An Efficient Multi-Mode Three Phase Biometric Data Security Framework For Cloud Computing-Based Servers

Ayesha Tarannum[1], Md. Zia Ur Rahman[1*], Srinivasulu T[2]

[1]*Dept. of E.C.E, KoneruLakshmanih Education Foundation, K L University, Green Fields, Vaddeswaram, 522052, Guntur, A.P, India.*

[2] *Department of Electronics and Communication Engineering, Kakatiya University, Warangal, T.S, India.*

[1]ayeshabad14@gmail.com; [2*]mdzr55@gmail.com; [3] drstadisetty@gmail.com

Abstract *— In public and private cloud servers, multimedia data is increasing day by day and it is hard to provide security properly because of limited storage capacity problems. So, to avoid these storage and security problems, conventional single biometric and various biometric model are used. These conventional models are depending on data size and file format with existed integrity and confidential methods on limited cloud data types. Therefore, to overcome these problems, integrity based a three stage multi use multi modal (MUMM) secured frame work along with large cloud data types is proposed. In the proposed work, to execute a strong data security system on cloud databases biometric images like IRIS and finger knuckle features are utilized. For improving large data security, classification-based CNN, hybrid feature extraction measures, integrity and encryption-based methods are used. Then results shows that proposed model has preferable efficiency compared to conventional multi modular security models for large data cloud data files and it has accomplished positive rate of 0.987, integrity bit variation of 8.7% and better runtime compared existed models.*

Keywords *— Biometric authentication, cloud computing, cyber physical system, convolutional neural network, multi-mode security.*

I. INTRODUCTION

Cloud computing give instant access to several healthcare resources, applications and tools for patients, doctors, health care workers and administrators. With the Cloud computing the cost of data centers establishment is going to be reduced, and smart hospitals can be enabled to provide remote diagnosis and treatment. In such a case, providing security for the data extracted from the patient is the major issue. Hence, an efficient and accurate privacy mechanism is needed to keep the medical data of patient securely in cloud server. Many techniques for encryption are proposed to protect the patient's data. The encryption procedure is very much difficult process and it has the responsibility to not permit the unauthorized data access. Homomorphic type of encryption process aims to support the process of complete computation process. Additionally, it provides enforce data integrity and security constraints. The major defect in the homomorphic encryption process is that it is a single user-based system. The traditional homomorphic encryption technique is unable to support multiple users. The number of operations of the cipher texts is restricted. Fully homomorphic encryption technique is implemented to support several computations of cipher texts. In [1] a fully distributed revocable cipher text aspect encryption process is developed to give scalability and flexibility for user revocation mechanisms in key delegation to control over cipher texts when it is accessed by unauthorized users in cloud. To overcome problems of existed multi authority attribute-based encryption scheme proposed a attribute based encryption scheme in mobile cloud storage to reduce privacy problems and to increase confidential information in cloud [2]. In [3] a policy hidden outsourced aspect-based encryption scheme (PHOABE) is developed to share efficient data among different users and also to overcome computational costs decryption problems in cloud based IoT. To improve data confidentiality in cloud computing over encrypted data used security principle i.e., access control aware search (ACAS) also proposed a hybridization of searchable encryption and attribute-based encryption to satisfy ACAS and it supports multi user access [4]. By using mobile cloud computing, phone user sharing information and it not fully secured, so proposed a online/offline attribute based keyword search engine (OOABKS) and implemented fine grained control access to user to provide data and keyword security to users [5-7]. Use of IoT and cloud computing increased rapidly in gadgets, it generates huge amount of data and this information is shared with the help of fine grained access control, then it is encrypted using cipher text policy attribute based encryption (CPABE) and it is having computational problems, to reduce this proposed a LIKC scheme using a proxy server [8-10]. In [11] an attribute aspect based online or offline searchable encryption technique is implemented to avoid burden on

encrypted retrieving data in application of cloud based smart grid. In [12] an attribute-based broadcast encryption is proposed to overcome drawbacks of decryption problems in cipher text attribute-based encryption and using this proposed scheme flexible and personal data sharing in cloud computing is shown. Lightweight attribute-based encryption scheme (LABE) is proposed f1or variable cloud based cyber physical system (CPS) for proxy service and cipher text policies then we get low overhead on mobile devices performs well in cloud [13-16]. To obtain secure data from cloud an efficient data collaboration mechanism is implemented using fine granted access control for cipher text with help of attribute-based encryption and attribute-based signature to relieve burden on key management of hierarchical attribute-based encryption [17-19].

