ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse115942020.pdf
https://doi.org/10.30534/ijatcse/2020/115942020

Data Security in Cloud Environment Based on Comparative Performance Evaluation of Cryptographic Algorithms

Nagesh Shenoy H[1], K. R. Anil Kumar[2], Suchitra N Shenoy[3], Abhishek S. Rao[4]
[1]Dept. of Computer Science & Engineering, Canara Engineering College, India, h.nagesh.shenoy@gmail.com
[2] Quality College of Management Studies and Science, India, anilkumar@dayanandasagar.edu.in
[3]Research Scholar, Canara Engineering College, India, suchiprab_16@yahoo.co.in
[4]Dept. of Information Science & Engineering, NMAM Institute of Technology, Nitte, India, abhishekrao@nitte.edu.in

ABSTRACT

With the extensive use of cloud environment to store sensitive data, the need for data security has been on the rise. The data being stored in multiple location servers, in fragments, makes it cumbersome to manage in terms of ease of access and privacy. Data security, being a crucial factor in several fields, is being extensively researched upon. In order to preserve data confidentiality from unauthorized access, hackers, and intruders, cryptography has proven to be highly effective. Although widespread research is already available on this area, the need to upgrade the degree of security witnesses the frequent introduction of new cryptographic schemes. This paper provides a review of some of the prevalent cryptographic techniques utilized in data storage, particularly cloud environments, to safeguard data integrity and privacy. The comparison of efficiency of various algorithms, in terms of operational time consumption, has been provided along with simulation results for comparative analysis of symmetric, asymmetric algorithms, as well as hashing mechanisms.

Key words: Cloud Computing, Data Security, Cryptography, Symmetric Key, Asymmetric Cryptography, Hybrid Cryptography, Hash Functions.

1. INTRODUCTION

With the advent of the Internet, there has been ease of accessibility to vast information, as well as widespread connectivity. Adding on to this, the cloud environment has aided companies and organizations to streamline their business with the centralization of data, thereby enabling global operations sans concerns pertaining to remote data accessibility. With global connectivity, data loss prevention, and expanded storage capacity (beyond that of personal devices), cloud environment has proved highly advantageous to its users. However, cloud service providers have the added responsibility of maintaining security and privacy. Around mid-2014, eBay reported a major breach wherein details (names, addresses, DOB, passwords) of all its 145 million users were compromised [2]. It took Yahoo close to four years (in October 2017) to estimate the breach that occurred in 2013-14 and again in December 2016, had in fact compromised the accounts of all its 3 billion users, including login details, DOB, and names. In November 2018, the world's biggest hotel chain, Marriott International, announced that hackers had managed to steal data of approximately 500 million customers. The compromised data was a combination of passport data, travel details, other customer including contact information, in addition to credit card details of more than 100 million customers. In 2019, Capital One (a bank holding company) made headlines with the biggest breach that compromised the personal information of about 106 million customers and applicants. While close to 140,000 social security numbers and 80,000 linked bank account numbers had been exposed, 1 million Canadian social insurance numbers of credit card applicants and customers had been accessed [1, 3]. Such incidents only showed the vulnerability that exists for data in cloud, hence making it the crucial responsibility of service providers to maintain customer confidentiality and avoid data breaches. With the ever-growing developments in IoT, the cloud is being utilized effectively for vast data aggregation and storage. At the currently overwhelming rate of growth, the International Data Corporation (IDC) has estimated that by the year 2025, about 41.6 billion connections to IoT devices will generate data of about 79.4 zettabytes. However, with the connection of several devices to the Internet, the vulnerability increases (breach in security or social media data leaks). In order to safeguard the vulnerable data extending over several channels in diverse networks, data security needs to be prioritized [22]. A comprehensive research on the existing cryptographic and security techniques would help assess their efficiency and capacity to safeguard the data. This paper focuses on the modus operandi of existing popular cryptographic algorithms, in addition to evaluating each one's efficiency. All simulations are carried out using JCE and BouncyCastle API.

The organization of the rest of this paper follows as: Section 2 outlines recent studies pertaining to cryptography, with a

literature review of the works incorporating cryptographic algorithms. Section 3 includes the fundamentals of cryptography along with its classification. Section 4 explains in-depth, some of the most widely used cryptographic algorithms. Section 5 provides a brief view of hybrid cryptography and its functioning. Section 6 summarizes the experimental outcomes of several test cases, of each algorithm. Section 7 provides the conclusion on the work together with a summary for possible future progress.

