Comparative Analysis of Light Weight algorithms based on Encryption in Cloud Data Security Environment

G.Sathish Kumar [1], Dr.A.Ramesh Babu[2]

[1] Research Scholar, Department of Computer Science, Chaitanya Deemed to be University,Warangal.
Email: sathishgundala86@gmail.com

[2] Professor, Department of Computer Science, Chaitanya Deemed to be University, Warangal.
Email: rameshadloori@gmail.com

Abstract: In the present era, data has becomechallenging, and humans needit more significantlytoperform various services. Those data are required to deploy and establish various services for multiple real-time applications. As data plays a significant role, it needs to be secure in transmitting and exchanging among the users, and those must be stored securely in various repositories. So, cloud computing comes into the picture as itcan handle a large amount of data and store it effectively. The data becomes critical and insecure as there is a drastic that needs to be secure and protected from attackers to achieve the security factors of AAAs such as Authorization, Authentication, and Accounting. Here the comparative analysis is done to ensure data in the applications in cloud computing. The various cryptographic algorithms include certain bits of a block cipher to perform encryption, hash functions, high system performance and reduce device resources for the environment of IoT. In this environment, the data can face various issues and challenges, such as power consumption on multiple devices, battery lifetime, shortage of memory, cost performance, and security level concerning the communication information. In the performance analysis, various algorithm is discussed concerning processing time, Accuracy, key generation, and data security levels as it helps to ensure security, key generation process, time complexity, storage, data reliability and integrity.

Keywords: Cloud Computing, Cryptography, Resource, Authentication, Integrity and IoT.

I. INTRODUCTION

In the current scenario, all real-time applications require a distributed environment, advanced technologies, and a large number of data to provide various services. As there is an increase in the data requirement, distributed framework, model, and protocol have to be redefined and deployed. In this scenario, the cloud plays a significant role and helps establish a communication network to provide the services and offers for a decentralized environment based on the user's needs. In general, the national information association has computed the data based on the cloud as the framework as it helps to manage and configure the resource being served. Based on the user's needs, those services provide a fast, easily accessible, and accessing networks [1]. The characteristics of the cloud environment computationare managing data scalability and affordable services effectively as represented in Figure. 1.

On-demand, a client being used in the cloud are utilize this kind of tools to create, operate, and applications and its services are being hosted that may be customized on any device.

The three service delivery models,

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

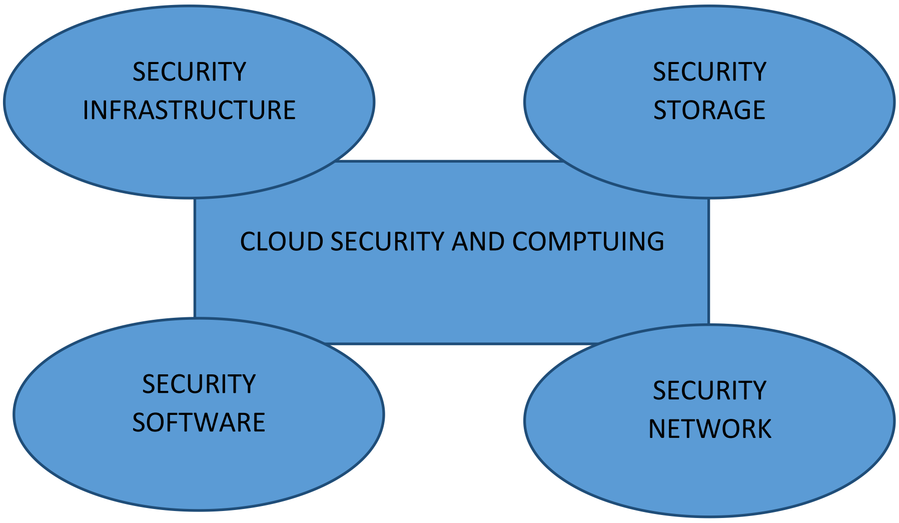

Figure 1. Cloud Security Framework

Numerous issues with interoperability, scalability, and multi-tenancy plague cloud infrastructure. However, the essential concerns are security since cloud infrastructure is vulnerable to several dangers because it uses internet networks. Security issues with cloud computing will prevent its broad adoption. Sharing cloud computing services makes keeping them safe and secure more challenging. This problem mainly affects cloud-outsourced data [2] and [3]. Network security is one of the most criticalcloud computing security challenges related to external and internal assaults. Establish a secure connection between service providers and users using various technologies and protocols.

The following list includes the two essential justifications for using new technologies for IoT.

1. End-to-end communication effectiveness: End-to-end security may be achieved with a lightweight symmetry key technique that uses less power on devices with limited resources.
2. Smart gadgets with limited resource adoption: The footprints of lightweight cryptography are substantially less than those of traditional encryption. It has the potential for more network connections with lower-resourceintelligent devices.

NIST describes lightweight cryptography as a subclass of cryptography that strives to offer solutions for quickly expanding applications that often use smart, low-power devices. It is intended for a wide range of hardware and software-based devices [4]. The performance of a standard cryptographic method may be good on PCs, servers, and some mobile devices. However, the lower ends of the spectrum include things like RFID tags, sensing equipment, sensor networks, and embedded systems. Lightweight cryptography platforms are necessary for these systems and networks.The Wireless Body Area Networks (WBAN), IoT, smart cards, and Wireless Sensor Networks (WSN) are a few examples of applications for the lightweight cryptographic technique.

