Comparison Analysis and Systematic Study on Secure Transmission of Data in the Cloud Using Steganographic Techniques and Cryptographic Algorithms

AKSA Anudini[1], G.Gayamini[2], and TL Weerawardane[2]

[1]*Department of Computer Science, General Sir John Kotelawala Defence University, Sri Lanka*
[2]*Department of Computer Engineering, General Sir John Kotelawala Defence University, Sri Lanka*

[#]36-cs-0011@kdu.ac.lk

Abstract: *Data and information can be considered the most precious assets in electronic communication systems, but security has become a struggle in this competitive world. Cloud computing has emerged as the most exciting technology for on-demand computing. It is now used by the military, healthcare, education, finance, and various other organizations to handle their large volume of information. Cloud computing has many benefits, including efficiency, high performance, scalability, accessibility, backup, and recovery. Security is a primary concern in cloud computing because everyone in the organization shares the same cloud platform. The most significant issue for the user is securely saving, retrieving, and transmitting data through the cloud network and storage. Cryptography and steganography can be defined as the most popular techniques that can be used to enhance data security. Cryptography scrambles the messages into an unintelligible format, while steganography hides the message as it is not observable to the attacker. High-level security is given for both the sender and the receiver inside the cloud platform when cryptography is used along with steganography. This paper analyzes the performance of cryptographic and steganographic techniques and suggests the best hybrid cryptographic algorithms and multilayer steganographic techniques that can be combined for efficient and secure data transmission in the cloud. This proposed system will provide availability, integrity, authenticity, confidentiality, and non-repudiation to the data and information.*

Keywords: *Asymmetric Key Cryptography, Cryptography, Image Steganography, Steganography, Symmetric Key Cryptography*

1. Introduction

Cryptography is a method of converting readable information into an unreadable format and vice versa. Cryptography consists of terminologies, namely plain text, ciphertext, encryption, and decryption. Encryption is the process of converting a regular communication (plaintext) into a meaningless message (ciphertext), while decryption is the process of returning a meaningless message (ciphertext) to its original form (plaintext). Symmetric key cryptography (private key cryptography) encrypts plaintext and decrypts ciphertext using the same cryptographic key. Asymmetric Key Cryptography (also known as Public Key Cryptography) has two keys, namely a private key and a public key. The message will be encrypted by the sender using the receiver's public key. Then the message will be decrypted by the receiver using his or her private key.

Steganography is an information-hiding technique that uses cover objects to send messages between a sender and a recipient without arousing suspicion and without allowing anybody else to know whether the communication is taking place. Steganography can be classified into five types depending on the nature of the cover object, namely text, video, audio, image, and network steganography. Text steganography secures a message by hiding it in a particular letter of each word or rearranging the text without altering its meaning. Audio Steganography makes use of the human ear to conceal information secretly. Video Steganography camouflages the secret message into a digital video. Network Steganography is hiding information using a network protocol as a cover object, such as UDP, IP, TCP, ICMP, etc. The secret message is hidden as an image in the cover object using Image Steganography.

Both steganographic and cryptographic approaches are used to secure data. The difference between steganography and cryptography is that cryptography scrambles a message such that it cannot be deciphered by unauthorized users or third parties. Steganography camouflages to hide the existence of a message; then anyone can know there is a concealed message hidden in a cover object. Steganography provides confidentiality and authentication only, while cryptography provides confidentiality authentication, data integrity, and non- repudiation.

Section II of this paper deals with the literature review on the research related to data and information security using steganographic or cryptographic techniques. Section III provides the proposed methodology; section IV presents the discussion, and section V presents the conclusion.

2. LiteraruereReview

This section deals with the vast number of research related to secure and efficient data in the cloud using steganographic or cryptographic techniques.

Research on performance analysis of Symmetric Cryptographic Algorithms (Vyakaranal and Kengond, 2018) has discussed different symmetric key cryptographic algorithms, namely Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), and Blowfish by analyzing encryption time, decryption time, avalanche effect, energy consumption, memory usage, and throughput by implementation using java. The results of the study reveal that the Blowfish algorithm requires less memory and high throughput, and it needs less time for the encryption and decryption of files when compared to other algorithms. Moreover, the study depicts that the blowfish algorithm is well suited for situations where memory and time usage play a significant role, while the AES algorithm is ideal for applications where strength and minimal energy usage is an important aspect. In addition, DES is the best algorithm for applications that need security with minimum bandwidth consumption.