2. RELATED WORK

A model was developed to capture a multi-stage scenario by linking the organizations from diverse industry sectors which are facing a sophisticated ransomware attacker. A study was also made to analyze the degree in which an investor can serve a deterrent for ongoing attacks [4]. An attempt was made in providing an asymmetric cryptographic capability of the tag to extend the ISO/IEC 18000-6c/EPC Gen 2 protocols which would support a varied number of security operations in dissimilar scenarios. The work also analyzed on various schemes of cryptography to select which requires low silicon area, low power demands and faster computations. Examinations were made to analyze the potential to perform Side Channel Attacks to break secure tags by recommending to tag developers to contemplate such attacks in their implementation process [5]. A research was also made to define the development process of analytics engine which could gather sensor data from different devices to provide relevant information from IoT data using data mining algorithms. [6]. An approach was made to initiate the innovation and competitiveness among European industries in identifying the potential transformational big data within several key sectors [7]. Various cloud models have been defined, in addition to discussing the ever-increasing popularity of cloud computing. Their focus was on cloud providers providing the added functionality of secure sharing. In order to achieve this, their proposed framework functions by allowing the cloud user to generate a key for selected users with permissions for file access, while utilizing cryptographic algorithms like AES and RSA. This implies that, while the selected users attempt to access the files on cloud with their assigned key, only permissions decided by the owner will provided to the user. By utilizing one of the most secure cryptographic algorithms - AES, only partial access is granted to the user, which is comparatively secure as compared to providing the user with a password. While this scheme imparts more security, it does include the downside of "partial access" to the users [8]. The use of data encryption and decryption to enhance data security has been explained in [9]. While classifying encryption algorithms as symmetric- and asymmetric-key encryptions, they have discussed, accordingly, DES and RSA algorithms in-depth. They performed a comparative analysis of both these algorithms by using several performance parameters like key length, speed, power consumption, level of security, and cost of implementation. In conclusion to this, they stated that the algorithm choice is not generic as it depends upon the application. The need for cryptography to maintain network security over information sharing has been mentioned in [10], along with defining different cryptographic techniques. The symmetric key algorithms presented are AES, DES, 3DES, and Blowfish, along with a comparison of their features and performance metrices. Likewise, asymmetric key algorithms like RSA, DH, ECC, and DSA have been presented along with each one's features, advantages, and downsides. They conclude by highlighting that improvements to some of the existing techniques can be done through further research and that use of symmetric key algorithm is preferable due to simplicity of implementation. [11] states that with the heightened use of Internet in the 21st century, the need to improve security and integrity of data, along with that of the system and network, is more than ever. They proceed by suggesting the use of a hybrid encryption technique utilizing RSA and Blowfish algorithms, along with the implementation methods for achieving the same in applications. In the proposed scheme, the user is first authenticated prior to providing access to store or retrieve data. The RSA algorithm is used to assign private keys, the files are encrypted using hybrid cryptography, and the decryption is performed with Blowfish keys. The functioning of this scheme has been proven with results obtained. [12] mentions that due to accessibility of data being possible from anywhere at any time, there is a greater need to make the cloud system secure, to achieve confidentiality and integrity. They discussed the types of clouds, with examples. and used statistical data to support the challenges faced over several aspects of data security. While utilizing one of the SHA variants, i.e. SHA-256 and AES encryption for securing data in cloud, experimental results were presented to support their concepts, along with the mention for further work being required in this domain. With the increasing use of clouds, by organizations, for data storage and retrieval, [13] utilized hybrid cryptography to impart a secure environment for data storage on cloud. Based on their proposed model, encryption of data is performed prior to outsourcing it to the cloud server, thereby concealing the original data from intruders, while providing the corresponding decryption key only to authorized users for retrieving the original data. They used symmetric key cryptography for the implementation, stating it to be more efficient than public key cryptography. [14] claims that a single cryptographic algorithm will not be able to provide highly effective security for the data stored or transmitted in cloud. They covered the advantage that different algorithms provided individually and highlighted the shortcomings that could be solved using hybrid cryptography. They proposed a new system that combined AES, Blowfish, RC6, and BRA algorithms. Following splitting of the file into eight parts, encryption of individual parts of the file is performed by distinct algorithms, with multithreading technique being used to simultaneously encrypt various parts of the file collectively. Additionally, the use of LSB steganography was introduced for key information security. Their implementation results were compared with