IoT facilitates establishing connections and expanding networks connecting disparate items or technology in a diverseenvironment. IoT devices communicate either with each other orwith very little human involvement the unrelated parties; like barcodes, they may be included indata communicationdevices [5]. IoThas also revealed several security breaches as it considers any device may get unwanted access to the network and damage the network connection. This results in a security breach of network privacy and settings. InIoT environments, cloud computing can also be used, whichhas several security problems and difficulties.

The main objective includes,

- Various cryptographic algorithms are discussed based on specific bits of a block cipher to perform encryption, hash functions, high system performance and reduce device resources for the environment of IoT.
- In this environment, the data can face various issues and challenges, such as power consumption on multiple devices, battery lifetime, shortage of memory, cost performance, and security level concerning the communication information.
- In the performance analysis, various algorithms are discussed concerning processing time, Accuracy, key generation and data security levels as it helps to ensure security, key generation process, time complexity, storage, data reliability and integrity.

The paper is organized as follows,

II. SCHEMA FOR LIGHTWEIGHT CRYPTOGRAPHY

In their study, lightweight encryption designed for low-resource devices is discussed [6] and [7]. Existing research has suggested several cryptographic algorithms to improve performance for technologies, including AES-128, RC-5 , TEA and XTEA as represented in Figure 2.

A. BLOCK CIPHER:

In general, several algorithms are created by reducing traditional block cyphers' complexity ciphers to improve their performance. The block size must be minimal to optimize the benefits of lightweight ciphers and conserve resources. It should be less than AES at 64 bits rather than 128 bits. When the block size is reduced, the size of simple text is diminished. Based on the smaller-sized keys, power consumption is achieved with limited battery life, and the key size in a lightweight encryption algorithm must be tiny [8]. For instance, the key size of Twine is 80/128 bits, whereas PRESENT has an 80-bit key size.

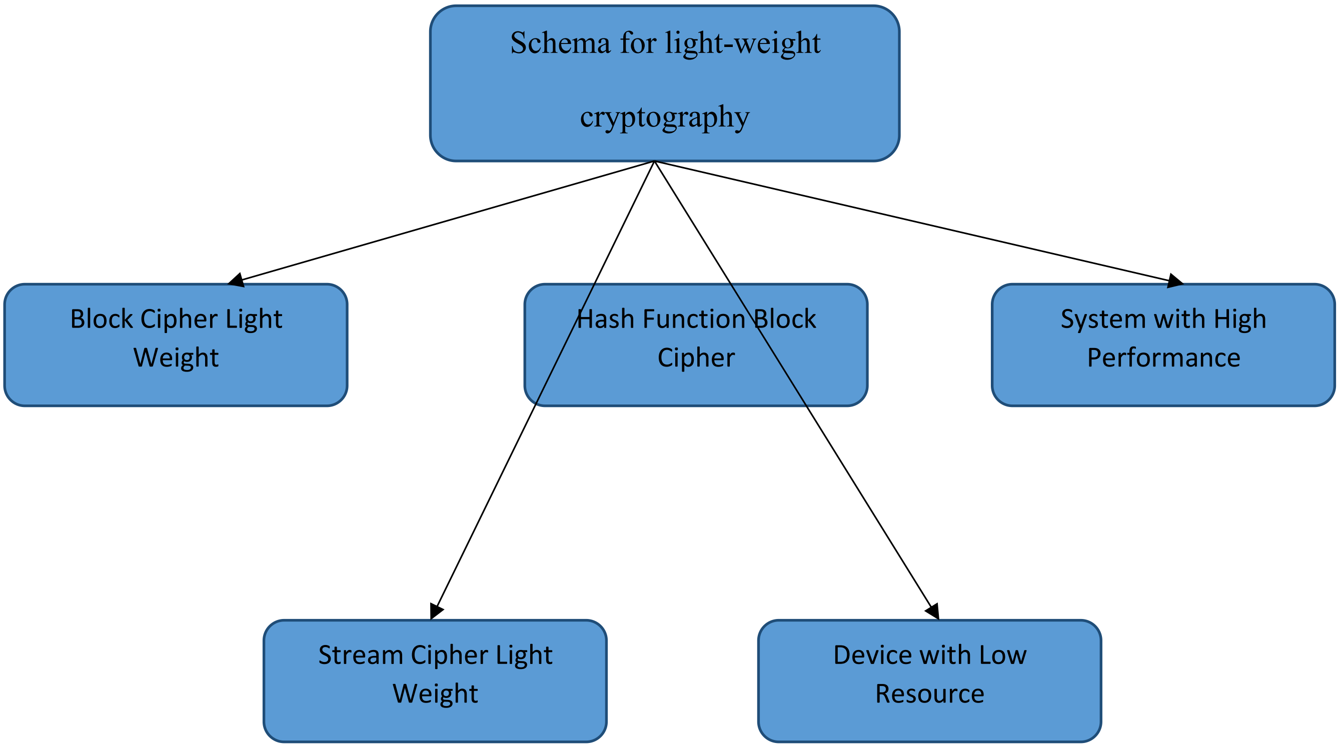
Schema for light-weight cryptography
Block Cipher Light Weight
Hash Function Block Cipher
System with High Performance
Stream Cipher Light Weight
Device with Low Resource

Figure. 2. Schema for light-weight cryptography

Table 1. Existing algorithms based on characteristics

Algorithm	Structure	Key Size	Block Size	Number of Rounds
AES	Substitution–Permutation Network	128/192/256	128	10/12/14
3DES	Feistel	56/112/168	64	48
DES	Feistel	54	64	16
Hummingbird	Feistel	256	16	4
XTEA	Feistel	128	64	64
RC5	Feistel	0-2040	32/64/128	1-255

Compared to traditional block cipher algorithms as tabulated in table 1, lightweight block ciphers that aim at low-resource-constrained devices naturally have simpler computation operations. In lightweight design methods, the number of rounds should be confined to a single S-box. In lightweight cryptography, 4-bit S-boxes have been utilized instead of 8-bit boxes [9].