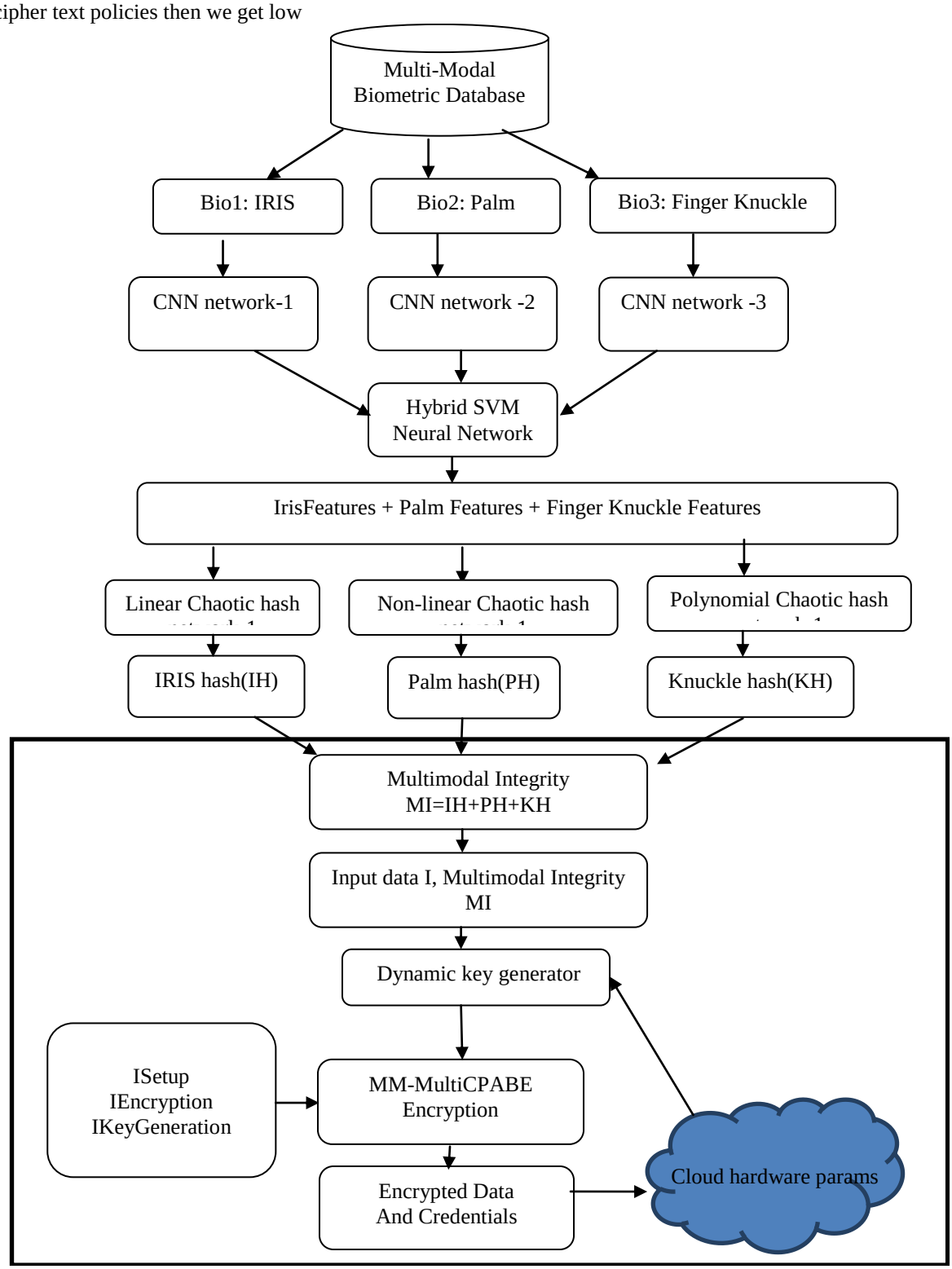

Fig.1: Proposed Multimodal based MI-CPABE Encryption Process

In [20] an efficient data retrieval scheme with help of attribute-based encryption is proposed to encrypt data in cloud and it retrieves large amount of data, the data is retrieved in a secure and user privacy also maintained with this method. Cloud computing is using tremendously in IT filed also but it has security and privacy problems. It is recovered by proposing an enhanced attribute-based encryption scheme using hash functions, asymmetric encryptions and signatures [21]. Multi-channel broadcast encryption (MCBE) and attribute-based encryption (ABE) are proposed techniques in cloud computing to send different messages in same time using a secret key also proposed a new method to compact header size problems in MCBE and ABE to with public key [22]. To recover unimodal biometric problems a secure multimodal biometric system is implemented using electrocardiogram (ECG) fusing and finger print based convolution neural network (CNN) to identify human authentication [23]. CNN based electrocardiogram (ECG) biometric authentication is proposed to know aliveness of person used scanning and removing method for human authentication [24].

II. PROPOSED MODEL

In this proposed system, a hybrid deep learning based muti-modal biometric framework is developed based on the different biometric databases. In this framework, a real-time cloud server is used as an intermediate system for data processing and storage services. Proposed technique is developed in 3 phases that are features extraction, classification, parallel multi-modal chaotic hashing and chaotic multi-modal [25] integrity-based data security. In the initial phase, biometric input databases such as finger knuckle and IRIS are taken to identify the necessary key features. In this phase, IRIS and knuckle features are obtained by using CNN network model with optimized filters and classification model. Biometric features are used in the second phase to compute the parallel chaotic hash value for encryption process as shown in fig 1. In the final phase, parallel bio-modal hash key [26] is used to encrypt and decrypt the cloud data for strong security. The overall parallel bio-modal multi-user encryption and decryption process are presented in fig 1. In the fig 1, the vital