A study (Shakti,2015) was conducted to analyze the performance of asymmetric cryptographic algorithms namely RSA (Rivest, Shamir, Adleman), Diffie-Hellman, El Gamal, Elliptic-curve cryptography (ECC), and Digital Signature Algorithm (DSA) algorithms. The results of the study have concluded that each algorithm had its advantages and disadvantages. Furthermore, the experiments prove that the efficiency of RSA is lower than the ECC algorithm. In addition, El Gamal is slower and DSA needs lots of time to authenticate and the verification process has complicated remainder operators. Moreover, the authentication procedure of the Diffie- Hellman algorithm is very low. Finally, the study concluded that all of the algorithms' performance is dependent on the application they choose.

Research (Jaspin et al., 2021) proposed a method to provide high security to the cloud platform using double encryption techniques. The proposed system combined the AES symmetric cryptographic algorithm and RSA asymmetric cryptographic algorithm to increase the security and reduce the drawbacks of using those algorithms separately. The results of the study depict that the proposed methodology takes the least time for encryption runtime and decryption runtime of the text file. In addition, the proposed system provides a higher level of security with resistance against propagation errors compared with DES, Blowfish, RC5, and 3-DES algorithms. The study (Timothy and Santra,2017) aimed to create a new security solution to protect the data in the cloud with a hybrid cryptosystem. The proposed system combined the Blowfish symmetric cryptographic algorithm to ensure the confidentiality of data and the RSA asymmetric cryptographic algorithm to guarantee the authenticity of data. In addition, this system consists of Secure Hash Algorithm-2 (SHA-2) to ensure data integrity. Therefore, the study has revealed that this hybrid cryptosystem provides high security for data transmission over the cloud. A review on data and information security in cloud computing using steganography (Alkhamese et al., 2017) depicts the types of steganography with a high focus on image steganography. The paper highlights the techniques of the Discrete Cosine Transform (DCT) and Least Significant Bit (LSB). Performance evaluation of the spatial domain and transform domain techniques of image steganography exposed the fact that spatial domain, the LSB technique, is mostly used to hide data that has a higher payload capacity, but it's easily encoded and detected by attackers. In the transform domain, the DCT technique is very complicated and has a low payload capacity compared to the LSB technique, but the DCT technique provides more security than the LSB technique. Furthermore, this research suggested that future work could combine LSB and DCT approaches to avoid the drawbacks that arise when applying these techniques individually and to increase the secret message's security.

A study (Chandran and Bhattacharyya, 2015) analyzed the performance of Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) steganographic techniques. The performance analysis of the above-mentioned steganographic techniques was carried out by analyzing the parameters namely invisibility, robustness, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Invisibility is the similarity of the stego image, and the original image. Robustness means the ability of the secret message to remain unchanged even if the stego image was subjected to changes. The square of the error between the cover picture and the stego image is MSE, while the greatest signal-to-noise ratio in the stego image is PSNR. As a result of the experiments, it can be concluded that the DCT algorithm is the most suitable technique compared with the DWT and the steganographic techniques. Research (Singh, et al., 2018) was conducted to analyze the performance of the LSB and modified DWT algorithm for image steganography. According to the results obtained by testing five RGB image sets, the researchers concluded that the modified DWT algorithm has a higher PSNR value, high security, invisibility, and robustness compared with the LSB algorithm. Furthermore, it was concluded that the overall performance of the modified DWT algorithm is better than the LSB algorithm.

Research (Biswas et al., 2019) has exposed an efficient algorithm to provide the confidentiality, integrity, and authentication of data and information using hybrid cryptographic and steganographic algorithms. Hybrid cryptography was used in this study, including the AES symmetric cryptographic method and the RSA asymmetric algorithm. The LSB steganographic approach was then used to embed the hidden message.

The study (Palathingal et al., 2019) focused on a cloud data security model using cryptography and steganography. Through the proposed system, data will be encrypted using the RSA asymmetric cryptographic algorithm. After that, the secret data will be embedded using Discrete Wavelet Transform (DWT) technique. Then the file will be uploaded to the cloud. The results of the proposed system will be provided with augmented security to the data that can be used anywhere without qualms.

Another research (Naidu et al., 2019) presented a multilayer security system to protect and hide multimedia data using cryptographic and steganographic techniques. Here, DES symmetric cryptographic algorithm is used as the symmetric cryptographic algorithm and the LSB technique is used to hide the secret message or data. Furthermore, the study has revealed that steganography is a highly effective technique used for confidential communications. Aside from secret communications, the researchers determined that the combination of cryptography and steganography may be utilized for a variety of others.