The following are some shorter, lighter cryptographic algorithms,

Hummingbird2 only have four rounds, whereas PRESENT employs 4-bit S-boxes. Easier key schedules A key schedule is a method that determines the subkeys for rounds for a given key. When implemented, complex keys need more memory and power [10]. As a result, a lightweight block cipher makes use of critical schedules that are easier to create subkeys,for instance, the block cipher of TEA divides a 128-bit key into four 32-bit keys.

B. HASH FUNCTIONS:

A traditional hash function has a substantial internal state size and high power consumption, which may be undesirable for resource-constrained systems. Therefore, a lightweight function based on lightweight block ciphers is presented in 2008 by Andrey Bogdanov et al. PHOTON, Quark, SPONGENT, and Lesamnta-LW examples of lightweight hash functions. It makes decreased output size Applications requiring hash-function collision resistance depend on the enormous size.Interior and balance sizes can be used for applications where collision resistance is unnecessary [11].

When collision-safe hash capacity is required, this hash job should have comparable security against pre-image and assault with a second picture and impact. Thus, the range of internal conditions may be decreased. Decreased message size The enormous size of about 264 bits is reinforced by using traditional hash capacity [12]. The regular information size is significantly smaller for most objective cryptographic hashing capability constraints (like at most 256 bits). In this approach, hash algorithms that have been optimized for brief messages could make more sense for simple applications.

C. SYSTEM PERFORMANCE

Some conditions must be met to create a high-performance system. Specialized CPU CPUs used by cryptographic processors like CPU and Crypto ALU are tuned to run the encryption algorithm. The Instruction Set Architecture (ISA) often includes cryptographically focused instructions. The wide range of encryption techniques makes choosing these kinds of instructions challenging [13]. The system software must be changed to something resembling a compiler to use a new instruction. Crypto co-processor, the encryption speed is increased by the equipment module, which is dedicated to the encryption co-processor, the encryption business, and is controlled by the host processor.

The processing of overhead data from and to the c-processor impacts how data is generally executed.A cryptographic array of processing units and a multicore cryptographic processor were created by employing parallel calculations to improve performance even more. A routing topology is needed to transport data between processor units and memory in cryptographic arrays, similar to algorithmic jobs [14].The multicore cryptographic processor, however, is algorithm-independent.It offers a high data encryption rate or supports many ciphers operating simultaneously. An 8-core cryptographic processor (MCCP) can be configured for multi-channel and multi-standard systems.On the FPGA device, the core used AES encryption.Switching out the AES core for another block cipher is simple by rearranging the FPGA circuitry [15].

D. STREAM CIPHER:

Stream ciphers are another motivating basis for required circumstances. The European Network of Excellence for Cryptology organized the eSTREAM competition to identify novel stream figures suitable for widespread deployment [16]. In 2008, the three-stream ciphers Grain, MICKEY, and Trivium were named competition finalists for hardware applications with constrained resources.

E. DEVICE WITH LOW RESOURCES:

The lightweight cryptographic algorithm considers performance criteria in low-resource systems to achieve the same security levels. Power usage, waiting time or latency, and throughput are three ways to describe performance. This part shows two types of cipher implementation in low-resource devices. Implementation and measurements relevant to software Running a cryptographic code on the CPU allowed the program to be implemented. The code may depend on the machine (assembly), or it may not (java). A system often uses 8- or 16-bit, inexpensive microcontrollers [17].

Software implementations are concentrated on the power, speed, and memory utilized for a low-restricted device. The software-specific metrics concern the needed number of registers in RAM and ROM.Implementation and measurements relevant to hardware the resources required for hardware design and implementation are frequently stated in terms of the gate area and made using full bespoke ASICs or FPGAs. Reduced development costs and more flexibility are two advantages of the FPGA architecture. It has flip-flops, multiplexers, and look-up tables [18]. In contrast, the customized ASIC design relies on an automated design pipeline to shorten the design time.

III. CHALLENGES AND COUNTERMEASURES BASED ON SECURITY

IoT's physical/perception layer is a hybrid of the MAC and physical layers of the Internet architecture. It is used to collect data utilizing sensors, RFID, or GPRS.The IEEE 802.15.4 IoT standard is used at this layer. IEEE 802.15.4 is a cheap, battery-operated standard. It is a user-friendly security solution, but there are still certain dangers it cannot detect.The network layer is the lowest layer that collects data from the physical layer. This layer divides the message into bundles and routes the parcels from source to destination using the IPv6 addressing tool [19].

The IPv4 address space, which has more excellent address spaces, outpaces IPv6 as the IoT network expands quickly. By leveraging IPsec at this layer, built-in cryptography protocols such as AES and DES may be realized. Conveyance layer IoT uses the User Datagram Protocol for end-to-end communication (UDP). A security mechanism utilizing DTLS is implemented into this layer since UDP is an unstable protocol [20] and [21].This is the top layer where the natural growth of IoT intelligence is understood.The Constrained Application Protocol (CoAP) has been used for low-resource IoT devices and networks.

