# A Hybrid Framework for Security in Cloud Computing Based on Different Algorithms

Jannatul Ferdous[1], Md. Fuad Newaz Khan[1], Karim Mohammed Rezaul[2], Maruf Ahmed Tamal[1], Md. Abdul Aziz[1], and Pabel Miah[1]

*(Corresponding author: Karim Mohammed Rezaul)*

Department of Computer Science & Engineering, Daffodil International University, Bangladesh[1]
Faculty of Arts, Science & Technology, Wrexham Glyndŵr University[2]
Mold Rd, Wrexham LL11 2AW, United Kingdom
(Email: rezababu@gmail.com)

*(Received Sept. 12, 2019; Revised and Accepted Jan. 3, 2020; First Online May 2, 2020)*

## Abstract

Cloud computing is the concept used to decode Daily Computing Issues. It is essentially a virtual pool of resources and also provides these tools to customers through the Internet. It is the net-based advancement and utilized in computer technology. The widespread problem connected with cloud computing is information privacy, protection, anonymity, and dependability, etc. However, the main issue involving them is safety and how the cloud supplier guarantees it. Securing the cloud means to secure the treatments (calculations) and storage (databases hosted by the Cloud provider). The paper reviews concurrent articles on security in cloud computing. By conducting research, we have managed to identify and analyze different security issues associated with the cloud as well as various cryptographic algorithms adaptable to better security for the cloud, and based on those algorithms, we have proposed a hybrid framework for security in cloud computing.

*Keywords: AES; Cloud Coputing; DES; Security Attack; Steganography*

## 1 Introduction

Cloud computing is a paradigm of information technology that provides scalable on-demand computing services such as computing, storage, network, software, and much more on the Internet [2] this enables businesses and organizations to concentrate their efforts on their key company or activity by outsourcing their IT resources [4, 27, 28]. This new technology offers many benefits such as cost efficiency, enhanced storage ability, backup and recovery, ongoing accessibility of resources and independence of location [9, 12]. Even though Cloud computing (CC) isn't entirely new, traction between organizations and individual users is still profiting. Transition into the cloud surroundings, however, isn't straightforward, and lots of operational and security problems exist.

The usage of a hypervisor and Virtual Machine (VM) technology is also a security problem since these and VM technology is vulnerable to VM level attacks. These programs have quite a few onsite computer organizations that might have a massive number of hardware and software systems. Vulnerabilities in VM infrastructure could be exploited by attackers to exfiltrate data or conduct attacks like DDoS (Distributed Denial of Services) [11,24]. This is a result of the inherent flaws in the TCP / IP stack. Additionally, several new strikes have emerged lately which use polymorphism and Metamorphosis to violate detection.

Attackers can inject kernel scripts into the server operating system (OS), and as all guest OS runs their OS with this kernel, attackers can command all VMs. Moreover, by successfully exploiting known or zero-day vulnerabilities in the hosted VM, the attackers may then obtain access to the host's VMs because the hypervisor shares the hardware and applications in the common virtual environment. Some hypervisors supply APIs which leave the VM facility entirely observable to Traffic however, these APIs provide additional paths for attackers to see and exploit network communication. Additionally, there are other strikes Such as information intrusion, information availability and data integrity targeting CC. Whenever consumers depend on these sides, information that is stored in the cloud is not reliable. Thus, nowadays users themselves are engaged in the process of encrypting their sensitive data before sending it for storage to the cloud [1, 18].

To demonstrate this, Gartner [10] predicts that 92% of workloads will be processed by cloud information centers by 2020. Cloud workloads are expected to rise 3.2 times over the same time, Cisco predicts [6]. However, the main drawback of this technology comes with the loss of control over the cloud infrastructure. Individuals, businesses and organizations, therefore, resist the adoption of pub-

lic clouds because of security and privacy concerns [5,19]. Recent cloud attacks, like the one in 2014 when Dropbox's 50 million user accounts were hacked which makes data security a hot topic.

## 2 Related Works

Cryptography is the main technique to secure data on clouds so that no one can steal our data and use it somewhere else or abuse it. Cloud computing confronts today's most common major issues with data integrity and confidentiality [25]. Cloud users store their information in different storage systems that cloud vendors provide. The problem, however, is that the user does not comprehend where the information is stored and has no control over it. Data acquisition is a technique or process of acquiring information from different hardware.