3. Proposed Methodology

This system will be developed by combining the blowfish symmetric key cryptographic algorithm, Elliptic-Curve Cryptography (ECC) asymmetric cryptographic algorithm and RSA asymmetric cryptographic algorithm as the hybrid cryptosystem to perform double encryption to secure the data.

Then Discrete Cosine Transform (DCT) and Least Significant Bit (LSB) image steganographic techniques are combined to create a multilayer steganographic algorithm to hide the encrypted file inside a cover image to provide extra security.

This system consists of 2 processes as Encryption & Embedding Process and the Decryption & Extraction Process.

A. Encryption & Embedding Process

Here Figure 1 shows the encryption and embedding process of the file to the cloud. If the user is new, the user should register and log in to the system. Then the user should choose the file to be uploaded to the cloud and then the file will be automatically encrypted using the blowfish symmetric key cryptographic algorithm, Elliptic- Curve Cryptography (ECC) asymmetric cryptographic algorithm, and RSA asymmetric cryptographic algorithm as the hybrid cryptosystem to perform hybrid encryption to secure the data. Then Least Significant Bit (LSB) image steganographic technique is combined to create a multilayer steganographic algorithm to hide the encrypted file inside a cover object to provide extra security.

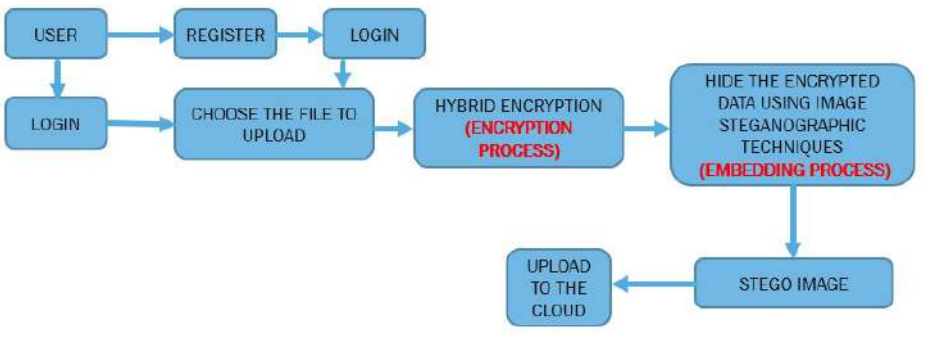

Figure 1. Encryption and Embedding Process
Source: Author

B. Decryption & Extraction Process

Here Figure 2 shows the decryption and extraction process of the file to the cloud. If the user is new, the user should register and log into the system. Then the user should choose the file to be downloaded from the cloud and then the steganographic image will be extracted and get the encrypted file in the extraction process. Next, the encrypted file will be decrypted in the decryption process

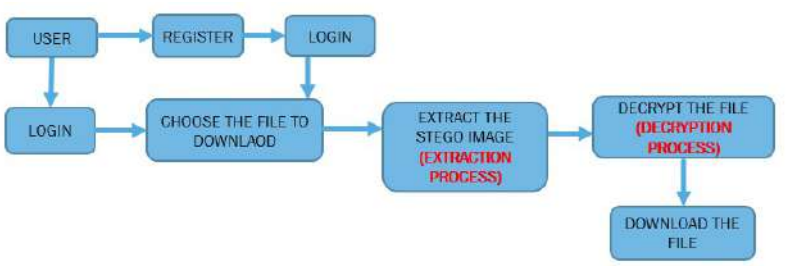

Figure 2. Decryption and Extraction Process
Source: Author

C. Key Management Server

The generated private key will be stored in another file and will be sent to the cloud Key Management Server. When a user decides to download a file, must first log in to the system and then provide the key to gain access to the storage. This key will be provided via a secure channel to the authorized user. The key is generated by using a hash function to the private key file. After the user enters the key, the system compares the produced key to the key entered by the user. If they are identical, the user obtains access to the private key and can decrypt the file.

4. Discussion

To minimize data breaches, reduce the danger of data exposure, and maintain regulatory compliance, data security functions are deployed. The purpose of data security in any company is to ensure that private data is used safely and securely while minimizing the risk of exposure.

