e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

FOG COMPUTING TO DEVELOP SECURITY MODEL USING BILINEAR PAIRING CRYPTOGRAPHY

Dr. P. Maragathavalli*[1], S. Atchaya*[2], N. Kaliyaperumal*[3], S. Saranya*[4]

*[1]Assistant Professor, Department Of Information Technology, Pondicherry Engineering College, Puducherry, India.

*[2,3,4]Student Member, Department Of Information Technology, Pondicherry Engineering College, Puducherry. India.

ABSTRACT

Cloud Computing Is A Significant Technology Which Is Deployed In Enormous Business Area Including Medical Field. The Main Objective Of The Proposed Work Is To Secure The Private Data Of The Medical Field In Cloud Computing With The Help Of Fog Computing. In Addition To That Tri-Party Authenticate Key Is Proposed Using Bilinear Pairing Cryptography That Generates The Key Among The Users And For Secure Communication. By Decoy Technique, The Data's Of The Healthcare Can Be Accessed And Stored. The Decoy Detects The Attacker When He Is Accessing The Data And Ensures The Data Security. Thus The Double Security Keeps The Encrypted Files When It Recognizes The Attacker By Securing The Medical Data Secure And Limit The Process To A Legitimate User By Verification. By Using Triple Des Algorithm The Execution Time Of Encryption And Decryption Process And Computational Complexity Will Be Decreased.

Keywords: Remote Database; Security And Privacy; Medical Big Data Analytics; Electronic Medical Record; Key Agreement Protocol, Cryptography Algorithm.

I. INTRODUCTION

Cloud Refers To Manipulate, To Configure And To Access The System Hardware And System Software Resources And Offers To Store The Data In Online, Infrastructure And Application. It Is A Group Of Servers Which Is Connected For Providing The Storage, Power, Services And Other Resources Over Internet. It Also Provides Adding And Releasing The Services At The Moment We Need. It Guarantees Maximum Resources On-Demand.

The Hybrid Cloud Which Has Healthcare Field For The Record Sharing And Record Accessing Is Used To Store The Healthcare Data's Of The Patient And Also By Managing The Records Of The Patient, Tracking Them When The Patient Moves Anywhere. It Also Has Many Security Issues Like Privacy, Security, Issues Of The Policy, Transparency, Data Protection And Licensing. In Order Achieve Safe And Secure Healthcare Field The Fog Computing Has Been Used In Our Proposed Methodology.

II. RELATED WORK

Table 1. Comparison Of Existing Works

S.No	Name Of The Journal, Year	Title	Techniques Used	Dataset	Parameter	Limitation
1.	Ieee Internet Of Things Journal,2021	An E-Healthcare Authentication Protocol Employing Cloud Computing	Decoy Technique	Multimedia Dataset	Computational Complexity	Time Consumption Is High
2.	Ieee International Conference On Communications (Icc), 2021	Privacy-Preserving Computation Offloading For Time-Series Activities Classification In	Grid Computing	Multimedia Dataset	Time Consumption	Not Applicable For Large Scale Medical Access

		E-Healthcare				
3.	Ieee System Journal, 2020	Improving Security And Privacy Attribute Based Data Sharing In Cloud Computing	Cipher Text-Policy Attribute Based Encryption (Cp-Abe)	Dataset From Google Url	Computational Overhead	Weak Security Model
4.	Ieee Transactions On Dependable And Secure Computing, 2020	A Novel Smart Healthcare Design, Simulation And Implementation Using Healthcare 4.0 Processes	Block Chain	Array Dataset	Time Consumption	Addition Of Implementation Shows An Error
5.	Ieee Transactions On Emerging Topics In Computing,2020	Secure Verifiable Database Supporting Efficient Dynamic Operations In Cloud Computing	Boneh–Lynn–Shacham(Bls) Signature	Array Dataset	Computational Cost	Pairing Is Not Efficient

In The Above Table The Related Work Is Done From An Existing System Which Has Some Limitations In Time Consumption, Pairing, Weaker Security Model And Those Limitations Are Considered In Our Project.