features of biometric data are extracted using the proposed filtered based CNN framework. In this CNN network model, the vital feature extraction and classification processes are used to find the secure bio-modal key for integrity computation and encryption process. In the integrity computation method, IRIS features are given to linear chaotic function to determine hash vale. In the same way, knuckle features are given to polynomial chaotic function to obtain the hash vale. Multi-modal parallel chaotic hash value is developed with the three biometric hash values. Here, the developed multi-modal chaotic hash is used to improve the encryption and decryption process of data as shown in fig 1. Multi-user encrypted data is saved in cloud server for real-time access. In the decryption process, the encrypted form of data from the server is considered as input along with multi-user biometric features [27-28].

Parallel Multi-Modal Feature Extraction Using CNN Deep learning Framework

For the prediction of features the conventional C3D deep learning network models use convolution kernels of 3 × 3 × 3 in the filtering process. This model is used to determine the features which are at low-level and filtering the vital features of input images. For the confidentiality of data, the vital features are obtained by using convolution layers, max pooling and filtering process. Then by using fully connected SoftMax function the vital features are filtered out from the corresponding images as described in figure 2. The classification of biometric features is performed by using the non-linear SVM model.

In the proposed CNN framework, different feature selection measures are used to extract the vital features in the IRIS and Knuckle biometric images. In the proposed CNN framework, log inverse differential moment and max correlation inertia are used to find the vital marked features for multi-modal integrity computation. The log inverse differential moment and max correlation inertia are determined by using the following considerations. In the CNN network model, different feature sets in the biometric images are classified using the hybrid non-linear SVM model. In the implemented integrity computational technique, the input for the generation of chaotic key and processing of sub blocks data is the multi-modal features of biometric images.

