IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Survey Analysis of Various Data Security Algorithms for Enhanced Cipher Logics

[1] M. Baskar, [2] S. Naganandini Sujatha

[1] Research Scholar, [2] Assistant Professor
[1]Dept of Computer Application, [2]Dept of Computer Application,
[1]Madurai Kamaraj University Madurai, Tamil Nadu, India,
[2]Sri Meenakshi Govt Arts College for Women(A) Madurai, Tamil Nadu, India

Abstract : In the era of Information and Communication Technology, there has been enormous data transfer across various platforms. In real time business analytics, the assortment of data on every granular level becomes inevitable. All state of art current software store and process massive volume of data in the real time applications. In such enormous data communication, it becomes inevitable to secure the data against swelling intimidations of breaches and leakage. The data protection against external intruders and internal malwares can be effectively incorporated using various cipher strategic frameworks and algorithms with enhanced cipher logics. In the paper, the contemporary data security scenario using the innovative and efficient security frameworks and cipher algorithms are discussed. Analysis carry-out is processed for the selective deep learning algorithms with the compatible features and limitations. Also, the comparison of various methods of frameworks to provide improved protection against hackers and intruders along with their algorithm techniques are presented to resolve the current and future security concerns.

Keywords: Big Data, Cipher encryption, Data Security, Security Frameworks, Survey Analysis

I. INTRODUCTION

Data communication over internet is established through various set of physical elements and devices which are interconnected to each other to afford communication among themselves and to the client-side users. Such a group may be connected in a cloud environment or arranged through Internet of Things. They are used for remote monitoring and control by the server-side users. In the last decade, the progress of cloud computing devices is exponential and it has found its way in various walks of life including traffic control, health care, navigation, smart home etc. Cloud computing and IoT have been identified as imminent technologies for the next decade. The physical devices furnished with sensors collect various data on a real time basis and send them for monitoring and decision-making process in a centralized server location through internet. These technologies can empower up-to-date information processing which progress life excellence and have the competence to gather, enumerate and comprehend the adjacent situations. This condition streamlines the new-fangled communication procedures amid elements and people and therefore authorizes the comprehension of smart cities. IoT and Cloud computing are the dynamically incipient domains in the computing technologies.

In such communication, the volume of data transfer is huge and there needs to be efficient mechanisms to process them in a dynamic manner. Such a gigantic volume of data processed is called as Big data. By using innovative Hadoop processing using parallelization and distributed hardware setup, the requirements can be fulfilled. Big data encompasses together existing and innovative knowledge repositories to analyze enormous data within an adequate time limit and to come up with intuitions of working of the business analytics.

For most of the threats and attacks, the data security frameworks and algorithms can logically provide a suitable solution to monitor IoT devices as shown in Fig 1. To observe the normal and attack behavior of the IoT devices, their interaction with the other devices in the environment can be considered. The contribution information of every fragment of the IoT scheme can be composed and examined to regulate regular forms of collaboration, thus categorizing malicious comportment at initial phases. Also, data security algorithms can be imperative in foreseeing new-fangled attacks, which are repeated transmutations of earlier attacks [1]. These algorithms can perceptively envisage imminent unidentified attacks by learning from prevailing instances. Accordingly, IoT schemes should have an evolution from simply enabling secure communication between devices to intelligence based secure transactions enabled by cipher encryption algorithms for operative and protected schemes.

Data security is fetching piercing attention in information and communication technology domain with varied computing facilities. For high profile business and research transactions, it becomes vivacious requirement [2]. Launching distinctiveness and security in the data processing is mandate in today's interconnected communications. Therefore, the necessity for dependable user

authentication practices has awakened of intense apprehensions about security and swift progressions in ICT domain. Contemporary cipher encryption frameworks are required to be established for competent data encryption for numerous comprehensive procedures for data transfer submissions over internet [3]. For establishing cipher encryption over the digital transmission mechanism, implementation of novel and hybrid cryptographic systems can be trust worthy.