IV. LITERATURE SURVEY

Numerous research has looked at the security concerns of cloud computing; however, this section presents some recent studies that looked at cloud computing cryptography. It divides typical cryptographic algorithms into three categories:

- advanced encryption algorithm (AES),
- international data encryption algorithm (IDEA),
- data encryption standard (DES).

A comparison between symmetric and asymmetric algorithms (such as AES, DES, and 3DES) (e.g. RSA). Based on Block Size, Protection Rate, Key Length, Rounds, and Execution Time, algorithms were introduced. The outcomes are more productive in a cloud environment [22]. The author introduced hybrid encryption technologies to improve the privacy of information kept on cloud servers, including Blowfish, RSA, AES, Eclipse IDA, DSA, and others.

This study focuses on not utilizing third parties to encrypt customer data but on giving consumers the ability to choose how to encrypt their data. A cloud computing paradigm based on data categorization has also been developed to reduce latency and processing time. The information was divided into three tiers [23]. "The study advised the adoption of hybrid encryption ways to maximize the safety of cloud computing data, such as,

- RSA Digital Signature
- RSA algorithm
- Blowfish algorithm

Encryption/decryption, Feistel, and XOR operating algorithms. Furthermore, it demonstrated how to combine two separate algorithms, such as DES and RSA, to eliminate Cloud Storage's security challenges.

The authors conducted a survey and found prior research on cloud data security. They recommended employing a hybrid encryption strategy utilizing Blowfish and MD5 to provide better security on the cloud server [24]. [25] investigated a few popular cloud service providers, including Google (Google Drive) and Microsoft (Azure and One Drive). Furthermore, they investigated cryptographic algorithms commonly used in cloud computing: modern cryptography, searchable encryption, homomorphic encryption, and attribute-based encryption (e.g. DES, 3DES, AES, RC6, and BLOWFISH), and as a fusion of two or more cryptographic techniques, they developed a hybrid encryption concept to capitalize on the potential of each system to protect cloud data. IDAs, SHA-512, 3DES, and AES-256 comparison done by [26].

It comprises of data encoding and decoding done on-site. The safety and speed for both large and small data files are substantially higher thanks to this technique. The classification of algorithms by hash, symmetric, asymmetric, and signature algorithms was examined by the author [27].There have been several studies on symmetrical cryptographic algorithms that are lightweight and were developed used in applications like L Block and LED. PRESENT, HIGHT, DESL, CLEFIA, TWINE, RECTANGLE, SIT, etc.

A compact 128-bit key, 64-bit block size cryptosystemwas made, iterated 32 times, and used the XOR technique together with either left- or right-hand rotations. Its primary goal was to install hardware on ubiquitous devices such as wireless sensor nodes and RFID tags that had roughly the same chip size as AES but ran substantially faster [28]. [29] The authors disclosed the symmetric block cypher CLEFIA-128, which was created by Sony and designed to work with both hardware and software.

It has 128-bit block size encryption,"The researcher created two different kinds of Data Encryption Lightweight systems, namely DESXL. In DESXL, instead of independent ones with no start and final permutations, a single S-Box u is utilized to boost protection by employing a 184-bit key. There was no attack on DESL and DESXL, as they said [30]. The research discovered the generalized multi-platform Feistel structure known as "TWINE." Each round has a 4-bit S-box, a 4-bit block permutation layer, and a nonlinear replacement layer. It is a block cipher size algorithm that runs 36 rounds with either an 80-bit or a 128-bit key length.

[31] described the "RECTANGLE" cryptosystem as being optimized for a block size of 64 bits with a key length of either 80 or 128, running just 25 rounds. In the lightweight, Stable IoT (SIT) encryption algorithm. The data must be encrypted using a 64-bit address since it is a 64-bit block cipher. The algorithm's structure is a hybrid of the Feistel and uniform substitution-permutation network. In [32], a lightweight encryption technique based on a 64-bit block cipher and an 80-bit key are used to encrypt data in IoT devices.

V. PERFORMANCE ANALYSIS

By employing the Block Size, Key Length, Possible Key, Mathematical Operations, Cipher Type, and Security Power parameters as stated in Table 6, the following ciphers were tested: DES [31], AES [32] and Blowfish [34],. The findings show how adaptable and extremely secure the NLCA algorithm is. The NLCA algorithm reduces computational complexity and processing power by having a clear architecture that includes five rounds of encryption; each round requires simple mathematical procedures. The dynamic key generation process is used during encryption to lessen the pressure on the system.The NLCA method reduces computational complexity and processing resources by having a straightforward design that contains five rounds of encryption; each round requires basic mathematical processes.

