Performance Enhancement and Security using Artificial Intelligence and Blockchain in Cloud Computing

Y. Kiran Kumar[1], Dr. R. Mahammad Shafi[2]

[1]*Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, T.N., INDIA.*
E-mail: ykkumar83@gmail.com
[2]*Research Supervisor, Department of Computer Science, Bharathiar University, Coimbatore, T.N., INDIA.*
E-mail: rmdshafi@gmail.com

***Abstract*— Due to the huge use of data made available in cloud computing, cloud computing challenged with issues of security on demand application resource management and self-monitoring without latency. This paper explores how Artificial Intelligence and machine learning can play a key role in enhancing the capabilities of security and privacy in cloud storage. Integrating machine learning techniques into the existing cloud can therefore offer improved effectiveness. We discuss the concept of blockchain technology and its burning research trends. In addition, we will study how to adapt blockchain security to cloud computing and its secure solutions in detail. An Artificial Neural Network (ANN) is a promising technique to improve the performance of Modified RSA cryptography algorithm, In this paper we explore the implementation of Modified RSA cryptography algorithm using ANN to reduce the execution time. This paper provides a fair comparison between RSA, Modified RSA and ANN RSA.**

***Keywords*— Cloud Computing, Artificial Intelligence, Blockchain Technology, RSA, Artificial Neural Network, Cryptography, Information and Communication Technology.**

I. INTRODUCTION

As we explore deeper into the Digital Era, we observe an unstable growth in the volume, velocity, and variety of data available on the Internet. For example, in 2012, about 2.5 quintillion bytes of data were created each day. The data created from multiple types of sources, including mobile devices, sensors, enterprises, individual archives, social networks, the Internet of Things, cameras, software logs, etc. Such data explosions have raised one of the most challenging research questions of the current Information and Communication Technology (ICT) era: how efficiently and optimally manage such huge amounts of data and identify new ways to analyse them in order to unlock information. Millions of financial transactions realised each day in today's global market generate hundreds of pet bytes of sensitive heterogeneous data, which requires it to be stored, distributed and processed efficiently, in a way that does not compromise end-user's Quality of Service (QoS) in terms of data availability, data privacy and data integrity. Many of the existing ICT systems that store distribute and process of pet bytes of heterogeneous data. So new paradigm are required for executing high-performance large data applications from physical hardware and software-enabled platforms managed locally, which should be processed, analysed and stored in safe ICT environments.

Blockchain technology is not just used for cryptocurrencies but can be used in many other sectors also. Potential use cases are video or audio streaming, cloud storage and much more. Blockchain has revolutionized the Internet. This new and ingenious technology allows blocks of data to be distributed across ledgers, without any central administering authority, but with the essential requirement that the data be validated by participants. This makes the data open and secure. Blockchain technology can be used to great advantage in cloud storage solutions.

A neural network is a parallel distributed processor which is made up of simple processing units. These units have a natural propensity to store the experimental knowledge and making it available for use. Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer technique. Cryptosystems are commonly used for protecting the integrity, confidentiality, and authenticity of information resources. [1]

Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. Other advantages include:

1. Adaptive learning: An ability to learn how to do tasks based on the data given for training or initial experience.
2. Self-Organization: An Artificial Neural Network (ANN) can create its own organization or representation of the Information it receives during learning time.
3. Real Time Operation: ANN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.[2]

Cryptography refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. A cryptosystem is simply an algorithm which converts the input data known as plaintext into something unrecognizable known as cipher text and converts the unrecognizable data back to its original form. [3]

There are two types of cryptosystems; symmetric cryptosystems and asymmetric cryptosystems. Symmetric cryptosystems use the same key for encryption and decryption. On the other hand, asymmetric cryptosystems use two different keys; a public key for encryption and a private key for decryption. [4]