existing works, while concluding that their proposal provided exceptionally good "block wise data security". With the objective of providing high security on data transmission using cloud, [15] utilized a hybrid cryptosystem, comprising of Blowfish symmetric algorithm to maintain data confidentiality, while authenticating data with the use of RSA symmetric algorithm. The blowfish secret key that is generated gets encrypted with the use of RSA. Additionally, SHA-2 algorithm is used for signature verification and data integrity. Their results of implementation claimed to provide increasingly efficient data security and proper network access on demand. [16] states that with the massive outsourcing of user data to cloud from popular websites and apps, there remains the need for improved security and access control. While highlighting the significance of cloud, they also mentioned several concerns pertaining to data security. Owing to instances of multiple major attacks on cloud, leading to confidentiality issues, several users are hesitant to outsource data and services. The prime factors of data security requiring immediate attention were stated to be privacy and integrity. Through their research, they demonstrated data security as a predominant concern in cloud usage, while showing that there is a huge scope for improvement. A survey was made to give an insight on the modern cryptography describing the technique of enciphering and deciphering with cryptographical algorithms and to develop software which could solve the problems related to security issues [17]. Modern developments in cryptography were examined in the area of teleprocessing to explore the novel cryptographic systems which could help in minimizing the need for secure key distribution channels and to solve cryptographic problems of long standing [18]. A systematic review of various symmetric key cryptography algorithms was made to highlight the passive and active attacks in data transmission [19]. Comparative analysis and selection method on various hash algorithms was made to analyze the awareness of attacks in password hashing based on the problem scenario [20].

3. FUNDAMENTALS OF CRYPTOGRAPHY

In order to secure the data being transmitted from intruders and unauthorized access, cryptography is utilized to convert the raw data (plaintext) into an unintelligible/encoded form (cipher-text); thereby leading to only authorized entities to access the original information, by decoding ciphers [8]. Cryptographic techniques date back to the "hieroglyph" used by Egyptians and was also used in the time of warfare by soldiers and even kings for transmitting crucial messages. While encryption in cryptography transforms the data into ciphertext by using a secret key, the process of decryption transforms the encrypted data into an intelligible form by using a decryption key. Figure 1 depicts the three types of cryptographic algorithms namely Symmetric (secret-key), Asymmetric (public-key), and Hash functions [10].

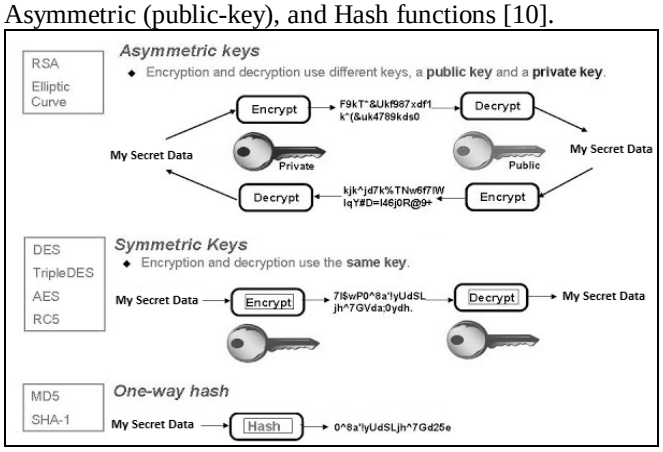

Figure 1: Classification of Cryptographic algorithms

3.1 Asymmetric Cryptography

Also referred to as public key cryptography, this algorithm generally utilizes pairs of keys - public key that may be distributed widely, and is used for encrypting a message, while decryption of the encrypted message can be achieved with a private key that only the owner can access. Some of the common asymmetric algorithms are RSA, DSA, ECC, Diffie-Hellman, etc.

3.2 Symmetric Cryptography

The symmetric cryptography techniques utilize a single key for plaintext encryption and ciphertext decryption. Common symmetric algorithms include Blowfish, AES, DES, RC4, RC5, RC6, etc.

3.3 Hash Function

This cryptographic technique is also referred to as one-way encryption, wherein decryption isn't possible. A compressed, fixed-length hash value is computed for an arbitrary length input message, hence making it impossible for the contents of the input message to be recovered. Hash functions are used by many operating systems to encrypt passwords.