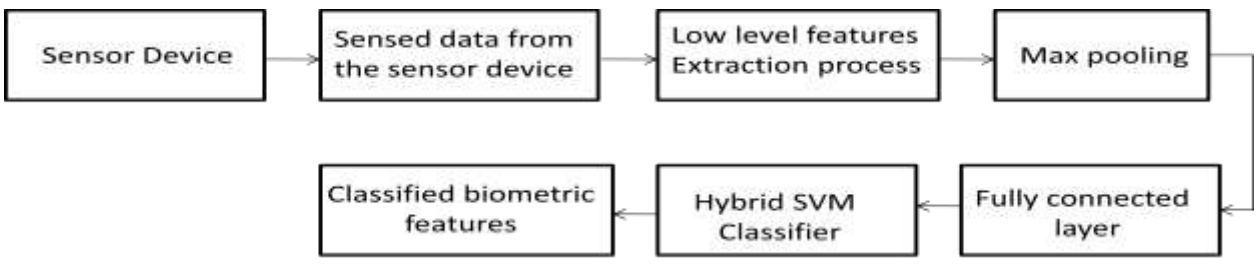

Fig.2: Classification based Bio-modal feature extraction

In this parallel chaotic integrity computation, the features of IRIS and Knuckle are applied to hybrid linear, extended non-linear chaotic and polynomial chaotic functions for the integrity computation as described in fig 2. There are only two parameters α and β are existed in dynamic chaotic map function. Moreover, the chaotic region can be estimated easily for the constant weighted parameters and as r is in between from 0 to N. In the proposed model hash algorithm, each biometric feature is given to each chaotic map for the implementation of secret key. Thus, this secret key is used as input for the hash algorithm. In the implemented integrity computation model, every block is divided into sub-blocks for the operations of chaotic sub block. Several mathematical functionalities such as SVD, eigen values, transformation etc are used in this process to obtain the integrity value with highest bit change.

III. EXPERIMENTAL RESULTS

The experiments are simulated in amazon cloud computing database with python and java programming environments. Proposed model is simulated on multiple biometric image databases. These databases are taken from https://www4.comp.polyu.edu.hk/~csajaykr.

A. Sample IRIS images for CNN key points extraction and multi-modal integrity generation.

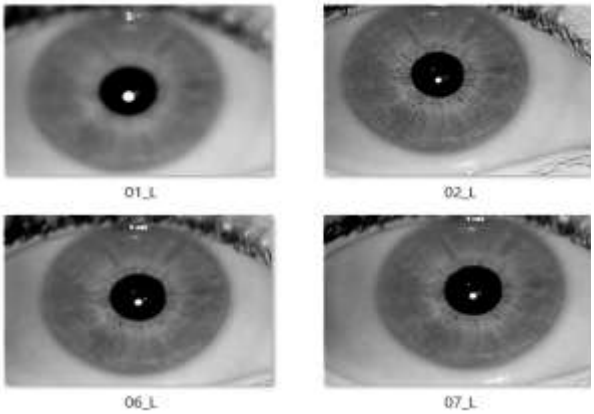

Fig.3: Sample IRIS images

Figure 3, describes the set IRIS images for the extraction of vital features. IRIS input images are given to CNN network model with customized filters for vital features extraction process. Here, several IRIS images of various users are used to integrate the multi-modal hash vale for cloud data security. IRIS key points and its 2048-bit hash values are shown in table 1.

B. Knuckle features evaluation

Figure 4, describes the set of knuckle images for features extraction and integrity computation. These sample knuckle images are given to filtered based CNN network model to extract vital feature for integrity computation. CNN generated key points and its hash values are shown in table 2.

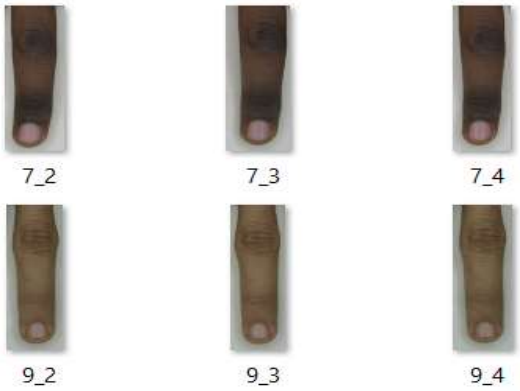

Fig.: Sample knuckle images

Figure 5, describes the performance comparison of parallel chaotic hash to the existing hash algorithms in terms of average cloud runtime computation. From this diagram, we can conclude that the developed parallel chaotic multi-modal integrity model gives better performance in the cloud computing environment than the existing models on large databases.

Table 3, describes the performance comparison of hash bit change of developed parallel chaotic integrity model to the traditional methods. In this we have taken the size of hash input as 2048 bits. From this table, we can observe that the implemented model integrity computation model shows better performance than existed integrity models on large cloud dataset.