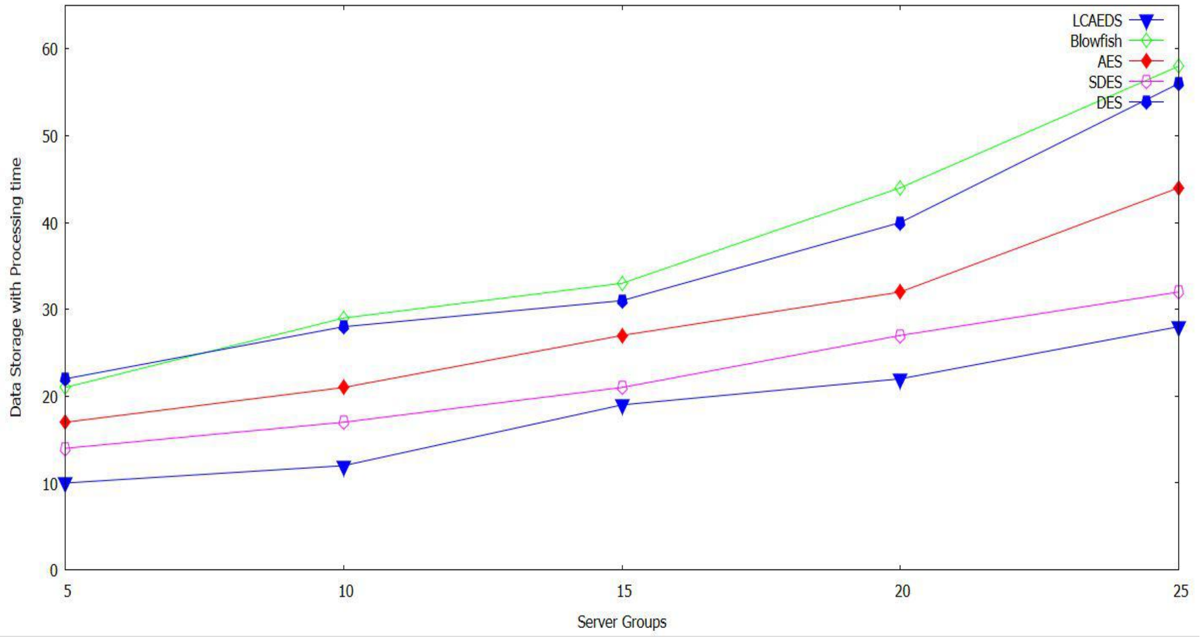

Figure 3. Server Group Vs. Data storage with processing time

In Figure 3, the processing time is calculated based on the data storage with respect to the server group, which varies from 5 to 25. Then the LCAEDS approach gets reduced processing time as compared to other existing algorithms such as Blowfish, DES, 3DES, and AES.

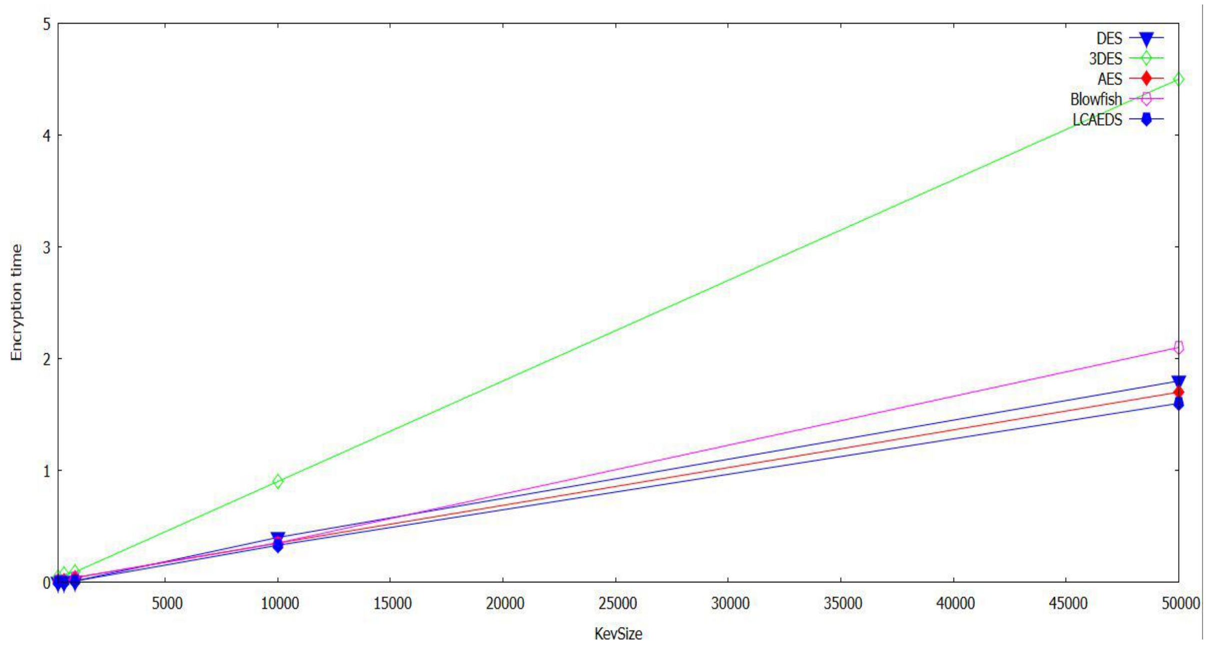

Figure 4. Key Size Vs. Encryption Time

In the Figure 4, the encryption time is calculated based on the variation in the key size from 5000KB to 50000KB. The LCAEDS gets less encryption time anf gets gradual reduce and it outperforms with other existing algorithms such as, blowfish, DES, 3DES and AES.