4. STANDARD ALGORITHMS

Table 1 shows the list of standard cryptographic algorithms with its type and description along with advantages and disadvantages.

Table 1: Standard Cryptographic Algorithms

Algorithm	Type	Description	Advantages	Disadvantages
RSA	Asymmetric	The public key used for encryption consists of two numbers, where one number is multiplication of two large prime numbers. Private key used for decryption also derived from same two prime numbers.	Safe and secure owing to the use of complex mathematics - due to factorization of prime numbers that are difficult to factorize.	Can be very slow when large data needs to be encrypted by same computer. Requires a third party to verify reliability of public keys.
DES	Symmetric	A block cipher algorithm that takes plain text in blocks of 64 bits and 56 bit key as input and converts them to ciphertext using keys of 48 bits, with totally 16 rounds of encryption.	A 56 bit key results in 2^{56} possibilities of keys, making a brute force attack impossible. With same algorithm used for encryption and decryption, it is convenient for software and hardware requirements.	Weak keys and semi-weak keys. Cryptanalysis attack is easier than brute force attack.
3DES	Symmetric	A symmetric key-block cipher that applies DES cipher in triplicate by encrypting with first key, decrypting with second key, and encrypting with a third key.	Significantly more secure than DES due to longer key length and repeated operations.	Inefficient and slow while encrypting large messages due to multiple operations involved.
AES	Symmetric	The plaintext is divided into 128-bit (16 bytes) blocks each and treats each block as a 4x4 array. The block is then encrypted using one of the three different key lengths, 128, 192, and 256 bits.	The longer key lengths provide increased security. Relatively faster implementation in software and hardware.	Increased key length increases execution time, hence slow performance. It has been proven to be a weak cipher, hence shouldn't be trusted to protect sensitive data.
RC2	Symmetric	A 64-bit block cipher with a variable key size that uses 18 rounds, i.e. 16 mixing rounds and 2 mashing rounds.	Two times faster software implementation in comparison to DES.	Increased implementation cost. This is obsolete as it is dangerously susceptible to brute force attack.
RC4	Symmetric	A stream cipher and variable length key algorithm that encrypts one byte at a time.	Simple and extremely fast. Can use broad range of key lengths.	The probability of key reuse is high, leading to chances of security compromise.
Blowfish	Symmetric	A 64-bit block cipher that takes a variable-length key, from 32 bits to 448 bits and uses 16 rounds.	Easy implementation and one of the fastest block ciphers. Blowfish security has been extensively tested and proven. Not subject to patents, hence freely available for use by anyone.	Longer messages increase computation time. Use of a 64-bit block size makes it vulnerable to birthday attacks. A reduced-round variant of Blowfish is susceptible to known plaintext attacks on relatively weak keys.
MD5	Hash Function	Compresses any variable length data into 128 bits (fingerprint of input), by processing the data in 512-bit blocks.	Computationally fast. Collision resistance. Provides a one-way hash.	Has known security flaws and vulnerabilities. Is less secure than SHA-1 algorithm.
SHA-1	Hash Function	Produces a 160-bit message digest for messages with length less than 2^{64} bits.	Longer hash value and comparatively more secure than MD5. Collision resistant.	Slower computation than MD5. Known security vulnerabilities.
SHA-2	Hash Function	Consists of 6 hash functions with hash values 224, 256, 384, or 512 bits.. SHA-256 and SHA-512 are novel hash functions computed with 32- and 64-bit words, respectively.	None of the hash algorithms is secure to ensure integrity except SHA-2. Provides better prevention against collision.	Not time efficient as SHA-1.
SHA-3	Hash Function	The SHA-3 (Keccak) generates almost unique 224-, 256-, 384-, or 512-bit signatures for a text.	Not vulnerable to length extension attacks.	Slower than SHA-2 on a general-purpose processor. Hardware implementation of SHA-3 costs more than that of SHA-2.