Biomedical waste management defines waste management as the practices & procedures or the administration of activities that provide for the collection, source separation, storage, transportation, transfer, processing, treatment & disposal of waste. Biomedical waste management is a routine procedure of hospital administration as prescribed by law. Hospital waste , hospital acquired infection , transfusion transmitted diseases, rising incidence of hepatitis B, HIV & Other diseases, create potential threat of infection, contamination & serious health hazards to doctors, nurses, ward boys, support staff, sanitation workers, rag pickers & other health care workers. Who are regularly exposed to biomedical waste as an occupation hazards as well as general public in the surrounding area.

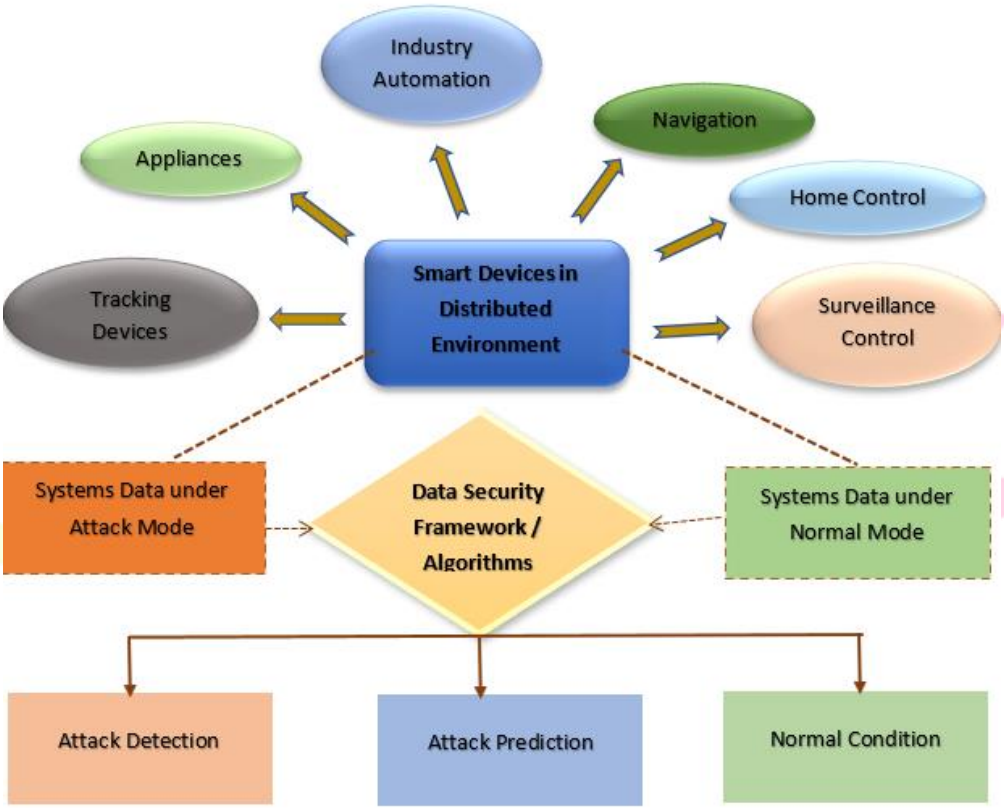

Fig 1: Role of Data Security Algorithms in Distributed Environment

II. RELATED WORKS

The development of advanced technologies can offer innovative paths for enrichment in diversified fields. Especially, the inclusion of computing and advanced cryptographic processes in machine learning, data science, biometric process and information security systems lead to swift and secured data communication in real time applications [4]. Researchers expanded the facility to illuminate data from a particular innovative computing system with the support of knowledge expertise. There are lot of exertions to establish a ciphering mechanism with genetic algorithm and encryption process. In this work, the unique way of encryption process combining data security and viability for real-world submissions.

Guaranteeing the confidentiality of digital information hoarded on computer schemes and the data communicated over the network or other web is presented in [5]. Implementation of symmetric encryption process using the feistel cipher is analyzed in the work. This is helpful in enhancing the security of the systems. In this method, a random number of block scope, repetitions, and dissimilar keys for respective blocks are created automatically. Two-fold or three-way encryption with dissimilar keys are used in the schematic for added security measure.
The process of reversible data hiding for substantiate encryption framework is proposed [6]. Encryption process is implemented using A-S algorithm with the support of dual key system, one for data hiding and another one for data encryption. In the date entrenching segment, data insertion is put in cover and encryption is implemented. At the receiver end, the user receives the key and decryption is done. The proposed algorithm ensures determined secrecy during the data encryption and data hiding processes. The Boolean expression and functionalities applied in the system framework is the robust function gratifying each and every cryptographic measure in the domain.