Cloud consumers and service suppliers should be acquainted with the information flow and Peer to Peer operations [20], how and where we access the data. For customers to collect their personal or confidential information in the cloud, data confidentiality is crucial. It's one of the major issues on the cloud. Cloud information is stored in remote places and cloud infrastructure used by providers to store information such as VM machine (image), copy and track logs or servers [20]. To divide the information and program, the client uses the shared storage. Due to attack, malicious action, and system failure, confidentiality problems sometimes arise. Hence, we want great safety processes and methods for fastening delicate information, unsecured transmission or storage. Ethics and Authenticity are another cloud security problem.

Integrity of information implies the provision of information from unauthorized deletion, production or modification. In standalone programs and databases, data integrity is easy; however, in cloud cases, it is hard because cloud suppliers work with countless databases, software, servers, and networks [26]. Authenticity refers to the practice of monitoring data and information accessibility. Only those consumers access the information that the supplier approves. Cloud is a data supply accessible, so many consumers have been facing the problem of permission and accessibility of information for a while. On the other hand, multi-tenancy indicates where computing tools, storage, services, and network shared by cloud technologies. It is a cost saving and provides better resource utilization. However, due to its data confidentiality due to shared resources, it is harmful. Many malicious activities ruin servers and community instruments, so it is not hard to control the flow of information or data (leakage). One of the following problems using multi-tenancy is a digital machine strike. Enhancing technologies and using networks provide people with a lot of equipment. It also improves many security issues, though; cyber-attack is just one of these.

Cyber-attacks use malicious code to alter computer code or information, resulting in damaging impacts that can undermine data and lead to cyber-crimes, including information and identity theft. Vulnerabilities of Shared Techniques make the cloud so intriguing is also a safety criticality point. As Navati et al. [23] showed that, attackers in the hypervisor could exploit vulnerabilities and achieve access to the physical host where other nearby virtual machines (VM) are located. Data from users can suffer from both accidental data loss and intrusive malicious behavior. Data loss is beyond the scope of this job, as we only consider data breaches here, i.e. stealing sensitive data (such as private or credit card details) [7]. A user can lose control over their own accounts. This enables the intruder to get into critical areas of a deployed service and possibly compromise the confidentiality, integrity, and availability of those services [7].

Denial of Service (DoS) is one of the most alarming scenarios is when the cloud infrastructure is made unavailable (just think that an outage costs Amazon 66 K dollars per minute). DoS in a cloud context is even more dangerous than in a traditional one since when the workload increases concerning a specific service, the cloud environment provides additional computational power to that service. This means that on the one hand, the cloud system counters the effects of the attack, but on the other hand, it supports the attacker in his evil activity, by providing him with more resources [8]. Malicious Insiders raise the list of top threats from the cloud. The chance of an insider being malicious – e.g. a worker possibly trying to take advantage of his privileged situation to access delicate data is becoming increasingly concrete and worrying [16].

## 3 Proposed Hybrid Model for the Security of Data

The algorithms emphasized in this research are: DSA (Digital Signature Algorithm), AES (Advanced Encryption Standard), and Steganography (hiding data behind an audio file or image).

**DSA.** The U.S. launched the Digital Signature Algorithm (DSA) in 1994. Digital signatures are extremely essential in the contemporary world to check the sender's identity. A digital signature is a digital signature that's used for confirmation and authentication of information. An electronic signature is represented as a series of binary digits in the pc system. The touch includes a set of parameters and rules (algorithm) like the identity of the individual signing the document in addition to the creativity of this information could be confirmed. The signature is created with the support of a personal key. A private key is known only to the sender. The signature is verified by the recipient using a public key that corresponds to the private key. A digital signature may be used with any sort of data, whether it's encrypted or not. Digital signatures are utilized to

detect unauthorized alterations of information by the third party. Additionally, the recipients of a digitally signed record assure that the record assigned by the person who it is promised to be signed up by. That is known as non-repudiation since the person who signed the record can't repudiate the signature afterward. Digital signature algorithms may be utilized in e-mails, electronic funds transfer, software distribution, data storage which guarantee the integrity, validity, and creativity of information. A hash function is being used in the signature generation process to get a condensed version of information, called a message digest [13].