5. HYBRID CRYPTOGRAPHY

Hybrid cryptography is the combination of symmetric encryption and public key/asymmetric encryption. This provides a cryptographic solution of preserving the speed associated with symmetric encryption, while also maintaining the security and flexibility of exchange associated with asymmetric encryption. Encrypting the message is done using symmetric encryption and the secrecy of the key is maintained by encrypting the key using asymmetric encryption. While overcoming the drawbacks of individual algorithms, it also enhances security [21]. Figure 2 shows the architecture of

data and key sharing in hybrid cryptography. The process of data and key sharing is illustrated as:

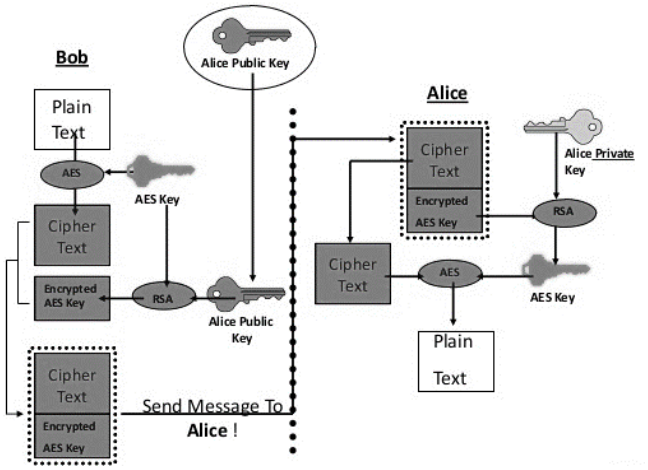

Figure 2: Data & Key Sharing in Hybrid Cryptography

Hybrid cryptography can be implemented in different ways, as mentioned below:

5.1 RSA-AES Hybrid Algorithm

As the name implies, this hybrid algorithm combines an asymmetric (RSA) and a symmetric (AES) algorithm. The Figure 3 shows the implementation of internal process of hybrid cryptography.

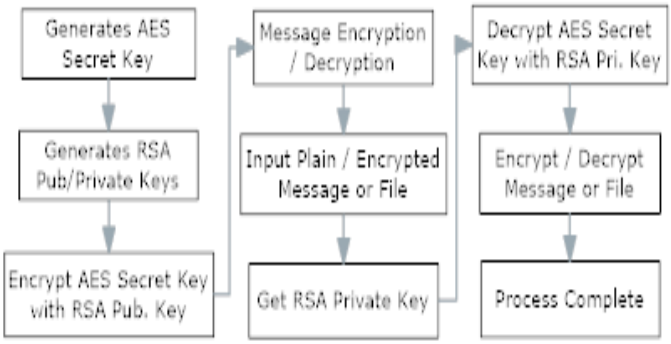

Figure 3: Hybrid Cryptography Internal Process

Apart from this hybrid cryptographic combination, there are several combinations available, such as RSA-DES, RSA-Blowfish, 3DES-AES, etc. The hybrid algorithm that is selected is dependent on the applications.

6. RESULTS AND DISCUSSION

In order to obtain statistical data, practical simulations have been conducted using a 64-bit Intel I5-2430M processor with 4-cores and a 4GB RAM. The coding language used is Java with JCE (Java Cryptography Extension) with BouncyCastle APIs. The Operating System used is 64-bit Windows 7. In order to evaluate the algorithmic efficiencies, testing is done with varying file sizes. Table 2 lists out the encryption and decryption time (ms) of different symmetric algorithms for multiple file sizes.

Table 2: Symmetric Algorithm Performance

	AES		DES		3DES		Blowfish		RC2		RC4	
File Size (mb)	Enc. time (ms)	Dec. time (ms)	Enc. time (ms)	Dec. time (ms)	Enc. time (ms)	Dec. time (ms)	Enc. time (ms)	Dec. time (ms)	Enc. time (ms)	Dec. time (ms)	Enc. time (ms)	Dec. time (ms)
1	15	42	36	53	121	114	19	24	37	38	9	27
2	32	100	90	93	224	241	58	38	87	61	55	41
5	108	88	185	261	511	628	93	183	192	245	43	37
10	178	180	430	412	1090	1124	250	237	404	316	99	97
15	195	196	544	553	1513	1578	288	348	553	441	120	142
20	338	399	811	872	2089	2168	505	463	822	660	292	246

Figure 4 illustrates the performance of the different algorithms about varying file sizes and encryption and decryption time (ms).

