P gets matched with the details given during the registration, P is considered as authorized user and can further proceed with processes on the website.

3.2 Booking appointment and online consultation

After successful login of P, P can book an appointment with doctor (D) of the corresponding hospital (H) using patient ID, Doctor ID, and Timestamp. After booking an appointment, consultation will be done and after

 ISBN: 978-93-83191-92-5

successful consultation, IoT image sensing takes place. During IoT sensing image (S), a watermark image is generated by P.

3.3 Watermark image

The watermark image is formed by fusion of morphologically processed hospital icon, department icon, and doctor signature with time-stamp images using the OLES-LWT technique.

Hospital Icon (HI)**:** To obtain watermark image, initially, HI is processed with morphological erosion and dilation process. The morphological process uses a small template called Structuring Element (SE) (E), which determines the number of pixel to be added or removed in HI.

The E eroded and dilated with HI to obtain image (HI_{er}, HI_{dil}) as,

$$HI_{er} = HI \Theta E \quad \ldots (1)$$

$$HI_{dil} = HI \bullet E \quad \ldots (2)$$

Where, $\Theta, \bullet$ depicts erosion and dilation operator.

After erosion and dilation are performed, obtained HI_{er} and HI_{er} are combined with XOR operation as,

$$HI_{image} = HI_{er} \oplus HI_{dil} \quad \ldots (3)$$

Here, HI_{image} depicts the combined HI_{er} and HI_{dil} image, $\oplus$ is XOR operation.

Department Icon (DI): The DI is processed with morphological opening and closing process to remove small objects and holes in DI with SE (ρ) as,

$$DI_{open} = (DI \Theta \rho) \bullet \rho \quad \ldots (4)$$

$$DI_{close} = (DI \bullet \rho) \Theta \rho \quad \ldots (5)$$

Then, morphological opening and closing images (DI_{open}, DI_{close}) are combined to generate image DI_{image} as,

$$DI_{image} = DI_{open} \oplus DI_{close} \quad \ldots (6)$$

Signature with timestamp (ST)**:** Next, doctor's digital signature with time-stamp image (ST) is processed with morphological thinning and thickening to remove and grow selected foreground pixels, which uses hit-and-miss transform (T) and SE (e) as,

$$ST_{thin} = ST - T(ST, e) \quad \ldots (7)$$

$$ST_{thick} = ST \cup T(ST, e) \quad \ldots (8)$$

Where, ST_{thin}, ST_{thick} is morphologically thinned and thickened ST image, and $-$ depicts logical subtraction.

Then ST_{thick} and ST_{thin} are combined to produce an image (ST_{image}) as,

 ISBN: 978-93-83191-

$$ST_{image} = ST_{thin} \oplus ST_{thick} \quad \ldots (9)$$

3.4 Image fusion

The obtained images HI_{image}, DI_{image} and ST_{image} are fused with OLES-LWT approach to obtain a watermark image.Lifting Wavelet Transform (LWT) is considered as it factorizes discrete wavelet transforms with reduced steps, but LWT has the disadvantage of end distortion and frequency aliasing in pixels. To solve this problem Odd Log Even Scaling (OLES) is introduced in LWT technique.

Split: Initially, HI_{image} is split into odd and even (HI_{odd}, HI_{even}) sequences with OLES as,

$$HI_{even} = 2\left(\frac{HI - \overline{HI}}{\sigma}\right)$$
$$HI_{odd} = K_B \log(2.HI + 1) \quad \ldots (10)$$

K_B, σ signifies Boltzmann constant and standard deviation.

Prediction and Updation: Then high-frequency component $(h(HI_{image}))$ prediction and low-frequency component $(l(HI_{image}))$ updationare obtained by,

$$h(HI_{image}) = HI_{odd} - \alpha(HI_{even}) \quad \ldots (11)$$

$$l(HI_{image}) = HI_{even} + \Delta(h(HI_{image})) \quad \ldots (12)$$

$\alpha(\ ), \Delta(\ )$ indicates prediction and updation operation which acts as the high pass and low pass filters. Thus coefficients set (C) of HI_{image} is viewed as,

$$C = \{h(HI_{image}), l(HI_{image})\} \quad \ldots (13)$$

Similarly, coefficient sets for DI_{image} and ST_{image} is obtained with OLES-LWT as (Z) and (X) which contains its corresponding high-frequency and low-frequency components.