**AES.** The Advanced Encryption Standard (AES) is the U.S. established electronic information encryption specification. National Standards and Technology Institute (NIST) in 2001 [3]. AES is based on a design principle known as a replacement-permutation network, combining both replacement and permutation, and is quick in both software and hardware [17]. Once DES was used as an encryption standard for over 20 years and it had been able to be deciphered in a relative short Quantity of time, NIST (United State National Institute of Standard and Technology) Chose a new Benchmark, the Advanced Encryption Standard (AES), had to be put into Position. AES is based on Rijndael cipher. AES was embraced by the US government and is popular nowadays. This decision was announced in January 1997, along with a petition for AES candidates had been created. The AES was to be a symmetric block cipher algorithm supporting keys sizes of 128-, 192-, and 256-bit keys. AES is based on substitution and permutation networks. It doesn't utilize the Feistel network. It's more secure than DES and difficult to crack. AES is much more complicated than DES, but it's quick and very effective. It operates with 128-bit fix block size plain text and version key sizes.

**Steganography.** Steganography is the science of concealing messages in this manner that nobody aside from the intended recipient knows of the presence of the message. Steganography is the practice of concealing just one medium of communication (text, audio or picture) in another. The term steganography comes from the Greek Steganos (covered or secret) and graphy (drawing or writing), and therefore it means, coated writing. Steganography is the tradition of encoding secret data in a way like the very existence of the info is hidden under the picture or picture in which it's hidden. Throughout history, many steganography techniques are recorded, for example, usage of cleverly-chosen words, invisible ink composed between traces, modulation of word or line spacing, and microdots. Normally the secret information is hidden by using an innocuous cover to arouse no distress to anybody. Edge of steganography over cryptography is that the key message doesn't draw attention to itself because the message could be hidden under picture file, video file, etc. [15].

There are various techniques available for steganography which are as follows:

1) Data hiding within wax pill;
2) Data hiding within noisy picture;
3) Hidden messages beneath sterile portion of some other message;
4) Data concealing inside a sound file;
5) Data concealing beneath video file.

# 4 The Proposed Scheme

## 4.1 Design of Proposed Framework

Figure 1 represents our framework's working process. At first, it will use DSA to create a digital signature, then it will use AES to encrypt the data of the user and to increase the security we have used steganography.

## 4.2 Elaboration of Overall System

There are some steps of the proposed scheme:

**Step 1.** Applying DSA for Generating Digital Signature:
A digital signature is a mathematical method used to validate a message, software or digital document's authenticity and integrity. A digital signature offers much more inherent security as the digital equivalent of a handwritten signature or stamped seal and is intended to solve the problem of manipulation and impersonation in digital communications.

The algorithm used for creating this signature is given Algorithm 1 [14].

**Algorithm 1** DSA for Signature Creation

1: Input: Domain parameters $(p, q, g)$; signer's private key $a$; message-to-be-signed $M$, with message digest $h = Hash(M)$.
2: Output: Signature $(r, s)$.
3: Choose a random $k$ in the range $[1, q-1]$.
4: Compute $X = g^k \bmod p$ and $r = X \bmod q$.
5: **if** r = 0 (unlikely) **then**
6: go to Step 3.
7: **end if**
8: Compute $k^{-1} \bmod q$.
9: Compute $h = Hash(M)$.
10: Compute $s = k^{-1}(h + ar) \bmod q$.
11: **if** $s = 0$ (unlikely) **then**
12: go to Step 3.
13: **end if**
14: Return $(r, s)$.