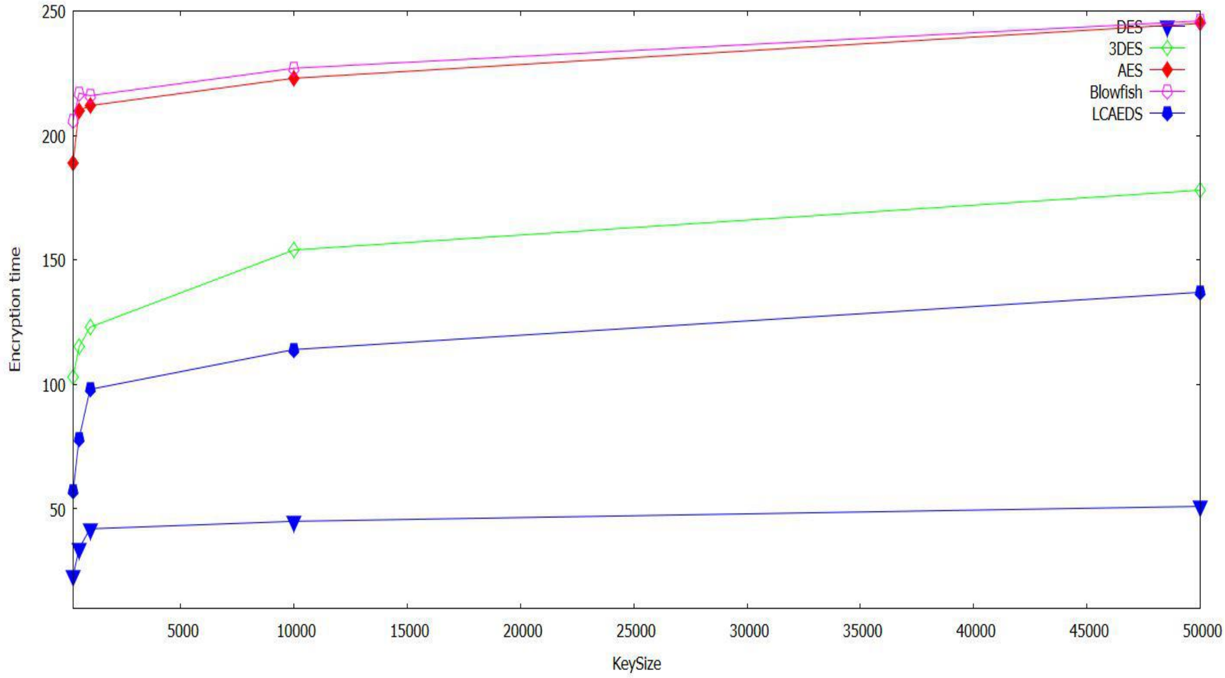

Figure 5. Key Size Vs. Encryption Time

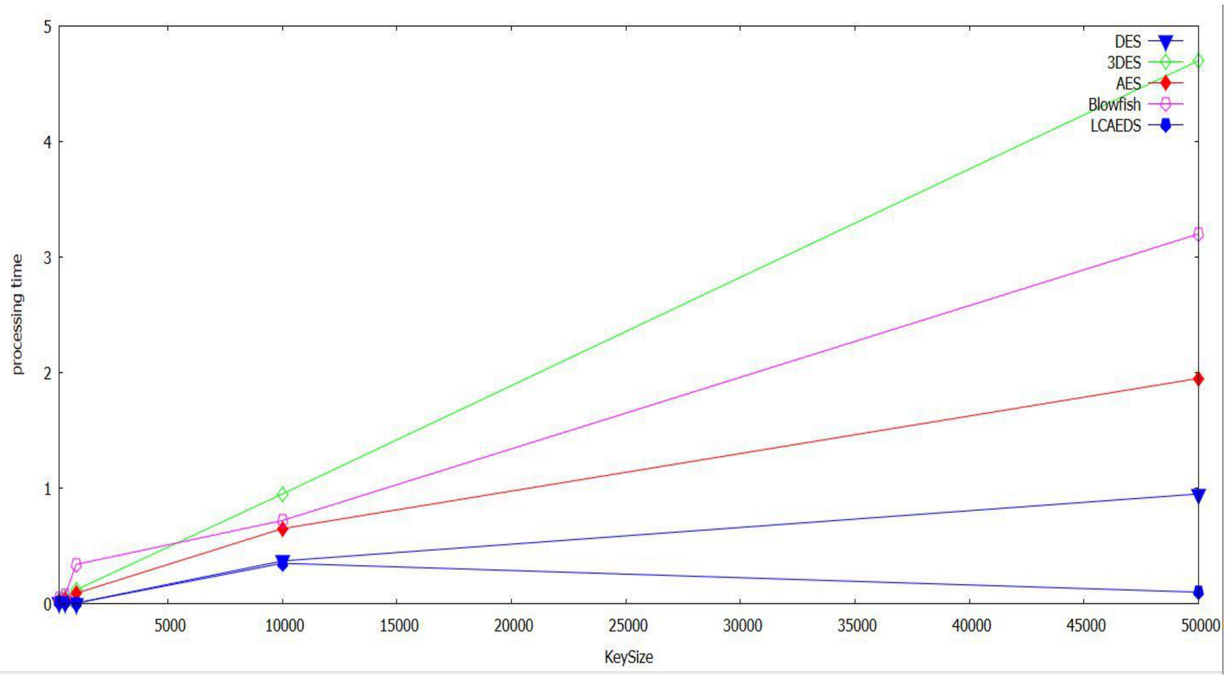

Figure 6. Key Size Vs. Processing Time

In the Figure 5 and 6, the encryption and processing time are calculated based on the variation in the key size from 5000KB to 50000KB. The LCAEDS algorithm performs better when compared with other existing algorithms.