II. ARTIFICIAL INTELLIGENCE FOR CLOUD SECURITY

As we move forward into the future of automation, Artificial Intelligence (AI) is proving to play a critical role in the area of both cyber and cloud security. The ability to learn at the rate which AI produces makes it extremely important to prioritize discovering the potential ways that AI can both assist security, as well as defining ways that standardization can be shaped around its proper uses, ensuring that businesses are prepared for the continued growth of AI. Artificial Intelligence is software that can solve problems and think by itself in a way that's similar to humans. Today, most of the fruitful research and advancements have come from the sub-discipline of AI called machine learning (ML), which focuses on teaching machines to learn by applying algorithms to data. Often, the terms AI and ML are used interchangeably. For a problem to be a candidate for an artificial intelligence/machine learning solution, it must be solvable with data and involve sufficient relevant acquirable data. In addition, sufficiently powerful computing systems must be available to perform the necessary processing within a reasonable time-frame.

Cyber Security systems produce massive amounts of data more than any human team could ever strain through and analyse. Machine learning technologies use all of this data to detect threat events. The more data processed the more patterns it detects and learns which it then uses to spot changes in the normal pattern flow. These changes could be cyber threats. For example, machine learning takes note of what's considered normal, such as from when and where employees log into their systems, what they access regularly, and other traffic patterns and user activities. Deviations from these norms, such as logging in during the early hours of the morning, get flagged. This in turn means that potential threats can be highlighted and dealt with in a faster fashion. By using a more data-driven approach, artificial intelligence can be used to detect and proactively alert on weaknesses and vulnerabilities both that are being exploited right now, or that might be exploited in the future. This works by analysing data coming in and out of protected endpoints, both detecting threats based on known behaviour, and spotting yet known threats based on predictive analytics.

A. Event detection and blocking

When AI and machine learning technologies process the data generated by the systems and find anomalies, they can either alert a human or respond by shutting a specific user out, among other options. By taking these steps, events are often detected and blocked within hours, shutting down the flow of potentially dangerous code into the network and preventing a data leak. This process of examining and relating data across geography in real-time enables businesses to potentially get days of warning and time to take action ahead of security events.

B. Delegating to automated technologies

Alerts about potential threats or anomalies are very common with many security platforms, but there is a lot of potential with automated technologies to eliminate a lot of the noise to be able to focus on the important things. When security teams have AI and machine learning technologies handling routine tasks and first-level security analysis, they are free to focus on more critical or complex threats. This does not mean these technologies can replace human analysts, as cyber attacks often originate from both human and machine efforts and therefore require responses from both humans and machines as well. However, it does allow analysts to prioritise their workload and get their tasks done more efficiently.

Corporations run hundreds, and sometimes even thousands of interconnected applications to support their operations. Traditional solutions store information in many different places, so keeping those systems in sync is a challenging task. Multi-tenancy Software as a Service (SaaS) with human resource, finance and planning data stored in one application makes all of this much easier. This central design has many benefits, including all systems working from a common framework, so there are no inconsistencies in data. It also eradicates the disconnect between the system and its users.

Conversely, it's important to make access control a serious priority. The modern workforce comes paired with all sorts of different hardware, meaning a spread of data across more access points, increasing the likelihood of vulnerability. By prioritising an access solution involving inspection applications used, specifying permissions and setting policies, the correct employees can access the tools they need in order to work efficiently.

C. Machine learning algorithms for cloud computing

With an increasing number of devices connected to the internet, the volume of data generated and processed at greater speed has increased significantly, especially with the demand for action in real-time. With the increasing variety and veracity of data, such processing has become more challenging to achieve within a relevant time-frame. For these scenarios, the existing cloud infrastructure is a sub-optimal solution as the data generated are sent to various distant cloud centres. Integrating machine learning techniques into the existing cloud can therefore offer improved effectiveness.