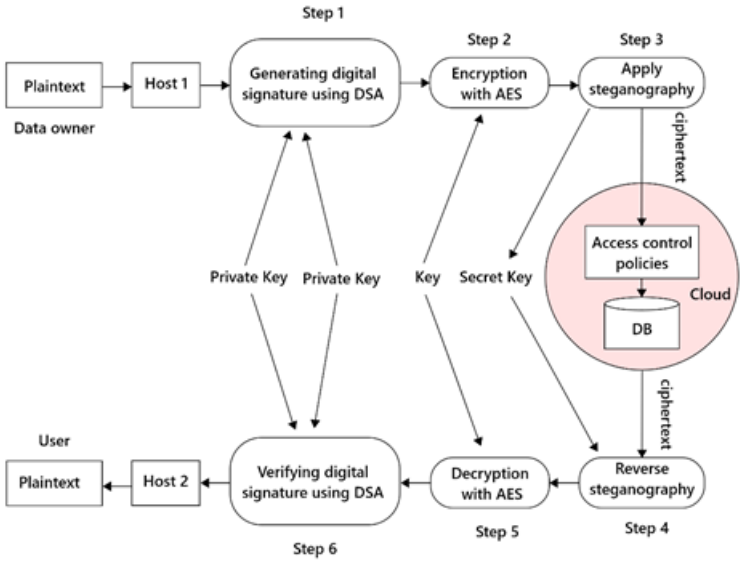


Figure 1: A hybrid framework for security in cloud computing

**Step 2.** Applying AES for Encryption:
AES is not a Feistel cipher, but an iterative one. It is based on the 'network of substitution – permutation'. It includes a series of linked operations, some of which involve replacing inputs with specific outputs (substitutions) and others involve shuffling bits (permutations) around them. Interestingly, AES performs all its computations on bytes rather than bits. AES therefore treats the 128 parts of the plaintext block as 16 bytes. These 16 bytes are arranged for matrix processing in four columns and four rows. The number of rounds in AES, unlike DES, is variable and depends on the key length. For 128-bit keys, AES utilizes 10 rounds, for 192-bit keys 12 rounds and 256-bit keys 14 rounds. Each round utilizes another 128-bit round key calculated from the initial AES key.

**Step 3.** Applying Steganography for Encryption:
Figure 2 shows a general structure for encryption using steganography. It is presumed that the sender wants to send a signal to a receiver through Steganographic transmission. The sender begins with a cover message, in which the integrated message is concealed, which is an input to the stego system. The message concealed is called the message integrated. A Steganographic algorithm combines the cover massage with the e1mbedded message, which is something to hide in the cover. The algorithm may or may not use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process [22].

**Step 4.** Applying Steganography for Decryption:
Usually, the same (or linked) key is required to retrieve the integrated massage. The Steganographic

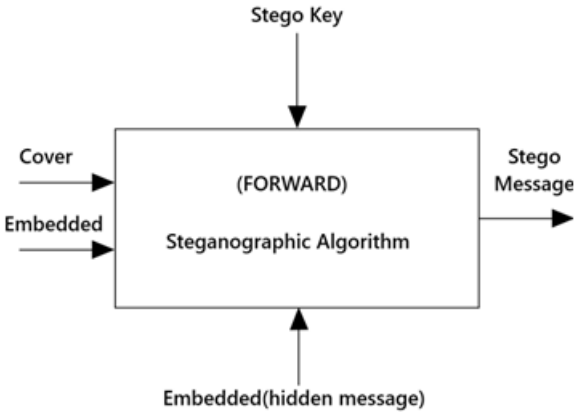


Figure 2: Encryption using steganography [21]

algorithm's output is the message of stego. The cover massage and stego text must be of the same sort of information, but another sort of information may be the integrated message. To extract the embedded signal, the receiver reverses the embedding process [22]. Figure 3 shows a general process of reverse steganography.

**Step 5.** Applying AES for Decryption:
The cipher text we got from Step 2 will have to be decrypted in this step by using AES again.

**Step 6.** Applying DSA for Verifying the Digital Signature:
The signature we created in Step 1 will have to be verified by using DSA in this step. Otherwise, the data will be lost.