III. PROPOSED METHODOLOGY

The Proposed Work Focuses On Keeping Original Medical Big Data (Ombd) Private By Detecting The Intruder By User Profiling And Using Decoy Medical Big Data (Dmbd) As A Honeypot. Pre-Existing Values Are Used To Protect Dmbd Data, And An Effective Tri-Party Authentication Key Is Provided. This Dmbd Is Located In User Profiling In The Fog Computing Layer And Contains Fake Medical Big Data (Mbd), Giving The Attacker The Impression That They Are Viewing The Ombd. The Intruder Is Identified By User Profiling, And An Email Is Sent To The User Informing Him That His Account Has Been Accessed, Along With Information Such As The Access Time, Date, And Ip Address. Now, If The Customer Wishes To Upload His Medical History, The Tri-Party Must Be Informed. The Tri-Party Receives The Secret Key, Which Is Provided By The Private Key Generator (Pkg). Each Party Must Now Authenticate With Another Party In Order To Connect With Others In Private. The Triple-Des Algorithm Is Then Used To Encrypt The Patient Records. This Encrypted Data Are Saved In The Cloud And Then Decoded Using This Protocol For Display Purposes. As A Result, Two Levels Of Encryption Are Proposed: First, Using Dmbd As A Honeypot, And Second, Secretly Storing Encrypted Medical Records In The Cloud. The Suggested Scheme Is Illustrated In Figure 1.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

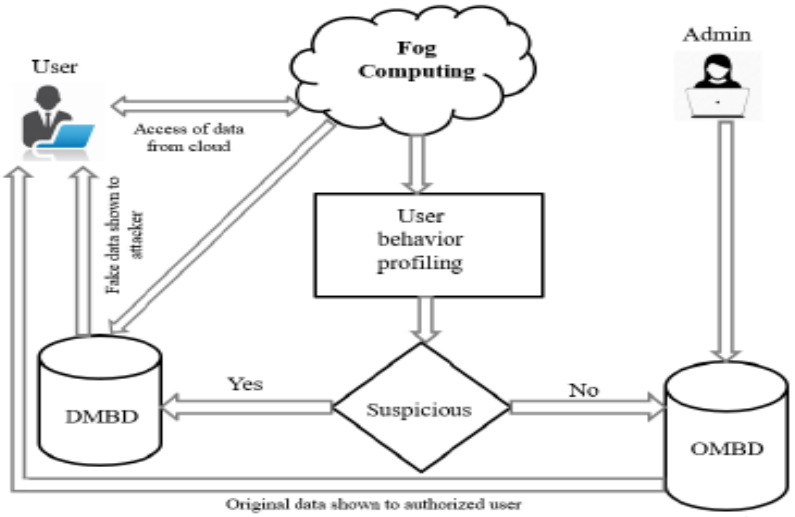

Fig. 1: Detailed Design Diagram

IV. IMPLEMENTATION

With User Profiling, The Decoy Technique Generates Fake Files Or Replica Medical Data And Detects Illegal Users. It Also Aids In The Protection Of Users' Medical Information By Providing A Fake Gallery To The Attacker.

4.1 Automatic Key Generation

Medical Healthcare Big Data Analysis For Preserving Security And Privacy With Hybrid Cloud Technology. So, The Data Must Be Secured Based On The Automatic Key Generation Protocol. In This Authentication And Authorization, To Eliminate The Key Details, It Should Be Joined Between The Supplicant And Authentication Server. It Is Transferred With Secure Channel From Server To The Authenticator. Using Automatic Key Generation Channel, Message Has Been Sent With The Secured Way, And Also Reception Of Message Is Also Secured. The Channel Initialized With Secure Way Is Explained And Is Given Below With Pseudo Code.

4.2 Authentication

Initially Both The User And Attacker Will Be Accessing The Dmbd And They Are Considered As The Unauthorized Users. This Dmbd Is Placed In The Fog Computing Layer Near User Profiling And It Contains The Fake Medical Big Data (Mbd) Which Makes The Attacker To Believe That They Are Accessing The Ombd. When The User Gets To Know That It Is Not His Profile He Will Be Going To The Next Process Of Verification And After Passing Some Security Challenges He Will Be Accessing The Ombd. By User Profiling The Attacker Is Detected And Sms Is Sent To The User That His Account Being Accessed And It Contains Information Like Access Time, Date And Ip Address.

4.3 Encryption

The Encryption Process Is Completed Until The Patient Uploads The Medical Record. Asymmetric Coding Is Used To Protect The Patient Record. With The Secret Key Provided By The Private Key Generator, Triple Des Is Used (Pkg). The Cypher Picture Is Now Created From The Original Record. With The Support Of A Cloud Service Provider, This Encrypted Cypher Image Is Safely Stored In The Cloud.