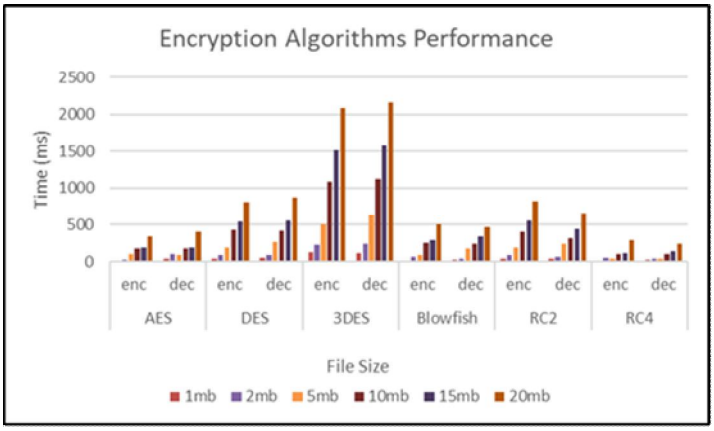

Figure 4: Symmetric Algorithm Performance Graph

Table 3 lists out the time (ms) for encryption and decryption of various hybrid algorithms for multiple file sizes. The hybrid algorithms used for comparison are RSA-AES, RSA-Blowfish, and RSA-RC2.

Table 3: Hybrid Algorithm Performance

	RSA_AES		RSA_Blowfish		RSA_RC2	
File Size (mb)	Enc. time (ms)	Dec. time (ms)	Enc. time (ms)	Dec. time (ms)	Enc. time (ms)	Dec. time (ms)
1	16	19	23	27	41	42
2	31	79	51	79	86	91
5	80	103	111	132	202	188
10	158	179	214	251	385	336
15	250	227	286	328	578	441
20	370	377	553	710	847	832

Figure 5 illustrates the performance of different hybrid algorithms about varying file sizes and encryption and decryption time (ms). With respect to time, the performance of RSA-AES is better in comparison with RSA-Blowfish and RSA-RC2.

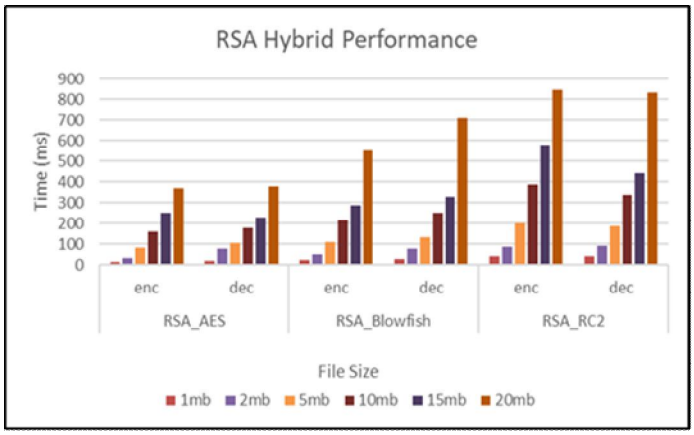

Figure 5: Hybrid Algorithm Performance Graph

Table 4 lists out the encryption time (ms) of different hash algorithms for multiple file sizes. For comparison, the MD5 and SHA variants have been experimented upon.

Table 4: Performance of Hash Algorithms

File Size

Hashing	1mb	2mb	5mb	10mb	15mb	20mb
MD5	7	13	34	96	99	125
SHA1	8	17	46	129	163	171
SHA2 (224)	13	26	67	168	190	254
SHA2 (256)	13	26	66	190	196	255
SHA2 (384)	9	19	48	139	173	184
SHA2 (512)	9	19	49	138	154	183
SHA3 (224)	63	127	316	719	958	1263
SHA3 (256)	82	136	335	768	1047	1338
SHA3 (384)	86	181	431	968	1310	1704
SHA3 (512)	124	249	617	1327	1859	2458

Figure 6 illustrates the performance of MD5, SHA-1, and SHA-2 variants about varying file sizes and encryption time (ms). The comparison has shown that SHA-2 (512) has better performance than other variants owing to reduced time consumption along with higher level of security.