In recent years, people used symmetric or asymmetric cryptographic approaches to increase the efficiency and security of data transmission inside the cloud. But with the development of technology hackers easily broke the algorithms and decrypt the ciphertext. As a solution for using symmetric or asymmetric cryptographic algorithms individually, the researchers proposed systems to combinesymmetric and asymmetric algorithms to enhance the security of the cloud. Therefore, the double encryption techniques using both symmetric-key algorithms and asymmetric key algorithms help to reduce the drawbacks that arise when they are used separately. In the double encryption process, the two-time encryption and decryption process is performed using symmetric and asymmetric algorithms. With technological advancement, cryptography was used along with steganography to give high security to the cloud. The fundamental drawback of cryptography is that anyone can understand there is that secret communication is taking place. As a result of that, hackers try to access the data by breaking the secret key. But when we use steganography, no one is aware of the ongoing secret communication. In this case, the secret message can be hidden inside audio, text, network, video, or image. The drawbacks that arise from using only steganography to hide the secret message are steganography doesn't provide non-repudiation, and authenticity, it provides only confidentiality to the data. Therefore, to provide high security to data when saving, retrieving, and transmitting in the cloud, it is best to choose the best hybrid cryptographic algorithm and multilayer steganographic algorithm. Table 1 shows the statistics of 6 cloud platforms used in the world, the security mechanisms used, and the latest attacks faced by them.

Table 1. Comparison of cloud platforms

Reference	Cloud Platform	Security Mechanism	Latest Attack Faced
(Nicholson,2020)	AWS (Amazon Web Services)	The AES-256 algorithm is used to encrypt data in AWS, including server-side encryption in Amazon Simple Storage Service (S3)	Amazon Web Services (AWS) claimed the largest Distributed Denial of Service (DDoS) assault on records at 2.3 Tbps in 2020
(Cimpanu,2021)	Microsoft Azure	The Advanced Encryption Standard (AES) encryption used by Storage Service Encryption is 256-bit. Transparent encryption, decryption, and key management are all handled by AES.	In early August 2021, a 2.4 terabits-per-second (Tbps) distributed denial of service (DDoS) assault was launched.
(Hope,2021)	Google Cloud	The Advanced Encryption Standard (AES) algorithm is used by Google to encrypt data at rest. By default, all data is encrypted with AES256 at the storage level. When encrypting data in the Cloud, GCP uses DEKs and KEKs, which are utilized and stored via Google's Key Management Service (KMS) API.	Google discovered that 86 percent of the 50 recently hacked Google Cloud instances were utilized for bitcoin mining.
(Goud,2021)	IBM Cloud	use 256-bit AES algorithm keys to data encryption.	Cyber-attacks exposed more than 8.5 billion records in 2019, according to IBM's X- Force Threat Intelligence Index 2020. As a result of faulty cloud servers and human mistakes, hackers obtained access to around 7 billion records.
(Staff, 2016)	Alibaba Cloud	An industry-standard AES-256 algorithm is used to encrypt data and associated keys. The overall key management architecture of Alibaba Cloud follows the guidelines in (NIST) 800-57 and employs cryptographic methods that meet the (FIPS) 140-2 standard.	In 2015, Chinese hackers attempted to use Alibaba Group Holding Ltd's own cloud computing service to get access to over 20 million active accounts on the Taobao e- commerce website.
(Whiting, 2019)	Oracle Cloud	The Transparent Data Encryption (TDE) Algorithm encrypts data at rest in Oracle Databases in a transparent manner. It prevents the operating system from accessing Database data stored in files without altering how SQL is used to obtain the data by applications.	In 2018, the Oracle cloud was hacked, and the attacks appeared to be intended at the company's Micros Systems credit card payment system.

Table 1 shows that most cloud platforms encrypt data using the AES or TDE algorithms but according to the statistics, cloud systems are vulnerable to massive data breaches.

Table 2 shows the comparison of mainly using symmetric key cryptographic algorithms namely AES, Blowfish, DES, 3-DES, and RC5.

Table 2. Comparison of symmetric and asymmetric cryptography

Parameters	**AES**	**DES**	**3-DES**	**RC5**	**BLOWFISH**
Key size and no: of rounds	128,192 and 256 bits. 10,12 and 14 rounds	64-bit key. 16 rounds	112 bits or 118 bits & 48 rounds	0 to 2040 bits & 12 rounds	32-448 bits 16 rounds
Block size	128 bits	64 bits	64 bits	32, 64, or 128 bits	64 bits
Security	Secure	Not secure	Better than DES	Partially secure	Very Secure
Speed	Fast	Very slow	Slow	Slow	Fast
Data Confidentiality	Yes	No	No	No	Yes
Data Integrity	Yes	No	No	No	Yes
Cipher Text Size	Similar to plain text	Larger than plain text	Larger than plain text	Larger than plain text	Same as plain text
Characteristics	Replacement for DES, Excellent security,	Not much secure but flexible	Good security, Flexible	Not much secure, simple, consume less memory	Excellent security, Flexible

Source: (Vyankaranal et al., 2018)

According to the previously discussed literature review and the comparison of the above-mentioned symmetric cryptographic algorithms, the best symmetric cryptographic algorithm that can be used is the Blowfish algorithm.