There is also a very large amount of data stored in the cloud which can act as input for machine learning algorithms. A simple machine learning method such as clustering can organize and group different data together, after which other cognitive and predictive techniques can be used to improve outcomes. Data scientists have recently begun using various Machine Learning and Artificial Intelligence methods in cloud for efficient computing. Examples include Amazon Web Services with Keras, IBM Watson, and Microsoft Cognitive AI. Furthermore, in this era of IoT, Big Data Analytics and Blockchain almost all of the data are processed in the Cloud, and Machine Learning and Artificial Intelligence play a prime role in satisfying the demand for effective and efficient computing.

III. SECURE BLOCKCHAIN SOLUTIONS IN CLOUD COMPUTING

If the user data is disclosed in the cloud computing environment, monetary and psychological damages can occur due to the leak of users' sensitive information. The security of the saving and transmitting data, such as confidentiality and integrity, in the cloud computing environment is mainly studied. Note, however, that studies on privacy protection and anonymity are not sufficient. Blockchain is a representative technology for ensuring anonymity. If combined with the cloud computing environment, blockchain can be upgraded to a convenient service that provides stronger security. User anonymity can be ensured if the blockchain method is used when saving the user information in the cloud computing environment. An electronic wallet is installed when using the blockchain technology. If the electronic wallet is not properly deleted, the user information can be left behind. The remaining user information can be used to guess the user information. To solve this problem, we propose a solution that installs and deletes the electronic wallet securely.

Cases of misrepresenting the ledger or bitcoin and double transactions of blockchain pose the biggest problem. A secure wallet is needed to solve such security problems. Although the electronic wallet installed in the PC is generally used, the security of electronic wallets in mobile devices must be verified as mobile devices have become very popular. Since a transaction occurs based on the time value of a mobile device, the security of a transaction can be confirmed only when both the integrity and accuracy of a time stamp generated in a mobile device are guaranteed. [5]

TABLE I: Comparison of related studies.

	Authentication	Security Incidents	Improved Blockchain	Secure Blockchain
Confidentiality		√	√	√
Integrity	√	√		√
Anonymity	√	√	√	√
Availability	√			√
Privacy Protection	√	√	√	√
Residual Information Protection				√

We compared the method with existing studies in terms of confidentiality, integrity, anonymity, privacy protection, and residual information protection. Confidentiality checks if the information is leaked to unauthorized peers, whereas integrity checks if the data used in transactions are altered or falsified without sanction during transfer or storage. Anonymity must assure that the peer involved in a transaction is not identifiable. Privacy protection protects the personal information of peers participating in the transaction, whereas residual information protection checks the safe removal of user data at the time of transaction termination and program removal. [6]

The authentication case [7] does not provide integrity since it has the problem of leaking the key by hacking the personal key to attack the blockchain. Also, it does not provide residual information protection since it does not verify the complete removal of the electronic wallet. The security incidents case [8] does not provide availability since the service becomes unavailable due to infection by malware and does not provide residual information protection since it does not verify the complete removal of the electronic wallet. The improved blockchain case [9] neither assures integrity nor provides availability since the vulnerability of double transaction remains. Moreover, it does not provide residual information protection since it does not verify the complete removal of the electronic wallet. The secure blockchain solution improves security by providing residual information protection since it encrypts the data using a public key and verifies the complete removal of the electronic wallet.

IV. TYPES OF NEURAL NETWORKS ARCHITECTURES

There are three network architectures:

1. Single Layer feed forward networks – In this layer, the input layer consist of source node that results the output in the form of neuron. It is feed forward type of network.
2. Multilayer feed forward networks – It only adds an extra layer known as hidden layer. Because of this hidden layer higher level of statistic is obtained.
3. Recurrent Network – This network contains at least one feedback loop. In this loop, output of a neuron is fed back into its own input which increases learning capability. And it also increases performance. [10]

V. PROPOSED DESIGN OF MODIFIED RSA ALGRITHM BASED ON ARTIFICIAL NEURAL NETWORKS (ANN)

In this proposed model, it was merged ANN with Modified RSA (MDRSA) In this design we used a neural network called feed forward network, These types of networks are somehow straight forward and associate inputs with outputs. This kind of organization is also referred to as bottom-up or top-down. The learning algorithm used here is the Backpropagation method in feed forward network architecture. The input is plain text that is encrypted by NN- using RSA algorithm and output of NN is Cipher text.