The essential task of cataloguing on a restricted quantity of training data models is measured for physical schemes with identified parametric system models. Hybrid classification model based on learning classifiers and statistical prototype measures is presented in [7]. In the hybrid framework, the existing suboptimal statistical procedures are estimated as first step and the physical schemes based statistical models are implemented as next step. Further, the data model samples are merged with the simulated data in a

learning-based classifier mechanism in a neural network environment. From the training data, the mapping is formed by the classifier to discourse the problem of disparity and common feature parameter space is simulated. At the same time, the classifier is accomplished to discover discriminatory parameters inside the space to accomplish the classification feature.

In the classification models, there is a popular concept called block cipher cryptography in which only one secret key is practiced for both encryption and decryption processes. Ciphertext is produced after various iterations of key reliant changes. Security assessment of light weighted block cipher key framework using active s-boxes is presented [8]. In the work, the competence of rectilinear and nonlinear machine learning classifiers in establishing security in block cipher framework is studied. Using number of active s-boxes, the particular block cipher parameter is classified as either secure or not secure by incorporating classification algorithms. Unlike most of the existing models, the work is not particular to a specific block cipher or a secret key. Rather, it is based on the concept of active s-boxes to envisage the security level of block cipher.

Distribution of data across various sources for combined cloud computing in IoT systems using privacy preserving is presented in [9]. With the implementation of latest expertise frameworks in IoT, the data user has been responsible for both generating and utilizing big data. In such scenario, implementation of collaborative cloud computing becomes functional. With deep learning mechanisms and neural network algorithms, the privacy preserving and security compatibilities are addressed in an efficient way. Distribution of data and argumentative training sample procedures are introduced in the work. Using the framework, solution for time complexity problem and confrontation training methods are improvised.

Issues related to confidentiality and integrity of the big data environments and the various security measures are presented in [10]. The protection of big data against illegal admittance, exploitation and accessibility preservation are the prime priorities with respect to data security. Effective usage virtual cloud environments and remote storage architectures are presented for information security necessities. Implementation of entity-based framework and advanced data privacy and integrity algorithms for threat desecration are framed for better data security establishments.

Based on the broader study of the related literature, the classification of the data security implementation algorithms can be done based on following categories:

1. Security threats
2. Learning methods of security
3. System architecture
4. Layer mechanisms
5.Threat issues and environment.

The cloud environment system and the data transferred through it are vulnerable to various security loopholes. The tampering can happen either from inside attacks or from outside attacks. So the security algorithms can be designed based on the requirements from threat mechanisms, learning methods, system design architecture, layer mechanisms involved and the nature of threat issues and the physical and virtual environment.

III. ANALYSIS CARRYOUT

As mentioned in the literature review, there have been various researches conducted on the data security mechanisms in the cloud environment. These mechanisms have provided an applied reference for the contemporary security susceptibilities of the cloud-based environment and roadmap for future research works. The main take outs of the existing algorithms and the necessity for improvising the existing works with novel and innovative security algorithms and frameworks overcoming the shortcoming of the existing algorithms are presented in this section.

1.In the schemes using common division and genetic algorithms, the scheme is consistent for currently prevailing unconventional computing methodical and stimulating issues for program-based submissions. However, the systems are not established for high level crypto processes.

2.The usage of genetic random number functions for scheming the suitability levels appropriate for valuation and assessment measures are to be incorporated for better security analysis.
3.The symmetric encryption mechanisms studied are useful in low scale environment for safeguarding the concealment of the digital data transferred over cloud environment. Though the complexity of the scheme is fast, the concept of meta data blocking and symmetric key generation and addressee public key generation are not available.

4. Defining the boundaries of the series to engender the block scope based on the simple text extent is one the primary challenge in overcoming the issue. New mechanisms to implement meta data blocking in symmetric key encryption is the need of the hour in the particular research domain.

5. In the process of reverse data hiding, substantiated encryption schemes are studied. However, the usage of reverse data hiding process incorporated with learning mechanisms is not studied. So, the research based on data hiding process combined with deep and machine learning algorithms to be explored further in data security domain.