The algorithm used for verifying this signature is

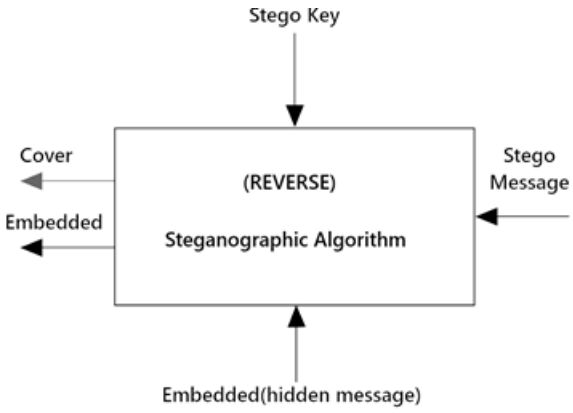


Figure 3: Decryption using steganography [21]

given in Algorithm 2 [14].

**Algorithm 2** Reverse DSA

1: Input: Domain parameters $(p, q, g)$; signer's public key $A$; signed message $M$; message digest $h = Hash(M)$; signature $(r, s)$.
2: Output: Accept or Reject.
3: **if** $r, s \notin [1, q-1]$ **then**
4: return "Reject"
5: stop.
6: **end if**
7: Compute $w = s^{-1} \bmod q$.
8: Compute $h = Hash(M)$.
9: Compute $u_1 = hw \bmod q$ and $u_2 = rw \bmod q$.
10: Compute $X = g^{u_1} A^{u_2}$.
11: **if** $v = r$ **then**
12: return "Accept"
13: **else**
14: return "Reject".
15: **end if**

### 4.3 How the Data will be Secured in Our System

In our hybrid framework, in the 1st step, we will create a digital signature using DSA to verify the owner of the data, then in the 2nd step that data will be encrypted by AES algorithm which is the best cryptographic algorithm since time, and then in the 3rd step, that encrypted data will be again encrypted using STEGANOGRAPHY for an extra layer of security.

From the 4th step, our system will start to reverse the whole process to get the original data. In the 4th step, it will reverse the data through reverse STEGANOGRAPHY to get the encrypted file from Step 2 and then it will decrypt that data using AES again in Step 5 to get the original data afterward in the 6th step or in the final step, it will verify the data using reverse DSA again to verify the owner of that data.

## 5 Future Work and Conclusion

Data security is the most important issue of cloud computing in the IT industry. Future work includes implementing Digital Signature Algorithm (DSA), Advanced Encryption Standard (AES) and STEGANOGRAPHY to provide maximum security in cloud computing. By implementing these three algorithms, it is possible to provide authenticity, security and data integrity to data. We hope this work helps secure data from outsiders or hackers, who try to access and destroy the important data. We have located that the Time complexity is high because it is a one by one process, but in the future, this time complexity could be reduced. We will carry on this research in order to improve the functionalities of these algorithms in terms of robustness, reducing time complexity, hiding capacity and use other security algorithms or methods to protect information (data) on the cloud.

For many Internet facilities, cloud computing provides a flexible and cost-effective alternative. The contemporary sector of IT is focused entirely on online service or Internet facilities. This article outlines security problems along with cloud computing techniques and how they can be averted. Here we use techniques of cryptography and steganography together to protect information. Algorithms for DSA and AES are somewhat more secure than other algorithms. In order to give more data protection, we integrate AES and DSA with steganography. We get an encoded image in the steganography operation in which the human eye looks exactly the same as the initial image. While studying the binary picture codes, we could see the differences. Otherwise, the original picture cannot be spotted. The suggested hybrid framework for cloud computing security can facilitate to create a strong data security structure in the cloud computing region or the Internet.

## References

[1] D. I. G. Amalarethinam, H. M. Leena, "Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud," in *World Congress on Computing and Communication Technologies (WCCCT'17)*, pp. 172-175, 2017.

[2] D. R. Bharadwaj, A. Bhattacharya, M. Chakkaravarthy, "Cloud threat defense – A threat protection and security compliance solution," in *IEEE International Conference on Cloud Computing in Emerging Markets (CCEM'18)*, pp. 95-99, 2018.

[3] B. M. Belkaid, L. Mourad, C. Mehdi, "Meteosat Images Encryption based on AES and RSA Algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 6, pp. 203-208, 2015.

[4] C. A. B. D. Carvalho, R. M. D. C. Andrade, M. F. D. Castro, E. F. Coutinho, N. Agoulmine, "State of the art and challenges of security SLA for cloud

computing," *Computers and Electrical Engineering*, vol. 59, pp. 141-152, 2017.