4.4 Decryption

The Method Of Translating Encrypted Data Into Plain Text Is Known As Decryption. With The Secret Key Produced By The Private Key Generator, The Cypher Image Back To The Cloud Service Provider Is Decrypted Into The Original Data, And The Original Data Is Made Available To The User.

Thus In This Section Of Paper The Above Implementation Are Implemented Involved With Workflow Diagrams In Developing The Proposed System Were Discussed With Detailed Explanation.

V. RESULT ANALYSIS

Our Proposed Method Is Medical E-Healthcare Big Data Analysis To Analyse The Performance With Various Strategies. The Performance Is Analysed Based On The Parameters Such As

1. Execution Time
2. Computational Complexity

5.1 Execution Time

The Execution Time Will Be Analysed Which Is Defined As The Rate Of The Amount Of Time Taken For Individual Key Size To The Total Rate Of The Time Consumption.

$$Execution\ time\ = Data\ size\ /\ Total\ rate\ of\ time\ consumption$$

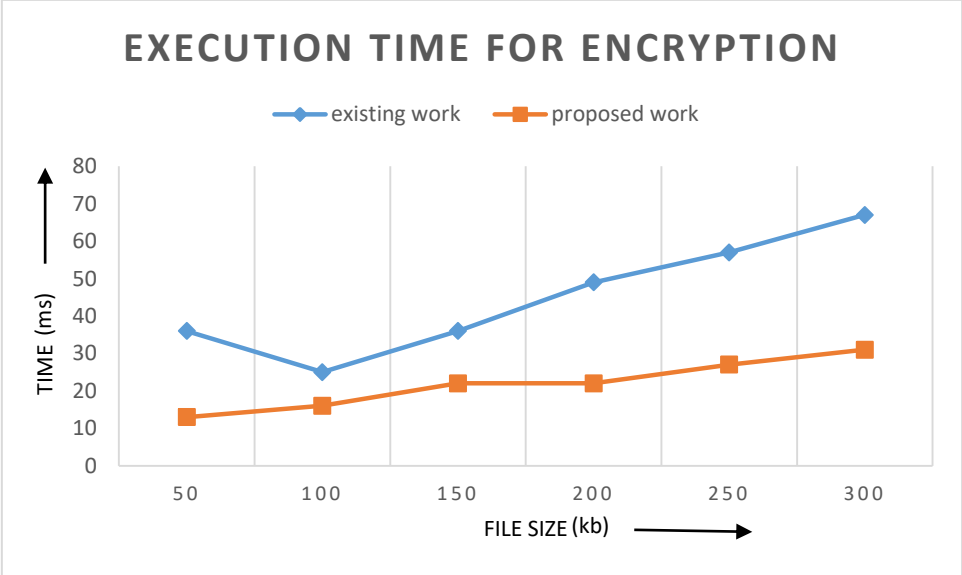

Fig. 2(A): Execution Time For Encryption

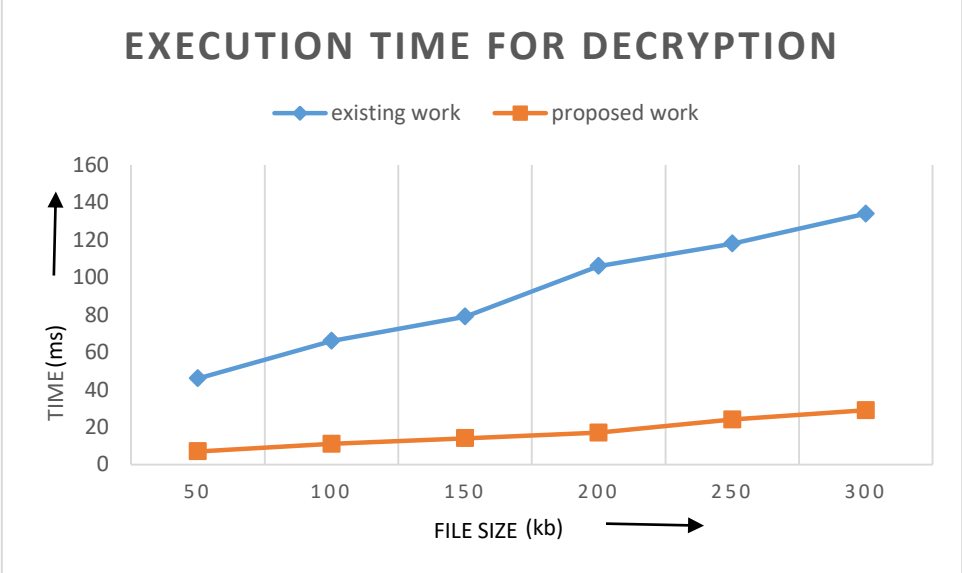

Fig. 2(B): Execution Time For Decryption

The Different Files Is Encrypted And Decrypted Against Encryption And Decryption Processes. That Evident From The Results Of Testing That The Proposed Encryption Process Is Faster Than Existing Work, As Well As The Decryption Process Is Also Faster Than Existing Is Given In The Figure 2(A) And 