TABLE 1
IRIS Key points and its hash value

183.0,131.0 := Integrity value :1379550a7cb1ef38411c8c84fbc0b835202e0b7223c5f652a6f9b9eb0a97e24e479031d9db0f5665be2566e08a25e580b58b19c07cf1c78ce4adda25ba564704e11991b3319868c30c6488bcaf88c6e744dc7157f8fa6066ff1c8c6116aee7e7642588cdf22ec30ff9042e06e585bc9dca9f808c7c0dcdf40aac5d9214372abf26d86d18f8d3bde11c14beb4105c21febc5b878d274b09026f6370daf61e3dde530b7a126ab3e178084f3f55387509da8808e9c94e6f5b3232fefd895b6b9690808c91d79d536619420f4ac3c443910e2ad4dedd586c92a6fc7581ffbbd466fb3c8880febcff37c51f9341ccb1f78444ae918bed85fccba9e30359ff0a8f2a9a

TABLE 2
Knuckle key points and its integrity values.

100.0,107.0 := Integrity value :bc0fa297f09d02712ea950158572dbca11fafe072394c01bf18512f7aa76cc6b2f4a83d2624d504e3aa37df 7cb7f13125944b348903e6d04086270ad5699ed8c65e32c66909b7d90ac3af715b84db05b8837169cb686 5cd062bbc207d935ff8bd21f1282fd052e9877f89dc6686abfe206bca9497c0582ee715bd24a182314994b e9b509fc1785ab80ee488d41f403c9436286007358b08f4514752b3d34163a54a17d23e15d54757939134 94b1c32907d631fcdf26ef56eb20469991dc3d9b7b9dacaeefe7b2dea24a27ff89976828b90503beacf2c8d 1193d83872cb49dbf890474d2f0eca7aba89f50af72d23164ba75ae1d06869faa48785638dd8df753f.

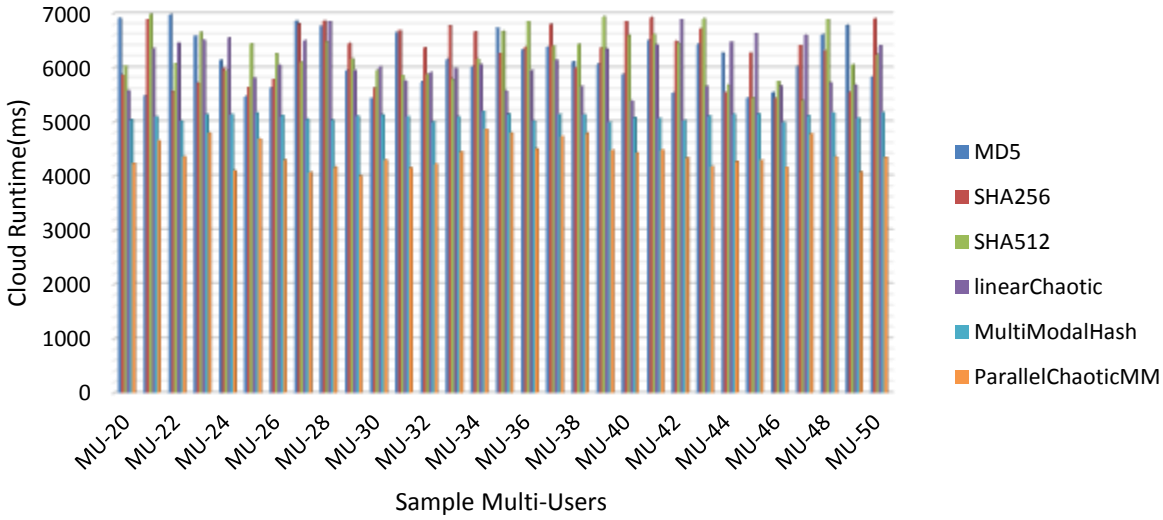

Fig.5: Comparison of proposed integrity algorithm to existing algorithm for multi-modal biometric (Hash size=2048 bits)

Table 4, describes the comparative analysis of filter-based CNN framework to the conventional CNN networks on the large data. From this table we can observe that the present technique exhibits high feature classification accuracy than the conventional models on large image database.

Figure 6, describes the performance comparison of implemented multi-modal framework in terms of runtime(s) of encryption and decryption processes with the traditional models. From this figure, we can observe that the developed model exhibits low average runtime(s) than the existed security models.