[5] V. Casola, A. D. Benedictis, M. Rak, "On the adoption of security slas in the cloud," *Lecture Notes in Computer Science*, vol. 8937, pp. 45-62, 2015.

[6] Cisco, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update*, Dec. 17, 2019. (https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html)0

[7] L. Coppolino, S. D'Antonio, G. Mazzeo, L. Romano, "Cloud security: Emerging threats and current solutions," *Computers and Electrical Engineering*, vol. 59, pp. 126-140, 2017.

[8] R. V. Deshmukh, K. K. Devadkar, "Understanding DDos attack & its effect in cloud environment," *Procedia Computer Science*, vol. 49, pp. 202– 210, 2015.

[9] M. A. Fera, C. Manikandaprabhu, I. Natarajan, K. Brinda, R. Darathiprincy, "Enhancing security in Cloud using trusted monitoring framework," *Procedia Computer Science*, vol. 48, pp. 198-203.

[10] Gartner, *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020, Nov. 13, 2019.* (https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020)

[11] Y. Gilad, A. Herzberg, M. Sudkovitch, M. Goberman, "CDN-on-Demand: An affordable DDoS defense via untrusted clouds," in *Proceedings 2016 Network and Distributed System Security Symposium*, 2016.

[12] W. F. Hsien, C. C. Yang and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133-142, 2016.

[13] M. S. Hwang, C. C. Lee, J. L. Lu, "Cryptanalysis of the Batch Verifying Multiple DSA-type Digital Signatures", *Pakistan Journal of Applied Sciences*, vol. 1, no. 3, pp. 287-288, 2001.

[14] D. Ireland and DI Management Services Pty Limited, *Public key cryptography using discrete logarithms. Part 4: Digital Signature Algorithm (DSA)*, Aug. 22, 2019. (https://www.di-mgt.com.au/public-key-crypto-discrete-logs-4-dsa.html)

[15] S. S. Iyer, K. Lakhtaria, "New robust and secure alphabet pairing text Steganography Algorithm," *International Journal of Current Trends in Engineering & Research*, vol. 2, no. 7, pp. 15–21, 2016.

[16] M. Kandias, N. Virvilis, D. Gritzalis, "The insider threat in cloud computing," *Lecture Notes in Computer Science*, vol. 6983, pp. 93–103, 2013.

[17] S. Kulkarni, "Study of Modern Cryptographic Algorithms," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 3, pp. 97-103, 2017.

[18] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing", *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[19] J. Luna, N. Suri, M. Iorga and A. Karmel, "Leveraging the Potential of Cloud Security Service-Level Agreements through Standards," *IEEE Cloud Computing*, vol. 2, no. 3, pp. 32-40, 2015.

[20] M. V. Malakooti and N. Mansourzadeh, "A Two Level-Security Model for Cloud Computing based on the Biometric Features and Multi-Level Encryption," in *International Conference on Digital Information Processing, Data Mining, and Wireless Communications(DIPDMWC'15)*, pp. 100-111, 2015.

[21] A. W. Naji, S. A. Hameed, B. B. Zaidan, W. F. Al-Khateeb, O. O. Khalifa, A. A. Zaidan and T. S. Gunawan, "Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques," *International Journal of Computer Science and Information Security*, vol. 3, no. 1, 2009.

[22] A. W. Naji, A. A. Zaidan, B. B. Zaidan, S. A. Hameed and O. O. Khalifa, " Novel Approach of Hidden Data in the Unused Area 2 within EXE File Using Computation Between Cryptography and Steganography," *International Journal of Computer Science and Network Security*, vol.9, no.5, pp. 294-300, 2010.

[23] M. Nanavati, P. Colp, B. Aiello, A. Warfield, "Cloud security: a gathering storm," *Communications of the ACM*, vol. 57, no. 5, pp. 70–79, 2014.

[24] O. Osanaiye, K. K. R. Choo, M. Dlodlo, "Distributed denial of service (Ddos) resilience in cloud: Review and conceptual cloud Ddos mitigation framework," *Journal of Network and Computer Applications*, vol. 67, pp.147-165, 2016.