IV. FORMULATION OF THE PROBLEM

The data processing and monitoring is pragmatic in innumerable fields including business analytics, economics, research analysis, surveillance, navigation etc. It empowers establishments to repossess and analyze huge volumes of valuable information and to

attain a profounder and more inclusive expertise and helpful in making effective decision-making process [10]. Data processing machines integrate the server-side configuration to the real-world clients in order to provide an intellectual communication between the physical world and its environments. Generally, such strategies are imparted in assorted settings to achieve dissimilar goals. Nevertheless, their procedures should encounter a wide-ranging security prerequisite in virtual and real-world scenarios. For establishing such security mechanisms, the following parameters are to be ensured.

Confidentiality: Defense against the expose of information is called as Data Confidentiality. This is achieved by guaranteeing that the data is restricted only to authorized personals. The semantics endure to be available for critical information access holders.

Integrity: The process of ensuring the precision, comprehensiveness, uniformity and validity of the data processed is called as the concept of data integrity. The process guarantees the accuracy and the correctness of the data across multiple platforms.

Availability: The obtainability of information to the legitimate users under various scenarios is called as data availability. Whenever the data is required by the user, it is made available without any complications.

For an operative IoT security system, the security parameters mentioned above has to be fulfilled along with the security framework measures: Authentication, Authorization and Accounting (AAA). AAA control admittance to data resources, imposes guidelines and inspections procedures. AAA deployments play a prime part in network architecture and web security by filtering clients and monitoring the procedures during the connection establishments. Though, these features can be oppressed by various security threats, as shown in Fig 2. In the pictorial representation, potential data security threats are elaborated which is required for understanding how the security frameworks need to be developed. To overcome the security threats there need to be efficient and innovative security frameworks and algorithms to establish a secured data processing environment.

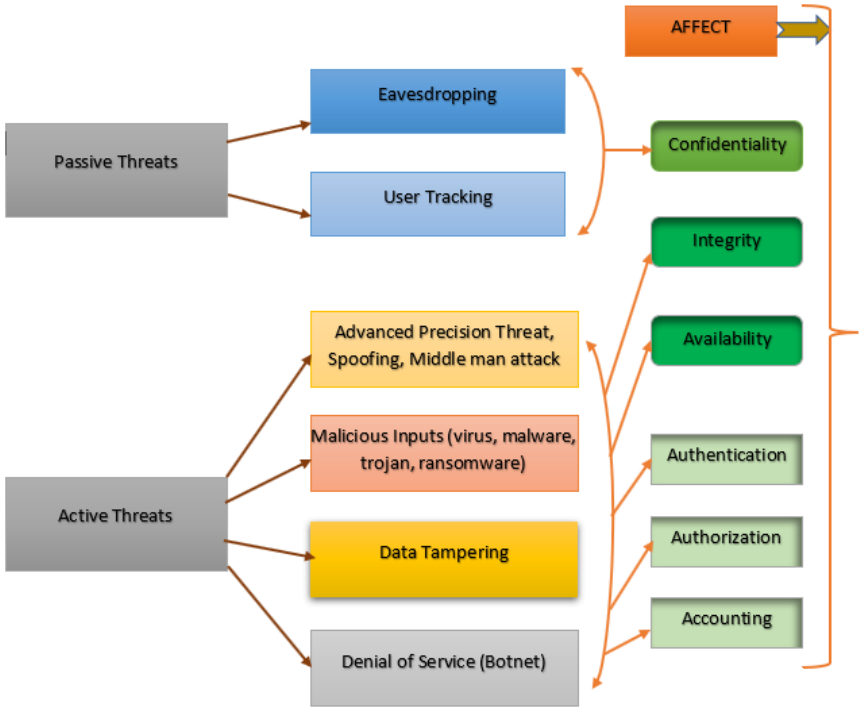

Fig 2: Potential Security Threats in Data Processing

V. REVIEW OF DATA SECURITY ALGORITHMS

There are various deep learning algorithms which could form the based of establishing a secured architectural framework in IoT systems. In deep learning procedures, there are four types of algorithms presented under each procedure. They are supervised, unsupervised, partially supervised and reinforcement learning approaches. The implementation of such algorithms in the IoT environment and their functionalities in establishing a secured data framework are explained in this section.