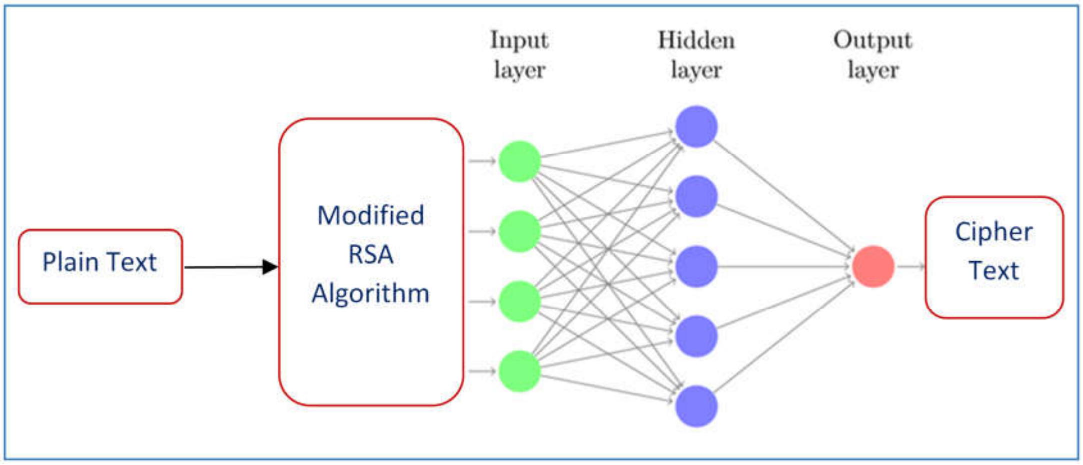

Fig. 1 Proposed Architecture of cryptography based on Neural network

Input layer – It contains those units (Artificial Neurons) which receive input from the outside world on which network will learn, recognize about or otherwise process.
Output layer – It contains units that respond to the information about how it's learned any task.
Hidden layer – These units are in between input and output layers. The job of the hidden layer is to transform the input into something that output unit can use in some way.

VI. RESULTS AND PERFORMANCE ANALYSES

The implementation results reported in this section makes the comparison between the RSA, Modified RSA and AAN RSA. In this paper, RSA, Modified RSA and ANN RSA implementation in the environment of MAT LAB. There are so many restrictions in single layer feed forward network. So we use backpropagation to reduce the errors. The errors for the units of the hidden layer are determined by back-propagating the errors of the units of the output layer. This method is Back propagation learning rule. It can also be considered as generalization of delta rule for multilayer function. [11]

TABLE II: Execution Time of RSA, Modified RSA and ANN RSA algorithms for encryption.

Input File Size (KB)	Time Required for Encryption (Seconds)		
	RSA	MDRSA	ANN RSA
15	5.64	7.58	4.89
30	11.28	13.88	10.48
45	16.92	19.21	15.05
60	22.54	25.97	20.21
75	28.21	31.84	27.29
85	34.89	39.68	33.89
100	40.86	46.96	39.55

Table II shows the execution time required by different size text files for encryption process. Here we reported three types of results. First of all, we show the execution time for different input File size, in RSA implementation. Afterwards, we show the result of MDRSA and ANN RSA implementation for same input plaintext size. [12][13]

TABLE III: Execution Time of RSA, Modified RSA and ANN RSA algorithms for encryption

Input File Size (KB)	Time Required for Decryption (Seconds)		
	RSA	MDRSA	ANN RSA
15	5.64	7.58	4.89
30	11.28	13.88	10.48
45	16.92	19.21	15.05
60	22.54	25.97	20.21
75	28.21	31.84	27.29
85	34.89	39.68	33.89
100	40.86	46.96	39.55

Table III shows the execution time required by different size text files for decryption process. Here we reported three types of results. First of all, we show the execution time for different input File size, in RSA implementation. Afterwards, we show the result of MDRSA and ANN RSA implementation for same input plaintext size.