[25] V. K. Pant, J. Prakash, A. Asthana, "Three step data security model for cloud computing based on RSA and steganography techniques," in *International Conference on Green Computing and Internet of Things (ICGCIoT'15)*, pp. 490-494, 2015.

[26] V. K. Pant, Mr. A. Saurabh, "Cloud security issues, challenges and their optimal solutions," *International Journal of Engineering Research & Management Technology*, vol. 2, no. 3, pp. 41-50, 2015.

[27] S. Rezaei, M. A. Doostari, M. Bayat, "A lightweight and efficient data sharing scheme for cloud computing," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 115–131, 2018.

[28] C. Yang, Q. Chen, Y. Liu, "Fine-grained outsourced data deletion scheme in cloud computing," *International Journal of Electronics and Information Engineering*, vol. 11, no. 2, pp. 81–98, 2019.

# Biography

**Jannatul Ferdous** was born in Chattogram, Bangladesh in 1997. He received the B.Sc. degree in Computer Science and Engineering department from Daffodil Interna-

tional University, in 2019.His research interests include information security, cloud security, data analysis based on the machine learning algorithm.

**Md. Fuad Newaz Khan** was born in Dhaka, Bangladesh in 1996. He received the B.Sc. degree in Computer Science and Engineering department from Daffodil International University, in 2019.His research interests include information security, cloud security, data analysis based on the machine learning algorithm.

**Karim Mohammed Rezaul** was awarded a PhD degree in Computing and Communications Technology from North East Wales Institute (NEWI) of Higher Education (presently Glyndŵr University), University of Wales, UK in October 2007. He received his BSc. degree in the field of Naval Architecture and Marine Engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka in 1998 and, MSc. degree in Marine Technology from Norwegian University of Science and Technology (NTNU), Trondheim, Norway in 2001. In February 2002, Dr. Karim was appointed as a visiting lecturer in the department of Computing, Communications Technology and Mathematics at London Metropolitan University, and continued until June 2005. Presently, he is a Visiting Professor of Computing & Communications Technology at Wrexham Glyndwr University, UK and Adjunct Professor in Management at IPE Management School Paris, France. Since 2002, Prof. Karim has been working as an Academic advisor and Programme director of various International colleges in UK. Prof. Karim is a member of the Institute of Electrical and Electronics Engineers (IEEE), Association for Computing Machinery (ACM), Centre for Applied Internet Research (CAIR, UK), and a fellow of the Institution of Engineers Bangladesh (IEB, Bangladesh). He is the founder and director of Applied Research Centre for Business and Information Technology (ARCBIT) UK, Global Academy of Professionals (GAP) UK, Centre for Applied Research in Software and IT (CARSIT) Bangladesh, and Centre for Applied Research in Business, IT & Engineering (CARBITE) Bangladesh.

Prof. Karim is an author of a numerous Scientific and Business articles (Scholarly & Refereed publications) which include book, book chapters, journals and International conference papers. He is an editor of several international journals and member of the Technical Program Committee (TPC) of multiple International conferences. His research interests include IS Design and Development; ICT-based Pedagogy; Internet of Things (IoT); Artificial Intelligence (AI); Fractals and Nanotechnology; Data Science; Networking - Traffic Engineering, Quality of Service (QoS) Control, Traffic modelling & simulation etc.; Distributed DBMS; Information Security; Business Intelligence; E-Business/E-commerce; ICT Project Management; Computing.

**Maruf Ahmed Tamal** was born in Barishal, Bangladesh in 1996. He received the B.Sc. degree in Computer Science and Engineering department from Daffodil International University, in 2019.His research interests include Machine Learning, Data mining and Pedagogy.

**Md. Abdul Aziz** was born in Rajshahi, Bangladesh in 1995. He received the B.Sc. degree in Computer Science and Engineering department from Daffodil International University, in 2019.His research interests include information security, cloud security, data analysis based on the machine learning algorithm.

**Pabel Miah** was born in Tangail, Bangladesh in 1997. He received the B.Sc. degree in Computer Science and Engineering department from Daffodil International University, in 2019.His research interests include information security, cloud security, data analysis based on the machine learning algorithm.