In current research environment, the submissions of deep leaning algorithms in secured data processing systems have turned out to be an imperious research topic. The primary benefit of implementing deep learning algorithms over traditional machine learning algorithms is because of its better executions in huge volume of large datasets. Also, deep learning algorithms can inevitably extract compound depictions from the information presented.

Convolutional Neural Networks (CNN): CNN is a part of supervised deep learning algorithm type in which the data structures are considerably reduced when compared to artificial neural networks. The reduction of data structures is achieved by means of spare communication, constraint distribution and equivariant illustration [11]. There are two types of sporadic levels available in CNN, they are convolutional level and pooling level. Equal sized multiple filters are available in convolutional level which sophisticate the data. Down-sampling to reduce the size of the data is implemented in pooling level. Studies have revealed that CNN algorithm can be successfully designed for cryptographic applications [17].

Working Principal of CNN: The working principle of convolution neural networks is based on two alternating types of layers; they are convolutional layer and pooling layer. The convolutional layers sophisticate statistics features using numerous kernels of identical scope. The pooling layer accomplish down-sampling to reduce the block scope of the succeeding layers by means of maximum or mean pooling. Feature extraction is carried out in processing segment containing above layers. Classification is performed in the subsequent active segment containing output layer. Classification is executed based on detection of attacks, prediction of attacks and normal data transfer scenario. The working demonstration of convolution neural networks is illustrated in Fig 3.

Recurrent Neural Networks (RNN): RNN is also a part of supervised deep learning algorithm type which is used handling sequential data. The analysis and forecasting of the future outputs are based on the repetitive iterations of the past and current data for which back propagation based RNN is accessible and trustworthy [12]. RNN merges a time-based level to seize sequential data and then acquires complex disparities by means of the secreted elements of the persistent unit. The secreted units are adapted in accordance with the data accessible to the network. Such processed data is recurrently restructured to disclose the current state of the network [18]. Recurrent neural network is the one with multiple layers of data processing. It is the deeper network with input layer and multiple hidden layers in between and output layer. Individual hidden layer has its respective weights (x) and biases (y). Each layer is self-governing and not dependent on other layer outputs. RNN changes the self-governing instigations into reliant initiations by delivering the identical weights and biases to entire layers. It decreases the complication of cumulative constraints and remembering each preceding outputs by providing respective output as input to the following hidden layer. So, these multiple layers can be combined so the cumulative weights and bias of total hidden layers is the equivalent and represented as single recurrent layer. The computation of RNN is illustrated in Fig 4.

Unsupervised Deep Learning Algorithms: In unsupervised frameworks, the deep autoencoders (DAE) and deep belief networks (DBN) are effectively functional. DAE has the mechanism of reproducing input to the output format. The learning and training procedures in DAE are designed for accomplishment of least rebuilding error. Nevertheless, DAE replication of input to output ratio is not perfect [13]. In DBN, the learning and training procedures are implemented layer wise. Here, greedy layer approach is used for malicious communication detection. The representation of deep belief networks is based on the initialization of training vector as noticeable elements and update the hidden elements in parallel fashion as noticeable elements using Sigmond function. Then the updated noticeable elements are convoluted as reconstruction and performed as weighted update. The training method is explained using gradient descent with equational solutions.

Generative Adversarial Network (GAN): GAN is a part of hybrid deep learning network in which both the generative and discriminative models can be trained in union under the structured framework. The prime aim of the learning and training process in the generative model is to upsurge the possibility of misclassification by the discriminative model samples [14]. GAN uses single pass for generating a sample in a rapid manner, making it better than other sequential models [19].

Ensemble of Deep Learning Network (EDLN): Multiple deep learning algorithms can collaboratively perform by combining generative, distributed and hybrid models to form ensemble of deep learning network. EDLN encompasses loaded distinct classifiers, either from similar or dissimilar group. It has enhancement in terms of multiplicity, accurateness, routine and generalization [15].

The GAN model construction includes two sub component models, one, generator model and the next one discriminator model. Generator model is used for engendering innovative samples for the delinquent domain. Discriminator model is used for classification purposes. The illustration of GAN model flowcharts is shown in Fig 5.