Finally, coefficients are fused to obtain fused coefficient image $(\lambda(W))$ as,

$$\lambda(W) = C \otimes Z \otimes X \quad \ldots (14)$$

Here, $\otimes$ is coefficient fusion operator. By applying inverse OLES-LWT on the $\lambda(W)$, the watermark image W is obtained.

Algorithm for proposed OLES-LWT

Input: Images HI_{image}, DI_{image} and ST_{image}
Output: watermark image (W)

Begin
Initialize LWT functions, $K_B, \alpha(\ ), \Delta(\ )$ and $\otimes$
For image (HI) **do**
Perform splitting (HI_{odd}, HI_{even}) via OLES
Predict odd samples with $\alpha(HI_{even})$
Update even samples
Repeat For DI_{image}, ST_{image}
End For

 ISBN: 978-93-83191-92-5

Determine C,Z,X
Apply $\lambda(W)=C\otimes Z\otimes X$
Perform inverse OEEE-LWT
Return W
End

Watermark embedding: This obtained W is then embedded on the IoT sensed image (S) and uploaded on hospital cloud server.

3.5 Hash code generation

For fused image (W), a hash code is generated and stored in block chain using Fishers Yates Shuffled–Tiger (FYS-Tiger) hashing algorithm. Tiger hashing was considered due to its design efficiency of 64-bit processors, but it has setback of pseudo-collision due to eight 64-bit words division of message. To solve this issue, Fisher Yates Shuffling (FYS) technique is included in Tiger Hashing algorithm.

The pixels in image (W), is extracted as bits and then bits are converted to eight 64-bit word and then shuffled with FYS as,

(i) Create a temporary array $(t[\,])$ and store the eight 64-bit words in it and give a value of $(1,2,..,8)$ to each word.

(ii) Select a random value w from $(1,2,..,8)$ and store corresponding word of $t[\,]$ in the end of a new array $(n[\,])$ and delete the word from $t[\,]$.

(iii) Then repeat the process (ii) until all words in $t[\,]$ is deleted. By doing this process, shuffled array of words $n[w_0,w_1,..,w_7]\,or\,n[w_i], i=0,1,..,7$ is obtained.

This array of words is then converted to hash values as,

State update transformation: Tiger hashing starts from fixed three words, which are updated in three passes. In each round, one 64-bit word w_i used to update three state variables β,δ,ε which are considered as initial hash value (λ_0). Thus, save operation in tiger hashing is performed as,

$$\begin{cases}\beta = w_0 w_0\\ \delta = w_1 w_1\\ \varepsilon = w_2 w_2\end{cases} \quad \ldots (15)$$

Key scheduling: After save operation, key scheduling is performed, in which inversion operation is carried out to prevent sparse attack. Thus key scheduling is given as,

$$\begin{cases}\lambda_0(\beta,\delta,\varepsilon)\\ \nabla_1(\beta,\delta,\varepsilon)\\ ks\\ \nabla_2(\beta,\delta,\varepsilon)\\ ks\\ \nabla_3(\beta,\delta,\varepsilon)\end{cases} \quad \ldots (16)$$

Where, $\nabla_1,\nabla_2,\nabla_3$ defines compression operation, and ks depicts the key scheduled.

 ISBN: 978-93

Compression: The compression operation undergoes eight rounds as,

$$\begin{cases} \partial(\beta,\delta,\varepsilon,w_0,mul) \\ \partial(\beta,\delta,\varepsilon,w_1,mul) \\ \quad\vdots \\ \partial(\beta,\delta,\varepsilon,w_7,mul) \end{cases} \quad \ldots (17)$$

Where, $\partial(\ ), mul$ signifies rounding operation and arithmetic multiplication. Then the output hash value is obtained in feed-forward stage as,

$$\begin{cases} \beta_{(1)} \oplus = \beta\beta \\ \delta_{(1)} - = \delta\delta \\ \varepsilon_{(1)} + = \varepsilon\varepsilon \end{cases} \quad \ldots (18)$$

Where, $\beta_{(1)}, \delta_{(1)}, \varepsilon_{(1)}$ is the output 192 bits hash value. This hash code is then stored in blockchain.