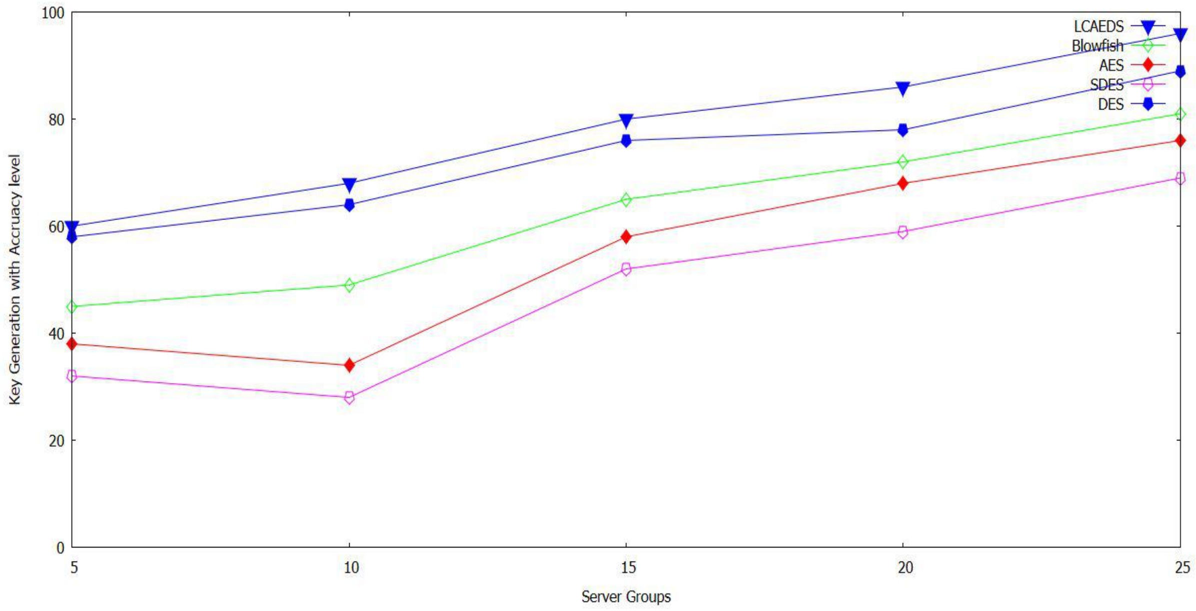

Figure 7. Server Group Vs. Key Generation with Accruacy Level

In the Figure 7, the Accuracy levels are calculated based on the variation in the server group from 5 to 25. The LCAEDS determines the better accuracy and gets gradual increase based on the increase in server group when compared with other existing algorithms.

Finally, a brief description of the NLCA method is provided based on the data encryption enforcement capabilities of cloud storage. • Security: Because of its complicated structure and combination of Feistel and SP architectural techniques, NLCA is a secure algorithm. • Process for generating keys Due to the matrix and f-function extension of a key rather than a single extension key, NLCA provides an efficient key process that helps to resist brute-force assaults. The security level will be raised since the Key Generation technique is being employed, according to NLCA. • Time Complexity: There is no additional difficulty in time due to the lowering of the demands of subsequent rounds. Storage: The suggested method makes sense for a distributed storage system in the context of cloud computing since it applies the concealed sharing concept to give secure access to data across unreliable nodes. • Reliability: A more dependable and secure algorithm. • Integrity: Because of the use of the transpose and swap procedures, a minor change in input data can result in a dramatic change in the ciphered output.

VI. CONCLUSION

In the performance analysis, various algorithm is discussed concerning processing time, Accuracy, key generation, and data security levels as it helps to ensure security, key generation process, time complexity, storage, data reliability and integrity. LCAEDS algorithm provides effective data encryption enforcement with the capabilities of cloud storage. Here the comparative analysis is done to ensure data in the applications in cloud computing. The various cryptographic algorithms include certain bits of a block cipher to perform encryption, hash functions, high system performance and reduce device resources for the environment of IoT. In this environment, the data can face various issues and challenges, such as power consumption on multiple devices, battery lifetime, shortage of memory, cost performance, and security level concerning the communication information. In the Future, the novel lightweight encryption algorithm has to be deployed to ensure the data authentication, authorization and Accounting features in cloud-based data security.

REFERENCES:

[1] Markus Klems, Jens Nimis& Stefan Tai, 2008. Do Clouds Compute? A Framework for Estimating the Value of Cloud Computing. Workshop on E-BusinessWEB 2008: Designing E-Business Systems. Markets, Services, and Networks. 110-123.

[2] Mehrdad Jangjou& Mohammad Karim Sohrabi. 2022. A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing. Archives of Computational Methods in Engineering. 29. 3587-3608.

[3] MohdTajammul, Rabindra Nath Shaw, Ankush Ghosh &Rafat Parveen. 2021. Error Detection Algorithm for Cloud Outsourced Big Data. Advances in Applications of Data-Driven Computing. 105-116.

[4] Marcel Medwed; VentzislavNikov; Joost Renes; Tobias Schneider; Nikita Veshchikov. 2021. Cyber Resilience for Self-Monitoring IoT Devices. IEEE International Conference on Cyber Security and Resilience (CSR).

[5] TanweerAlam. 2020. Efficient and Secure Data Transmission Approach in Cloud-MANET-IoT Integrated Framework. Journal of Telecommunication, Electronic and Computer Engineering. 12(1).

[6] GanduRamu, Zeeshan Mishra, Pulkit Singh and Bibhuendra Acharya. 2020. Performance optimised architectures of Piccolo block cipher for low resource IoT applications. International Journal of High Performance Systems Architecture.9(1). 49-57.

[7] MuyideenAbdulraheem, Joseph Bamidele Awotunde, Rasheed Gbenga Jimoh& Idowu Dauda Oladipo. 2021. An Efficient Lightweight Cryptographic Algorithm for IoT Security. International Conference on Information and Communication Technology and Applications, ICTA. 444-456.