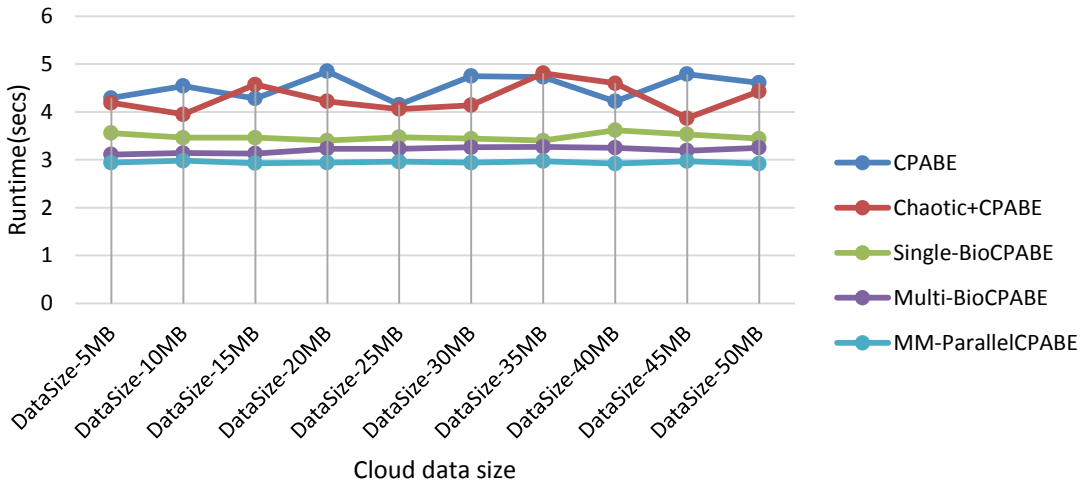

Fig.6: Performance of proposed parallel multi-user based multi-modal encryption model to the traditional integrity-based CP-ABE models for encryption and decryption rumtime(s)

TABLE 3
Comparison of proposed integrity algorithm to existing algorithm for multi-modal biometric (Hash size=4096 bits)

Multi-UserID	MD5	SHA256	SHA512	linear Chaotic	Multi ModalHash	Parallel ChaoticMM
MU-20	112	119	119	116	140	147
MU-21	116	117	124	128	135	149
MU-22	112	119	118	112	137	142
MU-23	119	120	116	125	140	145
MU-24	117	120	118	115	135	147
MU-25	110	116	120	121	135	143
MU-26	119	119	110	129	138	142
MU-27	111	116	112	125	138	149
MU-28	114	115	116	121	136	148
MU-29	118	117	115	118	140	149
MU-30	118	118	122	126	138	149
MU-31	112	116	118	123	136	146
MU-32	114	119	122	113	136	144
MU-33	117	112	113	119	139	146
MU-34	119	116	124	115	140	149
MU-35	120	117	119	116	139	142
MU-36	118	117	124	130	140	145
MU-37	111	117	123	110	135	144
MU-38	115	113	119	119	138	148
MU-39	112	119	120	118	139	142
MU-40	114	115	115	122	139	142
MU-41	111	114	115	125	138	142
MU-42	110	118	116	122	138	141
MU-43	114	112	111	119	137	144
MU-44	116	120	111	120	138	145
MU-45	114	115	121	124	137	144
MU-46	119	116	113	126	137	148
MU-47	117	118	111	117	135	145
MU-48	117	118	112	111	139	144
MU-49	117	115	116	115	136	148
MU-50	110	113	112	125	136	146

IV. CONCLUSION

For security purpose of large data file frameworks, in this paper multi user multi model security model is proposed. It is tested on cloud servers of both private and public frameworks, testing of cloud security frameworks mostly based on confidentiality and existed integrating methods, these methods are depending on file format and data size of media files. To solve these limitations, in this paper a multi user multi model-based framework is developed for large cloud data media files. For real time cloud database security, biometric images like IRIS and finger knuckle features are used for implementing a strong data security. Parallel chaotic integrity algorithm, CNN based frameworks and decryption techniques are used for improving cloud data security of large data files. Then simulation results show that the implemented framework exhibits better efficiency for larger cloud server data files with regard to true positive rate, integrity bit variation and runtime than exited models.

TABLE 4
Comparative analysis of proposed filter-based CNN framework to the existing frameworks on the large cloud databases.