3.6 Role-based access policy

When sensed image (S) is shared via cloud, a role-based access policy is created in block chain. Role-based access control policies represent the rights of users in terms of roles to access S. A role-based access control policy is created for D and digitally signed with the EDDH-DSA algorithm and then added to block chain.

3.6.1 Digital signature creation

The role-based access control policy is digitally signed with the EDDH-DSA technique. The Digital Signature Algorithm (DSA) is selected in the proposed model as it provides more message integrity. But, revoking a compromised key is impossible in DSA, which allowed malicious actors to impersonate user privacy without any method of confirmation. To solve this problem, Elliptic Defection Diffie Hellman (EDDH) is used for secret key generation in DSA.

Key generation: Initially, private and public keys are generated on patient and doctor side is generated with Elliptic Curve Cryptography during the P *and* D registration from elliptic curve equation,

$$q^2 = p^3 + a.p + b \quad \ldots (19)$$

Where, p,q denotes p and q-axes respectively, a,b are constant values, in elliptic curve a predefined generator point (g) is taken and multiplied random integers (i.e., private keys) (μ,ω) to generate points in curve as,

$$\left.\begin{aligned} k_P &= g * \mu \\ k_D &= g * \omega \end{aligned}\right\} \quad \ldots (20)$$

Here, k_P, k_D are the public keys generated at P and D side. With μ,ω,k_P,k_D, a

 ISBN: 978-93-83191-92-5

shared secret key (s) is generated with theDiffie Hellman technique as,

$$s = (k_D)^{\mu} \bmod g = (k_P)^{\omega} \bmod g \quad \ldots (21)$$

Where, $(k_D)^{\mu} \bmod g, (k_P)^{\omega} \bmod g$ are computed at the patient's and doctor's side respectively.

Signature generation: Then, a signature for user $(i.e\, D)$ identity (ϖ) is generated with DSA technique using a random integer (τ) and $SHA-1(\varpi)$ as,

$$\left.\begin{aligned} \zeta &= k_D \bmod h + s \\ t &= \tau^{-1}(\hbar + \mu.\zeta) \bmod h \end{aligned}\right\} \quad \ldots (22)$$

Where, $h, \hbar$ defines random constant and $SHA-1(\varpi)$ resultant integer value. (ζ, t) is the signature for identity (ϖ).

3.7 Data access

The registered doctor D, accesses S by successfully logging in to the hospital server. Then after, the digital signature and hash code verification on blockchain, D can successfully retrieve S from cloud.

Signature verification: When D access S then the access policy will be validated by signature verification as,

The $SHA-1(\varpi)$ is performed and integer $(\hbar)$ is generated at the doctor's side. Next, computes the following steps,

$$\left.\begin{aligned} y &= t^{-1} \bmod h \\ z_1 &= \hbar.y \bmod h \\ z_2 &= (\zeta - s).y \bmod h \end{aligned}\right\} \quad \ldots (23)$$

Where, y, z_1, z_2 are computation parameters. The signature is accepted and can access S if,

$$\xi = \hat{k}_D \bmod h = \zeta \quad \ldots (24)$$

Where, $\hat{k}_D$ is integer value computed for k_D. And if $\xi \neq \zeta$, the access of S by D will be rejected.

Hash code verification: After signature verification, watermark image is created at the doctor's side using the OLES-LWT. Then,the hashcode for the corresponding fused image is generated and matched with the $\beta_{(1)}, \delta_{(1)}, \varepsilon_{(1)}$ in the block chain. If generated hashcode gets matched, the S will be downloaded from the cloud.