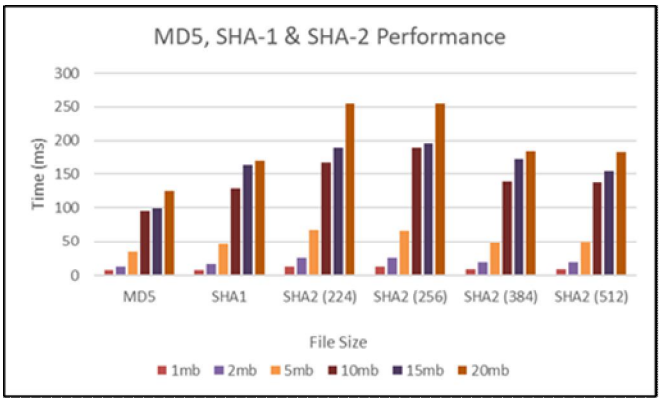

Figure 6: Hash Algorithms Performance Graph

Figure 7 illustrates the performance of different SHA-3 variants (hashing algorithms) about multiple file sizes and encryption time (ms). The comparison has shown that SHA-3 (384) has better performance than other variants owing to reduced time consumption along with higher level of security.

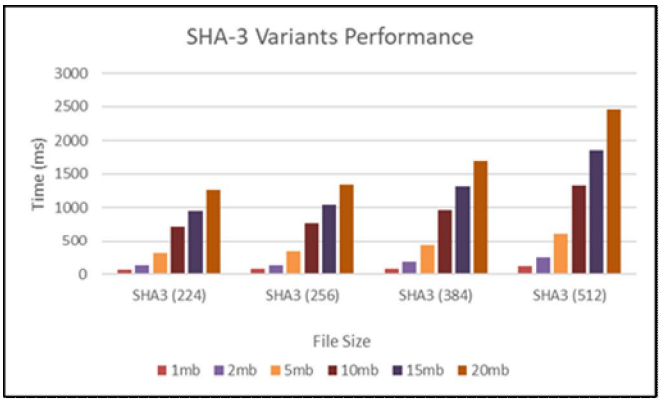

Figure 7: SHA-3 Variants Performance Graph

Table 5 lists out the ECDH (SEC) curve variants' time efficiency. Only NIST specified ECDH (SEC) variants have been experimented upon.

Table 5: ECDH(SEC) Curve Efficiency Comparison

ECDH (SEC)		
Curve	**Size (in bits)**	**Time(ms)**
secp192k1	192	772
secp192r1	192	785
secp224k1	224	819
secp224r1	224	808
secp256k1	256	841
secp256r1	256	823
secp384r1	384	952
secp521r1	521	1117

Figure 8 illustrates the time efficiency (ms) of different ECDH (SEC) curve variants. The comparison has shown that secp256r1, i.e. 256 bits variant has a slightly better performance that other variants.

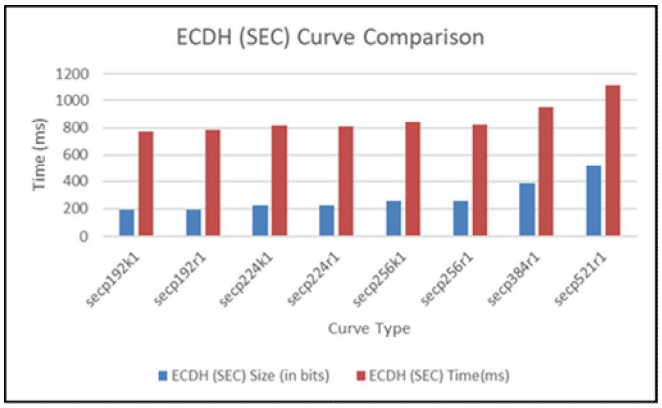

Figure 8: ECDH (SEC) Variants Comparative Performance Graph

7. CONCLUSION

With cyber criminals being aware of updated hacking techniques and tricks these days, maintaining data security has become a herculean task. The two dominant challenges encountered by cloud service providers are privacy

maintenance and managing information on servers. This paper presented a brief review on several cryptographic techniques in addition to evaluating several cryptographic algorithms based on efficiencies. The results quite evidently show that hybrid algorithms provide higher security and efficiency. Also, the most recent SHA variant, i.e. SHA-3, exhibited improved performance over its predecessors, thereby proving to be a suitable candidate for authentication or digital fingerprinting. For improved efficiency in future operations, optimization techniques like PSO or Genetic algorithm could be integrated along with symmetric algorithms.

REFERENCES

[1] E.Q. Freeman, **10 lessons learned from major retailers' cyber breaches, PropertyCasualty360** (2014). https://www.propertycasualty360.com/2014/09/23/10-lessons-learned-from-major-retailers-cyber-brea/.