FeatureSet	PSO+RF+CNN	IG+RF+CNN	PCA+RF+CNN	HFS+SVM+CNN
FeatureSet1	0.89	0.91	0.94	0.99
FeatureSet2	0.88	0.89	0.95	0.99
FeatureSet3	0.86	0.91	0.92	0.99
FeatureSet4	0.87	0.91	0.92	1
FeatureSet5	0.87	0.91	0.95	1
FeatureSet6	0.87	0.89	0.93	0.99
FeatureSet7	0.88	0.9	0.92	1
FeatureSet8	0.88	0.91	0.94	0.98
FeatureSet9	0.86	0.93	0.93	0.99
FeatureSet10	0.88	0.89	0.95	0.98
FeatureSet11	0.88	0.89	0.92	0.99
FeatureSet12	0.87	0.91	0.95	0.99
FeatureSet13	0.89	0.91	0.95	1
FeatureSet14	0.89	0.9	0.92	0.99
FeatureSet15	0.87	0.93	0.91	1
FeatureSet16	0.86	0.9	0.91	0.99
FeatureSet17	0.88	0.91	0.94	0.99
FeatureSet18	0.87	0.89	0.92	0.99
FeatureSet19	0.86	0.91	0.92	0.98
FeatureSet20	0.86	0.9	0.94	0.98

REFERENCES

[1] M. Ali, J. Mohajeri, M.-R. Sadeghi, and X. Liu, "*A fully distributed hierarchical attribute-based encryption scheme*," Theoretical Computer Science, vol. 815, pp. 25–46, May 2020, doi: 10.1016/j.tcs.2020.02.030.

[2] V. K. Arthur Sandor, Y. Lin, X. Li, F. Lin, and S. Zhang, "*Efficient decentralized multi-authority attribute-based encryption for mobile cloud data storage*," Journal of Network and Computer Applications, vol. 129, pp. 25–36, Mar. 2019, doi: 10.1016/j.jnca.2019.01.003.

[3] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "*PHOABE: Securely outsourcing multi-authority attribute-based encryption with policy hidden for cloud assisted IoT*," Computer Networks, vol. 133, pp. 141–156, Mar. 2018, doi: 10.1016/j.comnet.2018.01.036.

[4] Salman M.N., Trinatha Rao P., Ur Rahman M.Z.,*'Adaptive noise cancellers for cardiac signal enhancement for IOT based health care systems*',Journal of Theoretical and Applied Information Technology,vol.95,no.10,PP.2206-2213, 2017.

[5] J. Cui, H. Zhou, Y. Xu, and H. Zhong, "*OOABKS: Online/offline attribute-based encryption for keyword search in mobile cloud,"* Information Sciences, vol. 489, pp. 63–77, Jul. 2019, doi: 10.1016/j.ins.2019.03.043.

[6] K. Dhal, S. C. Rai, and P. K. Pattnaik, "*LIKC: A liberty of encryption and decryption through imploration from K-cloud servers*," Journal of King Saud University - Computer and Information Sciences, Feb. 2020, doi: 10.1016/j.jksuci.2020.01.011.

[7] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "*An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid,"* Journal of Systems Architecture, vol. 98, pp. 165–172, Sep. 2019, doi: 10.1016/j.sysarc.2019.07.005.

[8] Putluri S., Rahman M.Z.U., Fathima S.Y.,*"Computer based genomic sequences analysis using least mean forth adaptive algorithms"*,Journal of Theoretical and Applied Information Technology, vol.95, no.9,PP.2006-2014, 2017.

[9] Q. He, N. Zhang, Y. Wei, and Y. Zhang, *"Lightweight attribute-based encryption scheme for mobile cloud assisted cyber-physical systems*," Computer Networks, vol. 140, pp. 163–173, Jul. 2018, doi: 10.1016/j.comnet.2018.01.038.

[10] Kiran P.S., Komala G., Aneesh C.R.S.D., Rao S.K.,*"Electroencephalogram signal analysis using wavelet transform and statistical signal processing"*,Journal of Advanced Research in Dynamical and Control Systems,vol.9, no.2, 2017.

[11] Prasad K.V., Prasad G.R.K., Kranthiveer D., Sowmya D., Nikesh M., Sailesh T.V.,*'ECG signal acquisition and analysis for portable heart monitoring devices'*,Journal of Advanced Research in Dynamical and Control Systems, vol.9, no.14,PP.1685-1693,2017.

[12] Vidya Sagar Y., Chaitresh K., Baba Eleyas Ahamad S., Tejaswi M.,*"Validation of signals using principal component analysis"*,International Journal of Applied Engineering Research, vol.12, no.1,PP.391-398, 2017.