3.8 Fiddle detection

After S is downloaded by D, the watermark will be removed. If the watermark is completely removed, then it is considered as non-fiddled and will be analysed by D . Else, if the watermark cannot be removed completely, it is regarded as fiddled data and D asks P to resend the data.

4. RESULTS AND DISCUSSIONS

In this section, experimental outcomes of proposed approaches are evaluated in comparison with baseline approaches. The experiments are performed on the working platform of PYTHON, with synthetically generated datasets.

4.1 Performance analysis

Here, performance of the proposed framework is analyzed in three segments namely Image fusion, Hash Code Generation (HCG), and digital signature.

4.1.1 Performance analysis of image fusion

In this subdivision, experimental results based on entropy and fusiontime of watermark image are discussed in comparison with the LWT and Wavelet Transform (WT) techniques. The above table shows the Entropy and Fusion time.

Table 1: Entropy and Fusion Time

Alg	Hospital Icon	Department Icon	Signature with time stamp image	Fused Image using WT	Fused Image using LWT	Fused Image using proposed OLES-LWT
Entropy	6.11989	6.137579	6.174654	6.298994	6.34559	6.403327
Time (ms)	234	236	342	437	467	489

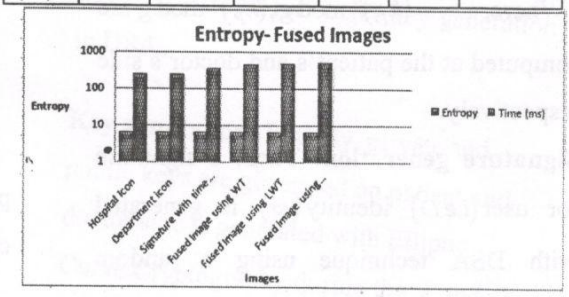

Figure 2: Entropy results of fused images

A system with a higher entropy value depicts that the fused image contains more detailed information. From figure 2, it is evident that entropy of OLES-LWT (6.4033) is higher than baseline LWT and WT techniques. This shows that fusion of HI_{image} , DI_{image} and ST_{image} gives a better watermark than existing techniques.

Table 2: Fusion time results

Algorithms	Fusion time (ms)
Proposed OLES-LWT	298
LWT	381
WT	437

Table 2 unveils fusion time of HI_{image} , DI_{image} and ST_{image} images, in which the proposed OLES-LWT approach

 ISBN: 978-93-83191-92-5

takes 139ms and 83ms lesser than WT and LWT respectively during image fusion. This shows that with OLES-LWT in the proposed framework, watermark image is obtained faster than other techniques.

4.1.2 Performance analysis of hash code generation

The experimental analysis of HCG time of the proposed FYS-Tiger is discussed in this segment in comparison with prevailing hashing algorithms of Tiger, Message Digest-5 (MD5), SWIFFT, and SHA-512. Table 2 shows the Hash code generation.

Table 3: Hash Code Generation

Alg	Hash Code (ms)
Proposed FYS-Tiger	2232
Tiger	2678
MD5	2845
SWIFFT	3158
SHA 512	3354

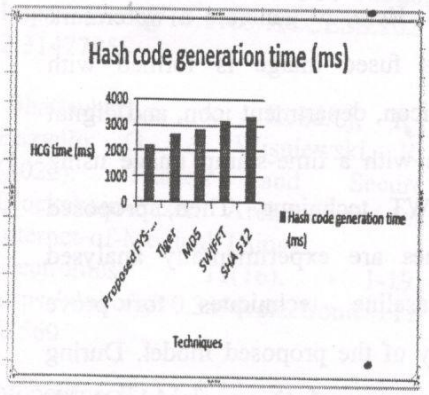

Figure 3: Results of HCG time

From Figure 3, it can be seen HCG is performed in less time with Tiger hashing during the experimental analysis of existing algorithms. But, with FYS in Tiger hashing, HCG time was reduced by 446ms. This shows that FYS-Tiger hash codes are generated in IoMT environment.

4.1.3 Performance evaluation of digital signature

In this phase, digital signature generation and verification times of the proposed EDDH-DSA technique are analyzed in comparison with baseline Elliptic Defection DSA (ECDSA), DSA, Rivest-Shamir-Adlemann (RSA) and Boneh–Lynn–Shacham (BLS). Table 3 shows signature creation and verification.