Table 3 shows the comparison of mainly using asymmetric key cryptographic algorithms namely Diffie-Hellman, RSA, ECC, EL Gamal, and DSA algorithms.

Table 3. Comparison of symmetric and asymmetric cryptography

Parameters	**RSA**	**DSA**	**ECC**	**Diffie-Hellman**	**El Gamal**
Key size	>1024	1024	Calculates key from Elliptic curve equations	1024 to 4096	1024
Efficiency	Not much efficient	Faster	Very fast & efficient	Not very efficient	Faster & efficient
Attacks	Brute force attack, a	The attacks may depend on	Doubling attack	Vulnerable to attack	Vulnerable to Meet-in-

	timing attack	implementation		the-middle	middle attack
Advantage	The private key is difficult to generate from the public key and modulus. As a result, it delivers a high level of security.	Provide authentication and non-repudiation	Uses elliptic curve equations theory	The symmetric key is short in length (256 bits); Therefore, the algorithm is quite fast	El Gamal encryption is different from El Gamal's signature. (Therefore, no confusion occurred)
Disadvantage	The complexity of generating keys is difficult	Needs lots of time to authenticate and the verification process has complicated remainder operators	It is complex, implementation is difficult	The authentication procedure is very low	Slow speed and the message is doubled in size as a result of the encryption procedure.

Source: (Shakti, 2015)

Table 4 shows the comparison of main image steganographic techniques namely LSB, DCT, and DWT.

Table 4. Comparison of Image Steganographic Techniques (Machit et al., 2019)

Parameter	**LSB**	**DCT**	**DWT**
Invisibility	Low	High	High
Robustness	Low	Medium	High
Payload	High	Medium	Low
Complexity	Low	High	High
Peak Signal to Noise Ratio (PSNR)	Medium	High	Low
Mean Square Error (MSE)	Medium	Low	High

According to the previously discussed literature review and the comparison of the above-mentioned image steganographic techniques, the best hybrid steganographic technique that can be used is the combination of LSB and DCT algorithms. LSB technique has low invisibility and robustness while DCT has high invisibility and medium robustness. The MSE value of DCT is low but LSB has a medium MSE value. Therefore, the combination of DCT and LSB techniques can reduce the drawbacks of using those algorithms separately.

5. Conclusion

Cloud security is a subset of cybersecurity that deals with policies, procedures, and technologies for safeguarding cloud computing systems. It protects data in the cloud and other digital assets from data breaches, distributed denial of service (DDoS), hacking, malware, and other cyber threats. This paper suggested using cryptography along with steganography to provide high-level security to the confidential data inside the cloud platform. Moreover, this paper discussed the concept of cryptography, the performance of different symmetric and asymmetric key cryptographic algorithms, the concept of steganography, and the performance of different steganographic techniques. The facts discussed above proved that the blowfish algorithm has better performance when compared with other symmetric key cryptographic algorithms (DES, AES, 3-DES, and RC5 algorithms). In addition, the ECC algorithm has better performance when compared with other asymmetric key cryptographic algorithms (RSA, ECC, Diffie-Hellman, El Gamal, and DSA algorithms). Furthermore, it can be concluded that the combination of LSB and DCT image steganographic techniques can provide extraordinary security when hiding the file inside a cover image. The blowfish symmetric key cryptographic technique and the ECC and RSA asymmetric cryptographic algorithm can be combined as a hybrid cryptosystem to perform double encryption to secure the data. Then LSB and DCT image steganographic techniques can be combined to create a multilayer steganographic algorithm to hide the encrypted file to provide extra security. This proposed system will provide

availability, integrity, authenticity, confidentiality, and non-repudiation to the data and information at same time.

References

E. Elgeldawi, M. Mahrous, and A. Sayed, 'A Comparative Analysis of Symmetric Algorithms in Cloud Computing: A Survey', *Int. J. Comput. Appl.*, vol. 182, no. 48, pp. 7–16, Apr. 2019, doi: 10.5120/ijca2019918726.