Deep Reinforcement Learning (DRL): DRL is implemented by successfully allowing learning and training framework tool to regulate their strategies and descend an optimum result through multiple iterations. It is used to achieve the optimum long-term purpose without knowing about the previous training patterns of the architecture [16] [20]. For establishing cyber security, the cross functional implementation of DRL across various deep learning combinations can be explored.

Deep Reinforcement Learning algorithm is the best means for handling unstructured situations. They can learn from huge volumes of information or determine designs and patterns resolving recognition problem. DRL is dignified to reform Artificial Intelligence domain and epitomizes a phase towards developing independent schemes with an innovative level of recognition pattern in the pictorial world. DRL can scale solution for multiple glitches that were formerly obdurate, such as training to play carious video games directly from pixel representation. The training process of DRL includes update, play and store procedures. Behavior policy is updated from the existing network. The new data is stored in the replay memory and then fed to the frozen memory. The existing network date which is sent to frozen memory is transformed with replay memory data through multiple iterations. Finally, the data is fed to target policy and loss function and then the entire process is repeated. The Training process of DRL is shown in Fig 6.

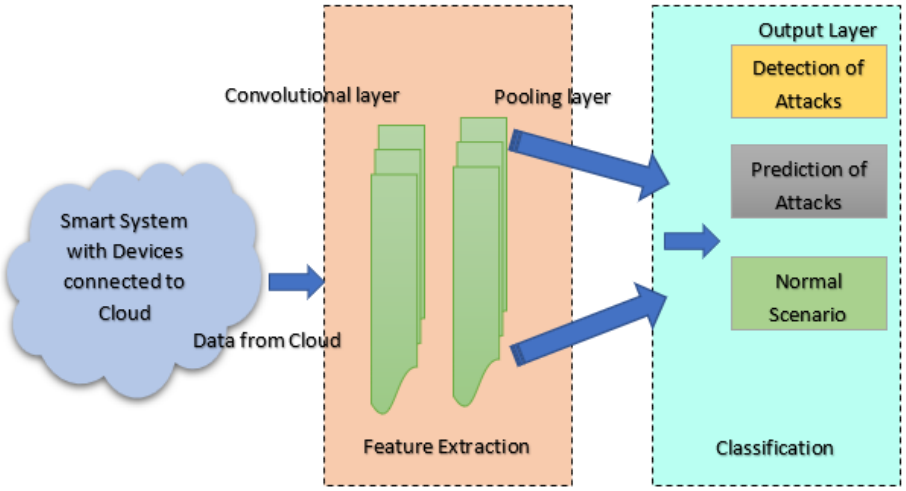

Fig 3: Demonstration of Convolution Neural Network

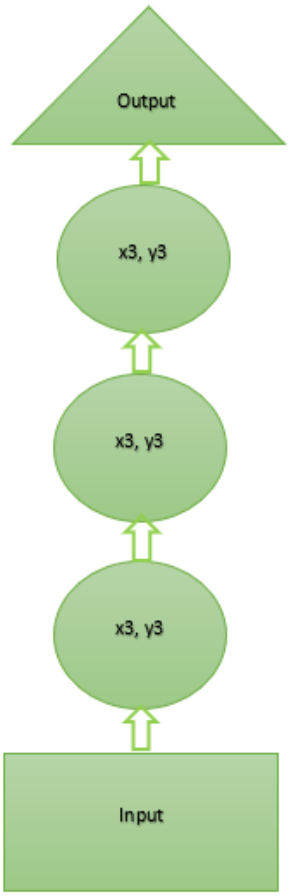

Fig 4: Computation of Recurrent Neural Network

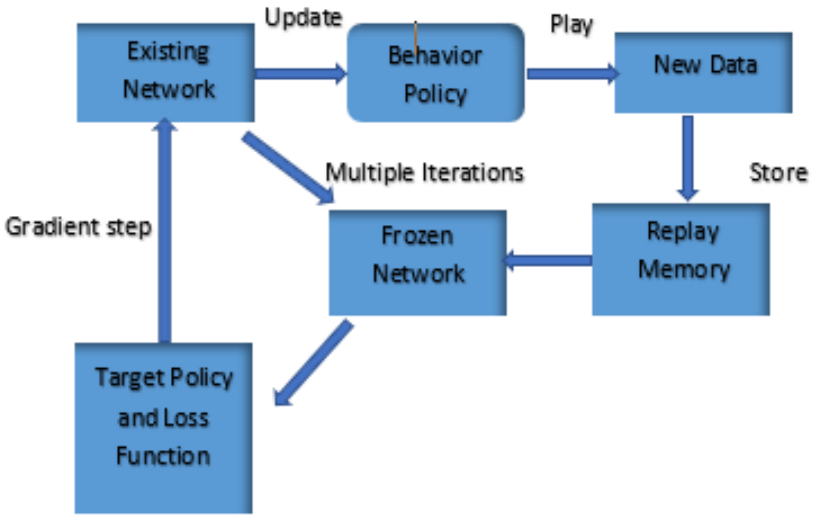

Fig 5: Training Process of Deep Reinforcement Learning algorithm

Table 1: Data Security Algorithms – Classification and Comparison

Algorithms	Algorithm Techniques	Functionalities	Pros	Cons	Real-Time Applications
Convolutional Neural Network	Usage of back propagation algorithm for learnable weights and basis. Implementation of multiple building blocks in convolution and pooling layers.	Minimize data features by implementing sparse exchanges, structure distribution and equivariant allocations	Robust with superior viable performance, increased scalability and complexity	Heavy computational cost, limitation of resources	Exposure of malware
Recurring Neural Network	Speech recognition and natural linguistic dispensation. Sequential data processing techniques are used. Previous information evidence with looped architecture is used in implementation.	Combine temporal level to input consecutive data and train with hidden block	Suitable for sequential data	Problem of disappearing or discharge variables	High accuracy malware detection
Deep Auto Encoders and Deep Belief Networks	Clustering mechanism is implemented in unsupervised learning principles for compress and encode data processing. Restricted Boltzmann Machines with unsupervised corrections is used.	Works on the principle of unsupervised learning, with hidden or stacked measure of data encryption	Useful for feature extraction with unlabeled data iterations	Consume substantial computational time, complicate the training and learning processes.	Detection of generalized malware attacks