Table 4 : Signature Creation and Verification

Alg	Signature Creation	Signature Verification
Proposed EDDH-DSA	361	464
ECDSA	393	494
DSA	423	506
RSA	534	522
BLS	541	557

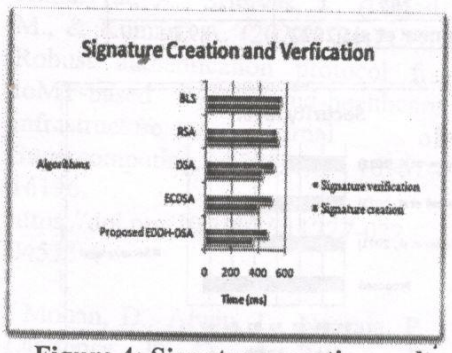

Figure 4: Signature creation and verification time outcomes

Figure 4 unveils experimental outcomes of digital signature creation and verification

 ISBN: 978-93-83191-92

times, in which ECDSA and DSA performed signature creation and verification in less than that of RSA and BLS. Yet, with EDDH key-generation in DSA technique, the proposed EDDH-DSA takes 361ms and 464ms only for signature creation and verification processes. Thus, it is concluded that EDDH-DSA gives better performance in the proposed architecture.

4.2 Comparative analysis

In this section table 5 shows , security level of the proposed framework is compared with the works with security as an objective, such as (Abbas et al., 2021), (Veeramakali et al., 2021), and (Kumar et al., 2022).

Table 5: Security Level

model	Security Level
Proposed	96.54
(Abbas et al.,2021)	94.86
(Veeramakali et al., 2021)	92.9
(Kumar et al., 2022	89.1

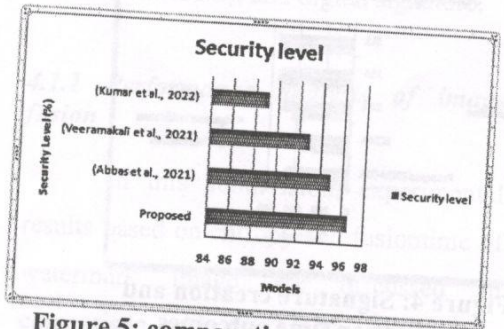

Figure 5: comparative analysis with security level

The comparative analysis of security level of proposed and existing models of(Abbas et al., 2021), (Veeramakali et al., 2021), and (Kumar et al., 2022) are shown in figure 5, where (Kumar et al., 2022)model attained less security by using centralized architecture. But, with watermarking and EDDH-DSA with FYS-Tiger-based user authentication in blockchain, the proposed model attained the highest security level of 96.34% in IoMT environment. Also, even with block chain technology, models of(Abbas et al., 2021)and (Veeramakali et al., 2021) attained 1.54% and 3.57% less security than the proposed model. Thus, it is verified that proposed model is suitable for securing data in IoMT.

5. CONCLUSION

In this paper, a novel fiddling detection and EDDH-DSA with Fys-Tiger-based block chain verification in IoMT is proposed. Here, to generate a watermark image, a fused image is formed with hospital icon, department icon, and digital signature with a time-stamp image using OLES-LWT technique. Then, proposed approaches are experimentally analysed with baseline techniques to prove reliability of the proposed model. During fusion image analysis, proposed OLES-LWT attained higher entropy (6.4033) and less fusion time (298ms). Also, HCG, signature generation, and verification times of the proposed techniques are less

than state-of-the-art techniques. Finally, security analysis proved the objective of proposed model by providing high security in IoMT environment. In this work, IoMT data fiddlingdetection is concentrated. In the future, the appropriate technique can be introduced to avoidfiddling with IoMT data.