[13] M. H. Le, V. D. Tran, V. A. Trinh, and V. C. Trinh, "*Compacting ciphertext in multi-channel broadcast encryption and attribute-based encryption*," Theoretical Computer Science, vol. 804, pp. 219–235, Jan. 2020, doi: 10.1016/j.tcs.2019.11.034.

[14] M. Hammad and K. Wang, "*Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network*," Computers & Security, vol. 81, pp. 107–122, Mar. 2019, doi: 10.1016/j.cose.2018.11.003.

[15] M. Hammad, S. Zhang, and K. Wang, "*A novel two-dimensional ECG feature extraction and classification*

algorithm based on convolution neural network for human authentication," Future Generation Computer Systems, vol. 101, pp. 180–196, Dec. 2019, doi: 10.1016/j.future.2019.06.008.

[16] Putluri S., Ur Rahman M.Z., Fathima S.Y., "*Cloud-based adaptive exon prediction for DNA analysis*",Healthcare Technology Letters, vol.5, no.1,PP. 25- 30, 2018.

[17] Salman N.M., Trinatha Rao P., Ur Rahman Z., "*Novel logarithmic reference free adaptive signal enhancers for ECG analysis of wireless cardiac care monitoring systems*",IEEE Access, vol.6,PP. 46382- 46395,2018.

[18] Rao G.A., Syamala K., Kishore P.V.V., Sastry A.S.C.S., "*Deep convolutional neural networks for sign language recognition*", Conference on Signal Processing and Communication Engineering Systems, SPACES 2018, PP. 194- 197,2018.

[19] Kumar E.K., Sastry A.S.C.S., Kishore P.V.V., Kumar M.T.K., Kumar D.A., "*Training CNNs for 3-D Sign Language Recognition with Color Texture Coded Joint Angular Displacement Maps*",IEEE Signal Processing Letters, vol.25, no.5,PP. 645- 649,2018.

[20] Cheerla S., Venkata Ratnam D., Teja Sri K.S., Sahithi P.S., Sowdamini G., "*Neural network based indoor localization using Wi-Fi received signal strength*",Journal of Advanced Research in Dynamical and Control Systems, vol.10,no.4,PP. 374- 379,2018.

[21] Babu Sree Harsha P., Venkata Ratnam D., "*Fuzzy logic-based adaptive extended kalman filter algorithm for GNSS receivers*", Defence Science Journal, vol.68,no.6,PP. 560-565, 2018.

[22] Gayathri N.B., Thumbur G., Rajesh Kumar P., Rahman M.Z.U., Reddy P.V., Lay-Ekuakille A., "*Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks*", IEEE Internet of Things Journal, vol.6,no.5, PP.9064-9075,2019.

[23] Tarannum A., Rahman M.D., "*Multi-modal biometric system using Iris, Face and fingerprint images for high-security application*", International Journal of Recent Technology and Engineering, vol.7, no.6, PP.314-320,2019.

[24] Ahammad S.K.H., Rajesh V., Ur Rahman M.Z., "*Fast and Accurate Feature Extraction-Based Segmentation Framework for Spinal Cord Injury Severity Classification*", IEEE Access, vol.7, PP.46092-46103,2019.

[25] Thumbur G., Gayathri N.B., Vasudeva Reddy P., Zia Ur Rahman M.D., Lay-Ekuakille A., "*Efficient pairing-free identity-based ADS-B authentication scheme with batch verification*", IEEE Transactions on Aerospace and Electronic Systems, vol.55, no.5, PP.2473-2486,2019.

[26] Suresh B., Manorama M., Bhupesh M.M., Sai Kiran K., Chandra Sekhar Yadav G.V.P., Ghali V.S., "*Advanced signal processing approaches for quadratic frequency modulated thermal wave imaging"*, International Journal of Emerging Trends in Engineering Research, vol.7, no.11, PP.599-603, 2019.

[27] Srivani I., Siva Vara Prasad G., Venkata Ratnam D., "*A Deep Learning-Based Approach to Forecast Ionospheric Delays for GPS Signals*", IEEE Geoscience and Remote Sensing Letters, vol.16, no.8, PP.1180-1184,2019.

[28] Narayana V.V., Ahammad S.H., Chandu B.V., Rupesh G., Naidu G.A., Gopal G.P., "*Estimation of quality and intelligibility of a speech signal with varying forms of additive noise*", International Journal of Emerging Trends in Engineering Research, vol.7, no.11, PP.430-433, 2019.