Generative Adversarial Network	Usage of generative and classification principles with adversarial mechanism for artificial intelligence domain implementation. Modelling of data in generation and discrimination process is implemented in the algorithm.	Training of two model frameworks simultaneously. Learning based on data distribution	One pass sample generation with reduced iterations	Unstable and complex process to achieve.	Establishing secured cyberspace architecture
Ensemble of Deep Learning Network	Adjustment of prediction and lessening in generalization error mechanism is used. Fitting of decision trees (Bagging), fitting different models (Stacking) and ensemble member sequential processing (Boosting) is involved.	Merger of multiple hybrid models with generative and discriminative algorithms	High model diversity, better performance and expansion of generalization	Increased time complexity	Building classifier model in distributed setting

Deep Reinforcement Learning	Policy learning in forward dynamics is implemented. Model predictive control with divergence in agent replanning, temporal learning and q-learning principles are used.	Trial and error process with training and learning agents for policy adjustment	Suitable for adversarial framework structure with optimal solution	Needs multiple assumption process in real-time implementation	Distributed Denial of Services and Brute force attack handling

VI. CONCLUSION AND DIRECTIONS FOR FUTURE RESEARCH

The necessities for safeguarding Cloud and IoT applications with server and multiple client technologies have become multifaceted. From wired to wireless, mobile and cloud deployments, there need to be a reliable and efficient communication process. The progression of hybrid deep learning algorithms with cryptographic functionalities is paving way for considerable authoritative systematic approaches which can augment data security. In the current work, multi-dimensional security threat factors and the wide-ranging assessment of the possible deep learning measures along with their, pros and cons and also their application in real-time frameworks for data security is studied. Also, the comparative analyses in the tabulation formats are presented. This will be helpful in understanding the data security concerns in the ICT domain and providing a research solution for remote server data security based on the hybrid cipher strategy with enhanced cipher logics. The paper focused on the various approaches which will lay foundation for establishing a novel framework to provide an efficient data protection technique to clients to preserve the data securely over the server environment and to introduce new hybrid cryptography logic by combining the powerful and robust cryptographic schemes derived from Conventional Neural Network based algorithms. This will pay way to provide in-depth analysis and implementation of novel hybrid security algorithms for the real-time versatile applications.