REFERENCES

[1] Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2021). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and Ubiquitous Computing. https://doi.org/10.1007/s00779-021-01583-8

[2] Bataineh, M. R., Mardini, W., Khamayseh, Y. M., & Yassein, M. M. B. (2022). Novel and Secure Blockchain Framework for Health Applications in IoT. IEEE Access, 10, 14914–14926. https://doi.org/10.1109/ACCESS.2022.3147795

[3] Bhattacharjya, A., Kozdrój, K., Bazydło, G., & Wisniewski, R. (2022). Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things. Electronics, 11(16). 1-19. https://doi.org/10.3390/electronics11162560

[4] Fotopoulos, F., Malamas, V., Dasaklis, T. K., Kotzanikolaou, P., & Douligeris, C. (2020). A Blockchain-enabled Architecture for IoMT Device Authentication. 2ndIEEE Eurasia Conference on IOT. https://doi.org/10.1109/ECICE50847.2020.9301913

[5] Garg, N., Wazid, M., Das, A. K., Singh, D. P., Rodrigues, J. J. P. C., & Park, Y. (2020). BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment. IEEE Access, 8, 95956–95977. https://doi.org/10.1109/ACCESS.2020.2995917

[6] Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2021). Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. IEEE Internet of Things Journal, 8(11), 8707–8718. https://doi.org/10.1109/JIOT.2020.3045653

[7] Hao, J., Tang, W., Huang, C., Liu, J., Wang, H., & Xian, M. (2022). Secure Data Sharing With Flexible User Access Privilege Update in Cloud-Assisted IoMT. IEEE Transactions on Emerging Topics in Computing, 10(2), 933–947. https://doi.org/10.1109/TETC.2021.3052377

[8] Kumar, V., Mahmoud, M. S., Alkhayyat, A., Srinivas, J., Ahmad, M., & Kumari, A. (2022). RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. Journal of Supercomputing, 78(14), 16167–16196. https://doi.org/10.1007/s11227-022-04513-4

[9] Mohan, D., Alwin, L., Neeraja, P., Lawrence, K. D., & Pathari, V. (2022). A private Ethereum blockchain implementation for secure data handling in Internet of Medical Things. Journal of Reliable Intelligent Environments, 8(4), 379–396. https://doi.org/10.1007/s40860-021-

00153-2

[10] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain. IEEE Internet of Things Journal, 8(14), 11743–11757. https://doi.org/10.1109/JIOT.2021.3058953

[11]Nishi, F. K., Shams-E-Mofiz, M., Khan, M. M., Alsufyani, A., Bourouis, S., Gupta, P., & Saini, D. K. (2022). Electronic Healthcare Data Record Security Using Blockchain and Smart Contract. Journal of Sensors. https://doi.org/10.1155/2022/7299185

[12] Ogundokun, R. O., Awotunde, J. B., Adeniyi, E. A., & Ayo, F. E. (2021). Crypto-Stegno-based model for securing medical information on IOMT platform. Multimedia Tools and Applications, 80(21–23), 31705–31727. https://doi.org/10.1007/s11042-021-11125-2

[13] Quasim, M. T., Algarni, F., Radwan, A. A. E., & Alshmrani, G. M. M. (2020). A Blockchain-based Secured Healthcare Framework. 2020 International Conference on Computational Performance Evaluation. https://doi.org/10.1109/ComPE49325.2020.920002

[14] Swetha, M. S., Pushpa, S. K., Muneshwara, M. S., & Manjunath, T. N. (2020). Blockchain enabled secure healthcare Systems. IEEE International Conference on Machine Learning and Applied Network Technologies. https://doi.org/10.1109/ICMLANT50963.2020.9355970

[15] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 1-13. https://doi.org/10.1016/j.jisa.2019.102407

[16]Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P. C., & Krishnaraj, N. (2021). An intelligent internet of things-based secure healthcare framework using block chain technology with an optimal deep learning model. Journal of Supercomputing, 77(9), 9576–9596. https://doi.org/10.1007/s11227-021-03637-3

[17] Zulkifl, Z., Khan, F., Tahir, S., Afzal, M., Iqbal, W., Rehman, A., Saeed, S., & Almuhaideb, A. M. (2022). FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs. IEEE Access, 10, 15644–15656. https://doi.org/10.1109/ACCESS.2022.3149046