[2] S.M. Kelly, **EBay's Massive Security Breach: What it Means for You, Mashable**, 2014. http://mashable.com/2014/05/21/ebay-breach-ramifications/

[3] E. Dunnand, **Kmart is latest victim of US retail data breach, Bus. Insid.** (2014). https://www.businessinsider.com/afp-kmart-is-latest-victim-of-us-retail-data-breach-2014-10.

[4] Laszka, A., Farhang, S. and Grossklags, J., 2017, **October. On the Economics of Ransomware**, *International Conference on Decision and Game Theory for Security* (pp. 397-417). Springer, Cham. https://doi.org/10.1007/978-3-319-68711-7_21

[5] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, Eds., **Vision and Challenges for Realising the Internet of Things.** rue Mercier, Luxembourg: Publications Office of the European Union, 2010.

[6] D. Evans. **The Internet of Things—How the next evolution of the Internet is changing everything**. Cisco, Inc., http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_ 0411FINAL.pdf

[7] V. Turner, J. F. Gantz, D. Reinsel, and S. Minton, ‘‘**The digital universe of opportunities: Rich data and the increasing value of the Internet of Things**,’’ IDC Anal. Future, Framingham, MA, USA, Tech. Rep., 2014.

[8] K. Chachapara and S. Bhadlawala, "**Secure sharing with cryptography in cloud computing**," *2013 Nirma University International Conference on Engineering (NUiCONE)*, Ahmedabad, 2013, pp. 1-3.

[9] “N. Jayapandian, A. M. J. M. Z. Rahman, S. Radhikadevi and M. Koushikaa, "**Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption**", *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, Coimbatore, 2016, pp. 1-4.

[10] S. Chandra, S. Paira, S. S. Alam and G. Sanyal, "**A comparative survey of Symmetric and Asymmetric Key Cryptography**", 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, 2014, pp. 83-93.

[11] S. Purevjav, K. H. Kim, M. Sain and H. Lee, "**Design of hybrid cryptosystem for cloud system**", *2015 IEEE Conference on Wireless Sensors (ICWiSe)*, Melaka, 2015, pp. 67-70. https://doi.org/10.1109/ICWISE.2015.7380356

[12] V. K. Soman and V. Natarajan, "**An enhanced hybrid data security algorithm for cloud**", *2017 International Conference on Networks & Advances in Computational Technologies (NetACT)*, Thiruvanthapuram, 2017, pp. 416-419

[13] S. Kaushik and C. Gandhi, "**Cloud data security with hybrid symmetric encryption**", *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, New Delhi, 2016, pp. 636-640.

[14] P. V. Maitri and A. Verma, "**Secure file storage in cloud computing using hybrid cryptography algorithm**", *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, 2016, pp. 1635-1638.

[15] D. P. Timothy and A. K. Santra, "**A hybrid cryptography algorithm for cloud computing security**", *2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, Vellore, 2017, pp. 1-5.

[16] S. H. Nagesh, K. R. A. Kumar and K. T. Rajgopal, "**Cloud architectures encountering data security and privacy concerns — A review**", *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, 2017, pp. 1729-1735. https://doi.org/10.1109/ICECDS.2017.8389745

[17] Schneier, Bruce, “**Applied Cryptography. Protocols, Algorithms, and Source Code in C**”, New York: *Wiley & Sons*, 1996.

[18] W. Diffie and M. Hellman. “**New directions in cryptography**”. *IEEE Transactions on Information Theory*, IT No.2(6):644C654, November 1976.

[19] Preeti Singh, Praveen Shende, “**Symmetric Key Cryptography: Current Trends**”, *International Journal of Computer Science and Mobile Computing*, 3(12), December 2014, pp. 410-415.

[20] Thomas, C.G, and Jose, R.T. “**A Comparative Study on Different Hashing Algorithms**”, *International Journal of Innovative Research in Computer and Communication Engineering*, 3(7), 2015, pp. 170-175.

[21] P. Kuppuswamy, Saeed Q. Y. Al-Khalidi, “**Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm**”, *National*

Chengchi University & Airiti Press Inc, 2014, 19(2), Pages 1-13.

[22] Nagesh Shenoy H, K R Anil Kumar, Rajgopal K T, Abhishek S. Rao, "**An Audit on Cloud Architectures Addressing Data Privacy and Security Concerns**" International Journal of Advanced Science and Technology, 2020/5/20,Page 6373-6382.