2(B). Thus By Using The 3des Algorithm In The Encryption And Decryption Process The Time Consumption Is Reduced In The Proposed Work Whereas In The Existing Work, It Slows Down The System By 20% Using Des Algorithm.

5.2 Computational Complexity

The Computational Complexity Is To Be Estimated Based On The Performance Of The System; The Complexity Is To Be Analysed Based On The Number Of Bilinear Pairing. The Quadratic Computational Complexity Is To Be Analysed Which Is Denoted As The Following Equation:

$$B(n) = O(n^2)$$

Where B(N) Is The Bilinear Pairing Function And The O(N) Is The Complexity Analysis Function.

Here The Computational Complexity Is Measured Based On Number Of Bilinear Pairing As The Parameter. Figure 3 Shows The Comparison Of Computational Complexity In Existing And Proposed Work Where Our Proposed Work Is 20% Efficient Than The Existing Work And Number Of Bilinear Pairing Is Considered As The Parameter.

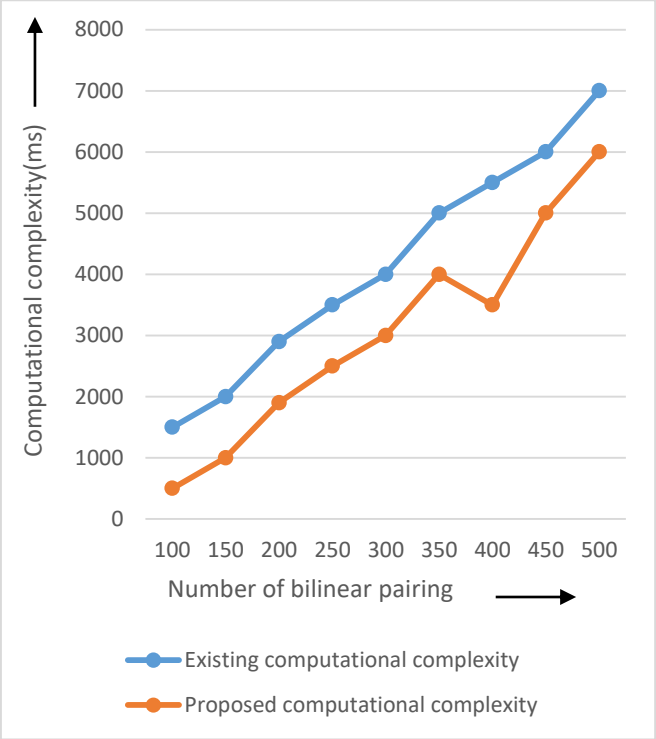

Fig. 3: Computational Complexity Analysis

Figure 3 Shows The Computational Complexity Present In The Number Of Bilinear Pairing Methods Compared To Existing Method. It Gives The Details About The Computational Complexity Present In The Big Data (Cloud Server) For Existing Method And Proposed Method. Rate Of The Task Should Be Completed To The Total Time Taken From That Particular Task. It Depends On The Various Kinds Of Resources And Various Levels.