C. Biswas, U. D. Gupta, and Md. M. Haque, 'An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography', in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Cox'sBazar, Bangladesh, Feb. 2019, pp. 1–5. doi: 10.1109/ECACE.2019.8679136.

S. Vyakaranal and S. Kengond, 'Performance Analysis of Symmetric Key Cryptographic Algorithms', in *2018 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, Apr. 2018, pp. 0411–0415. doi: 10.1109/ICCSP.2018.8524373.

S. Shakti, 'International Journal in Multidisciplinary and Academic Research (SSIJMAR) Vol. 4, No. 1, February 2015 (ISSN 2278 – 5973)',
p. 6.

K. Jaspin, S. Selvan, S. Sahana, and G. Thanmai, 'Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm', in *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, Pune, India, Mar. 2021, pp. 791–796. doi: 10.1109/ESCI50559.2021.9397005.

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

A. Y. AlKhamese, W. R. Shabana, and I. M. Hanafy, 'Data Security in Cloud Computing Using Steganography: A Review', in *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*, Aswan, Egypt, Feb. 2019, pp. 549–558. doi: 10.1109/ITCE.2019.8646434.

S. Chandran and K. Bhattacharyya, 'Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography', in *2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO)*, Visakhapatnam, Jan. 2015, pp. 1–5. doi: 10.1109/EESCO.2015.7253657.

A. Singh, M. Chauhan, and S. Shukla, 'Comparison of LSB and Proposed ModifiedDWT Algorithm for Image Steganography', in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida (UP), India, Oct. 2018, pp. 889–893. doi: 10.1109/ICACCCN.2018.8748546.

A. G. Palathingal, A. George, B. A. Thomas, and A. R. Paul, 'Enhanced Cloud Data Security using Combined Encryption and Steganography', vol. 05, no. 03, p. 4.

D. Naidu, A. K. K S, S. L. Jadav, and M. N. Sinchana, 'Multilayer Security in Protecting and Hiding Multimedia Data using Cryptography and Steganography Techniques', in *2019 4th International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, Bangalore, India, May 2019, pp. 1360–1364. doi: 10.1109/RTEICT46194.2019.9016974.

H. B. MaciT, A. Koyun, and O. Güngör, 'A REVIEW AND COMPARISON OF STEGANOGRAPHY TECHNIQUES', p. 9.

P. Nicholson, "AWS hit by Largest Reported DDoS Attack of 2.3 Tbps," A10 Blog, June 24, 2020.

C. Cimpanu, "Microsoft said it mitigated a 2.4 Tbps DDoS attack," The Record, 2021

A. HOPE, "Hackers Use Compromised Google Cloud Accounts for Cryptocurrency Mining," CPOMagazine, 2021.

N. Goud, "IBM says more than 8.5 billion records were leaked in Cyber Attacks," Cybersecurity Insiders.

R. Staff, "Hackers attack 20 million accounts on Alibaba's Taobao shopping site," Reuters , 2016.

R. Whiting, "Oracle's Micros Point-Of-Sale Systems Hit With Security Breach," CRN

Acknowledgment

This research was supported by General Sir John Kotelawala Defence University, we would like to pay our gratitude to all the lecturers at the Faculty of Computing for the guidance provided throughout this research.

Author Biographies

AKSA Anudini is a final-year undergraduate of General Sir John Kotelawala Defence University. Following the BSc (Hons) Computer Science Degree Programme. Studied at Sanghamitta Balika Vidyalaya, Galle.

Gayamini Gnanasuganthan working as a Lecturer (Prob.) in the Department of Computer Engineering, Faculty of Computing, General Sir John Kotelawala Defence University. This author was awarded the M.Sc. degree in Computer Science and Technology from Wuhan University of Technology, Wuhan, P.R. China in the year 2020. Her current research interests lie in Artificial Intelligence, Multi-agent systems, Machine Learning, IoT and Robotics.
& Automation.

Prof. Thushara Lanka Weerawardane was graduated in Electrical Engineering from the University of Moratuwa in 1998 and consequently he received MSc Degree “Communication and Information Technology” in 2004 and received Ph.D. from the University of Bremen, Germany in 2010. Currently, Prof. Thushara Lanka Weerawardane worked in Kotelawala Defence University as senior lecturer Gr.1 from 2012 to 2016 during this period he held several academic and administrative positions such as Head of the Department and Dean, Faculty of Engineering. Currently, he is working in Kotelawala Defence University as a Professor.