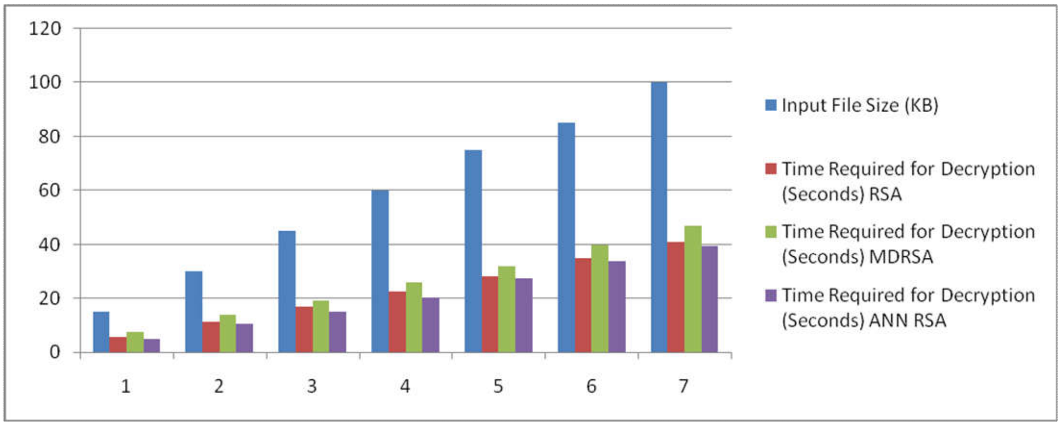

Fig. 2 Graphical representation of time for encryption process in RSA, MDRSA and ANN RSA implementation

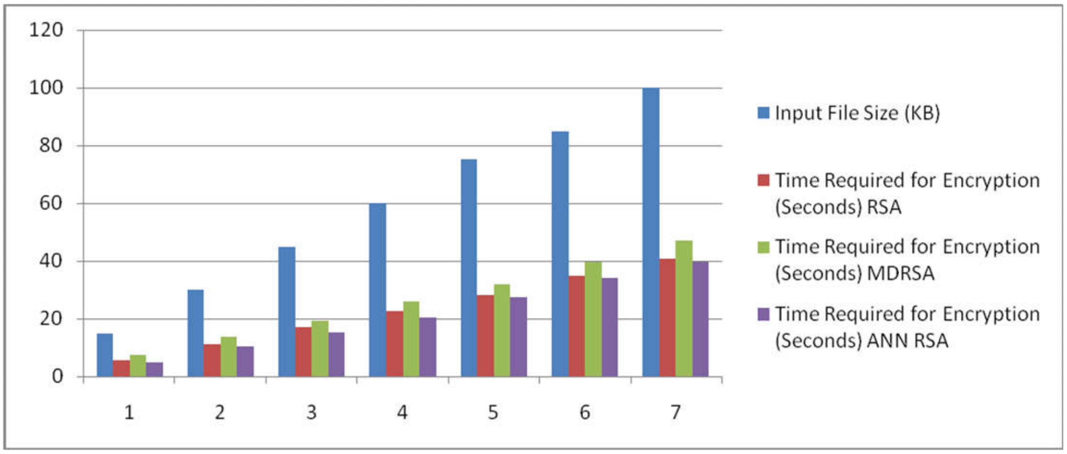

Fig. 3 Graphical representation of time for decryption process in RSA, MDRSA and ANN RSA implementation

Figure 2 and 3 shows graphical representation of time for encryption and decryption process respectively. In this graph blue column shows the input file size in KB for RSA, MDRSA and ANN RSA implementation, the red column shows the encryption and decryption time for RSA, the green column shows the encryption and decryption time for MDRSA and the purple column shows the encryption and decryption time for ANN RSA implementation. Graph shows the difference in execution time for RSA, MDRSA and ANN RSA implementation for encryption and decryption process [14]. Here we can see the performance improvement in the ANN RSA implementation compare to both RSA and MDRSA.