[8] Bassam Aboushosha; Rabie A. Ramadan; Ashutosh Dhar Dwivedi; Ayman El-Sayed; Mohamed M. Dessouky. 2020. SLIM: A Lightweight Block Cipher for Internet of Health Things. IEEE Access. 8. 203747 – 203757.

[9] Reynier Antonio de la Cruz Jiménez. 2019. Generation of 8-Bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-Bit S-Boxes and Finite

Field Multiplication.International Conference on Cryptology and Information Security in Latin America, LATINCRYPT, 191-206.

[10] Subodha Charles; Prabhat Mishra. 2020. Securing Network-on-Chip Using Incremental Cryptography. IEEE Computer Society Annual Symposium on VLSI (ISVLSI).

[11] Sa'ed Abed, Reem Jaffal, Bassam J. Mohd& Mohammad Al-Shayeji. 2021. An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. Cluster Computing. 24, 3065-3084.

[12] Yushu Zhang; Ping Wang; Liming Fang; Xing He; Hao Han; Bing Chen. 2020. Secure Transmission of Compressed Sampling Data Using Edge Clouds. IEEE Transactions on Industrial Informatics. 16(10). 6641-6651.

[13] Iqbal Ahmed. 2020. A brief review: security issues in cloud computing and their solutions. TELKOMNIKA Telecommunication, Computing, Electronics and Control. 17(6).

[14] K. Kaviya, K. K. Shanthini& Dr. M. Sujithra, 2019. Evolving Cryptographic Approach for Enhancing Security of ResourceConstrained Mobile Device Outsourced Data in Cloud Computing. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 5(1). 101-106.

[15] Md Arefin Rabbi Emon; Hasan Jamil Apon; Fahim Faisal; Mirza Muntasir Nishat; Khandakar Adil Morshed; Ahmed Mujtaba Al Naser, FatemaZerinJaba and FarihaAnzum. 2021. Advanced Encryption Standard for embedded applications: An FPGA-based implementation using VHDL. 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM).

[16] OlexandrKuznetsov, OlexandrPotii, Artem Perepelitsyn, Dmytro Ivanenko& Nikolay Poluyanenko. 2018. Lightweight Stream Ciphers for Green IT Engineering. Green IT Engineering: Social, Business and Industrial Applications. 113-137.

[17] Longteng Yi; Xiaojun Tong; Zhu Wang; Miao Zhang; Honghong Zhu; Jing Liu. 2019. A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network. IEEE Access. 7. 53079 – 53090.

[18] George Provelengios; Daniel Holcomb; Russell Tessier. 2020. Power Wasting Circuits for Cloud FPGA Attacks. 30th International Conference on Field-Programmable Logic and Applications (FPL).

[19] Li-HsingYenaWei-TingTsai. 2010. The room shortage problem of tree-based ZigBee/IEEE 802.15.4 wireless networks. Computer Communications. 33(1). 454-462.

[20] JasenkaDizdarević, Francisco Carpio, AdmelaJukan and Xavi Masip-Bruin. 2019. A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. ACM Computing Surveys. 51(6). 1-29.

[21] Harth Ghassan Hamid, Zainab T. Alisa. 2021. Survey on IoT application layer protocols. Indonesian Journal of Electrical Engineering and Computer Science. 21(3). 1663-1672.

[22] L. Tawalbeh, N.S. Darwazeh, R.S. Al-Qassas, and F. AlDosari, "A secure cloud computing model based on data classification, "2015, doi: 10.1016/j.procs.2015.05.150.

[23] R. Arora , A. Parashar , Secure user data in cloud computing using encryption algorithms, Int. J. Eng. Res. Appl. (2013) .

[24] S.S. Khan, P.R. Tuteja, Security in cloud computing using cryptographic algo- rithms, Int. J. Innov. Res. Comput. Commun. Eng. (2015), doi: 10.15680/ijircce.2015.0301035

[25] D.P. Timothy, A.K. Santra, A hybrid cryptography algorithm for cloud computing security, 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore (2017) 1–5, doi: 10.1109/ICMDCS.2017.8211728 .

[26] J.R.N. Sighom, P. Zhang, L. You, Security enhancement for datamigration in the cloud, Futur. Internet (2017), doi: 10.3390/fi9030023 .

[27] Z. Gong, S. Nikova, and Y.W. Law, “KLEIN: a new family of lightweight block ciphers, ”2012, doi: 10.1007/978-3-642-25286-0_1.

[28] G. Leander, C. Paar, A. Poschmann, and K. Schramm, “New lightweight des variants, ”2007, doi: 10.1007/978-3-540-74619-5_13.

[29] T.P. Berger, J. Francq, M. Minier, G. Thomas, Extended generalized feistel networks using matrix representation to propose a new lightweight block cipher: lilliput, IEEE Trans. Comput. (2016), doi: 10.1109/TC.2015.2468218 .

[30] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, I. Verbauwhede, RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms, Sci. China Inf. Sci. (2015), doi: 10.1007/s11432-015-5459-7 .

[31] M. Usman, I. Ahmed, M. Imran, S. Khan, U. Ali, SIT: a lightweight encryption algorithm for secure internet of things, Int. J. Adv. Comput. Sci. Appl. (2017), doi: 10.14569/ijacsa.2017.080151 .

[32] A.H.A. Al-ahdal , G.A. Al-rummana , G.N. Shinde , N.K. Deshmukh , A Robust Lightweight Algorithm for Securing Data in Internet of Things Networks, ustain- able Communication Networks and Application. Lecture Notes on Data Engineering and Communications Technologies, vol 55. Springer, (2021) In press .