REFERENCES

[1] Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I. and Guizani, M., 2020. A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), pp.1646-1685.

[2] Vaidya, G.M. and Kshirsagar, M.M., 2020, May. A Survey of Algorithms, Technologies and Issues in Big Data Analytics and Applications. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 347-350). IEEE.

[3] Patel, N.A., 2018, December. A survey on security techniques used for confidentiality in cloud computing. In 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET) (pp. 1-6). IEEE.

[4] Aparna, G., Rao, G.V.R. and Vasavi, G., 2016, February. Computationally efficient ciphering scheme for image encryption using common division and genetic algorithm. In 2016 IEEE 6th International Conference on Advanced Computing (IACC) (pp. 304-307). IEEE.

[5] Baker, S.I.B. and Al-Hamami, A.H., 2017, October. Novel algorithm in symmetric encryption (NASE): Based on feistel cipher. In 2017 international conference on new trends in computing sciences (ICTCS) (pp. 191-196). IEEE.

[6] Dhande, K. and Channe, R., 2019, April. A Brief Review on Reversible Data Hiding in Encrypted Image. In 2019 International Conference on Communication and Signal Processing (ICCSP) (pp. 0135-0138). IEEE.

[7] Nooraiepour, A., Bajwa, W.U. and Mandayam, N.B., 2021. A hybrid model-based and learning-based approach for classification using limited number of training samples. IEEE Open Journal of Signal Processing, 3, pp.49-70.

[8] Lee, T.R., Teh, J.S., Jamil, N., Yan, J.L.S. and Chen, J., 2021. Lightweight Block Cipher Security Evaluation Based on Machine Learning Classifiers and Active S-Boxes. IEEE Access, 9, pp.134052-134064.

[9] Zhang, P., Wang, Y., Kumar, N., Jiang, C. and Shi, G., 2021. A Security-and Privacy-Preserving Approach Based on Data Disturbance for Collaborative Edge Computing in Social IoT Systems. IEEE Transactions on Computational Social Systems, 9(1), pp.97-108.

[10] Miloslavskaya, N. and Makhmudova, A., 2016, August. Survey of big data information security. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 133-138). IEEE.

[11] Chen, X.W. and Lin, X., 2014. Big data deep learning: challenges and perspectives. IEEE access, 2, pp.514-525.

[12] Hermans, M. and Schrauwen, B., 2013. Training and analysing deep recurrent neural networks. Advances in neural information processing systems, 26.

[13] Mohammadi, M., Al-Fuqaha, A., Sorour, S. and Guizani, M., 2018. Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials, 20(4), pp.2923-2960.

[14] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. and Bengio, Y., 2014. Generative adversarial nets. Advances in neural information processing systems, 27.

[15] Kuncheva, L.I., 2014. Combining pattern classifiers: methods and algorithms. John Wiley & Sons.

[16] Comșa, I.S., Zhang, S., Aydin, M.E., Kuonen, P., Lu, Y., Trestian, R. and Ghinea, G., 2018. Towards 5G: A reinforcement learning-based scheduling solution for data traffic management. IEEE Transactions on Network and Service Management, 15(4), pp.1661-1675.

[17] McLaughlin, N., Martinez del Rincon, J., Kang, B., Yerima, S., Miller, P., Sezer, S., Safaei, Y., Trickel, E., Zhao, Z., Doupé, A. and Joon Ahn, G., 2017, March. Deep android malware detection. In Proceedings of the seventh ACM on conference on data and application security and privacy (pp. 301-308).

[18] Pascanu, R., Mikolov, T. and Bengio, Y., 2013, May. On the difficulty of training recurrent neural networks. In International conference on machine learning (pp. 1310-1318). PMLR.

[19] Salimans, T., Goodfellow, I., Zaremba, W., Cheung, V., Radford, A. and Chen, X., 2016. Improved techniques for training gans. Advances in neural information processing systems, 29.

[20] Mankowitz, D.J., Dulac-Arnold, G. and Hester, T., 2019. Challenges of real-world reinforcement learning.