VII. CONCLUSIONS

In this paper, we have designed and implemented of Modified RSA algorithm by using An Artificial Neural Network (ANN), we provided an extensive quantitative evaluation of execution time for both Modified RSA and ANN RSA implementation. After evaluation of execution time, we reported that ANN implementation of RSA takes less time for performing the encryption and decryption than the both RSA and Modified RSA implementation. Overall, we can conclude that An Artificial Neural Network (ANN) provide an efficient and reliable way to implement RSA, MDRSA and ANN RSA cryptography algorithms. In this study, we also discussed the blockchain technology and related core technologies and surveyed the trend of areas. In addition to that identify the current issues should be taken into account to use blockchain in the cloud computing environment. Blockchain gives rise to many problems even now, such as the security of transactions, wallet, and software and various studies have been conducted to solve these issues.

REFERENCES

[1] Tope Komal, et al., " Encryption and Decryption using Artificial Neural Network" , IARJSET , Vol. 2, Issue 4, April 2015 pp. 81-83

[2] Yousif Elfatih Yousif, Dr.Amin Babiker A/Nabi Mustafa, Dr.Gasm Elseed Ibrahim Mohammed" Review on Comparative Study of Various Cryptography Algorithms",IJARCSSE , Volume 5, Issue 4, April- 2015, pp. 5155

[3] William Stallings, "Cryptography and Network Security: Principles and practices, Dorling Kindersley (india) pvt ltd., 4th edition(2009).

[4] Yousif Elfatih Yousif, Dr.Amin Babiker A/Nabi Mustafa, " Cryptography Techniques based on Neural Networks",IJARCSSE , Volume 7, Issue 4, April- 2017, pp. 308-311

[5] Haber, S.; Stornetta, W.S. How to time-stamp a digital document. In Proceedings of the Conference on the Theory and Application of Cryptography, Sydney, NSW, Australia, 8–11 January 1990; Springer: Berlin/Heidelberg, Gemany, 1990.

[6] Jin Ho Park and Jong Hyuk Park , Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions, Symmetry publications, 2017, pp. 1-13.

[7] Mann, C., Loebenberger, D. Two-factor authentication for the Bitcoin protocol. In International Workshop on Security and Trust Management; Springer International Publishing: Cham, Switzerland, 2015.

[8] Vasek, M.; Thornton, M.; Moore, T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Gemany, 2014.

[9] Karame, G.O.; Elli, A.; Srdjan, C. Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, CA, USA, 16–18 October 2012.

[10] Oludele Awodele, Olawale Jegede" Neural Networks and Its Application in Engineering ", InSITE, 2009

[11] Andrej Krenker, Janez Bešter and Andrej Kos " Introduction to the Artificial Neural Networks", Methodological Advances and Biomedical Applications

[12] M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya, An Enhanced and Secured RSA Key Generation Scheme (ESRKGS), journal of information security and applications, 2014, Elsevier, pp. 1-8.

[13] Ajay Pal Singh , Parvez Rahi " Performance Enhancement in Public key Cryptosystems for Security using RSA Algorithm " , IJARCCE , Vol. 5, Issue 11, November 2016 , pp. 359-362.

[14] Yousif Elfatih Yousif, Dr. Amin Babiker A/Nabi Mustafa, Performance Enhancement of RSA Algorithm Using Artificial Neural Networks, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.9, September- 2017, pp. 21-27.