VI. CONCLUSION

Fog Computing Has Been Used To Build A Cloud Data Management Model For Securing Patient Information In The Ehr Environment, With Two Layers Of Security. By Using User Profiling, The Intruder May Be Identified As The Honey Pot As In Decoy Gallery. The Original Medical Big Data (Ombd) Is Kept Locked In Private Cloud, While The Decoy Medical Big Data (Dmbd) Is Kept In The Fog Computing Field. When A Person Wishes To Use The Ombd, They Must First Verify Their Identity. As A Result, Saving The Ombd As A Secret Gallery Secures It. A Private Key Generator (Pkg) Is Used To Communicate Between Ombd And Dmbd. The Suggested Approach Reduces The Execution Time For Encryption And Decryption By 0.25s And Computational Complexity By 20%. The Future Direction Is To Include Developing Appropriate Privacy Solutions.

VII. REFERENCES

[1] G. Manogaran, T. Baabdullah, D. B. Rawat And P. M. Shakeel, " An E-Healthcare Authentication Protocol Employing Cloud Computing"In Ieee Internet Of Things Journal, 06 May 2021, Doi: 10.1109/Jiot.2021.3077895.

[2] Y. Zheng, R. Lu And M. Mamun, "Privacy-Preserving Computation Offloading For Time-Series Activities Classification In Ehealthcare," Icc 2020 - 2020 Ieee International Conference On Communications (Icc), 2020, Pp. 1-6, Doi: 10.1109/Icc40277.2020.9148875.

[3] Y. Zheng And R. Lu, "An Efficient And Privacy-Preserving K-Nn Query Scheme For Ehealthcare Data," 2020 Ieee International Conference On Internet Of Things (Ithings) And Ieee Green Computing And

Communications (Greencom) And Ieee Cyber, Physical And Social Computing (Cpscom) And Ieee Smart Data (Smartdata), 2018, Pp. 358-365, Doi: 10.1109/Cybermatics_2018.2018.00088.

[4] Shanmugapriya. E And Kavitha.R. "Medical Big Data Analysis: Preserving Security And Privacy With Hybrid Cloud Technology", Soft Computing, Springer 23, 2585–2596 (2019). Https://Doi.Org/10.1007/S00500-019-03857-Z.

[5] M. Joshi, K. Joshi And T. Finin, "Attribute Based Encryption For Secure Access To Cloud Based Ehr Systems," 2018 Ieee 11th International Conference On Cloud Computing (Cloud), San Francisco, Ca, 2018, Pp. 932-935, Doi: 10.1109/Cloud.2018.00139.

[6] M. Du, K. Wang, X. Liu, S. Guo And Y. Zhang, "A Differential Privacy-Based Query Model For Sustainable Fog Data Centers," In Ieee Transactions On Sustainable Computing, Vol. 4, No. 2, Pp. 145-155, 1 April-June 2019, Doi: 10.1109/Tsusc.2017.2715038.

[7] J. Liu, H. Tang, R. Sun, X. Du And M. Guizani, "Lightweight And Privacy-Preserving Medical Services Access For Healthcare Cloud," In Ieee Transaction On Dependable And Secure Computing, Vol. 7, Pp. 106951-106961, 2019, Doi: 10.1109/Access.2019.2931917.

[8] L. Zhang, Y. Cui And Y. Mu, "Improving Security And Privacy Attribute Based Data Sharing In Cloud Computing," In Ieee Systems Journal, Vol. 14, No. 1, Pp. 387-397, March 2020, Doi: 10.1109/Jsyst.2019.2911391.

[9] P. Maragathavalli, S. Atchaya, N. Kaliyaperumal And S. Saranya, "Security Model Using Modified Decoy Technique In Fog Computing For E-Healthcare", Published Under Licence By Iop Publishing Ltd, Iop Conference Series: Materials Science And Engineering, Volume 1065, February 2021, Https://Doi.Org/10.1088/1757-899x/1065/1/012044.

[10] Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover And E. Hossain, "A Novel Smart Healthcare Design, Simulation, And Implementation Using Healthcare 4.0 Processes," In Ieee Transaction On Dependable And Secure Computing, Vol. 8, Pp. 118433-118471, 2020, Doi: 10.1109/Access.2020.3004790.

[11] J. Shen, D. Liu, M. Z. A. Bhuiyan, J. Shen, X. Sun And A. Castiglione, "Secure Verifiable Database Supporting Efficient Dynamic Operations In Cloud Computing," In Ieee Transactions On Emerging Topics In Computing, Vol. 8, No. 2, Pp. 280-290, 1 April-June 2020, Doi: 10.1109/Tetc.2017.2776402.

[12] Https://Www.Kaggle.Com/Nikhilpandey360/Chest-Xray-Masks-And-Labels