Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, August 2021: 5936-5945

Security Aware Cryptography Approaches on the Internet of Things (IoT) including Military Applications: A Review

[1]Pushpinder Singh, [2]Sukhpreet Kaur
[1]Assistant Professor, [2]Research Scholar
[1]University College Ghanaur (Patiala), India
[2]Punjabi University, Patiala

Abstract

With the huge incidents of terrorist attacks and sniffing of security personnel, there is a need to integrate the higher degree of security in the defense vehicles. The key modus operandi by terrorists is that they intrude bypassing the security devices because of the vulnerabilities in the scenarios. In such a manner, to ensure sight and sound substance, cryptology, which has all the earmarks of being a compelling path for data security, has been utilized in numerous handy applications. In this manuscript, the key mechanisms related to cryptography and dynamic encryption are presented which can be used so that the defense personnel can communicate with each other with a higher degree of security, privacy, and anti-sniffing attempts. This paper presents the cryptography and hash-based approaches on assorted parameters with key features and the availability of specific secured implementations. The paper presents the assorted approaches and algorithms which can be integrated into the laser-guided defense weapons as well as vehicles so the overall communication will be secured.

Keywords: Cryptography, Defense Security, Encryption, Internet of Things, Network Security, Wireless Security

1. Introduction

India has been one of the key victims as far as the terrorist attacks are concerned and the numbers of such attempts are very high for last ten years. The security forces and law enforcement agencies are developing and launching the high security weapons to guard their regions still this area is under research and needs higher efficiency protocols.

Various values in the following Table 1 depict the incidents of enormous terrorist attacks in India. There is need to work out and address the specific implementations so that such incidents can be avoided.

Table 1: Incidents of Terrorist Attacks in India

(Source: National Consortium for the Study of Terrorism and Responses to Terrorism. (2018). Global Terrorism Database)

Year	Deaths	Injuries	Number of incidents
2017	470	702	1000
2016	467	788	1,025
2015	387	649	884
2014	490	776	860
2013	467	771	694
2012	264	651	611
2011	499	730	645
2010	812	660	663

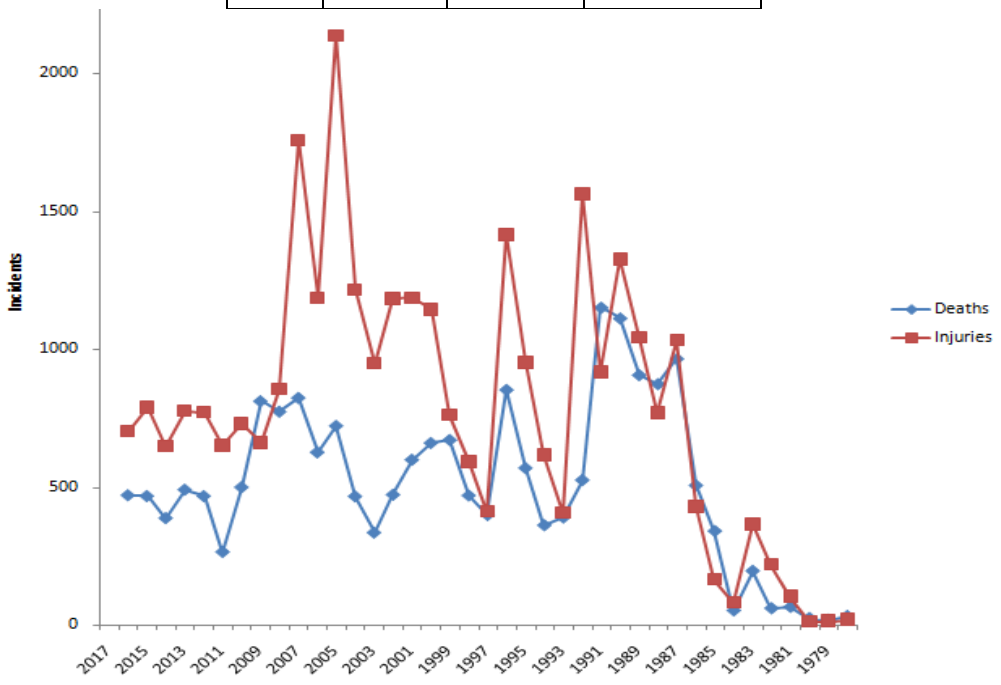

Figure 1: Incidents of Terrorist Attacks in India

2. Need of Cryptography

The domain of network security associated approaches of cryptography and hash functions are quite enormous and there is huge need of research as there are so many weakness issues from arranged sources and channels. In this research manuscript, the focus towards the network environment is taken with the case analysis of diversified works by researchers in the segment of the Internet of Things (IoT). IoT is solely based on the sensor-based technologies in which the need to integrate the security is of paramount importance. In a wireless system including advance situations, a key exchange process is pursued with the dynamic cryptography includes so the whole system condition can be made anchored. This manuscript is having the extensive audit on research points of the methodologies used

for security. In IoT, the items are associated with one another utilizing wireless correspondences and there is to relate the exceptionally useful methodologies for cryptography in the wireless condition for anchored trust-based transmission. In this research manuscript, different measurements and parts of cryptography are given the proposed use and joining with the very efficacious methodologies of quantum cryptography that is increasing colossal distinction and the unmistakable quality in the area of information encryption and anchored transmission utilizing cryptography.

The wireless communication has increased tremendous development in innovation in different spaces since its commencement in year 1880 when A. Graham Bell and C. S. Spoiler protected photophone. In the underlying time of the advent of wireless advances, it was utilized for individual communications. Presently days, the wireless innovation is dealing with various frequencies to meet the applications for corporate, individual and protection. The wireless communication relies upon the radio innovation and related grouped angles for compelling and anchored information transmission. There are various viewpoints of wireless communication, including wireless sensor systems, mobile ad hoc systems, Wi-Max and numerous others. To execute the higher level of security, system administrators actualize the cryptography and dynamic encryption, so the general communication can be made anchored with no sniffing endeavors.

3. Cryptography and Related Perspectives

Cryptography alludes to the methodologies and procedures which are produced and executed for anchored communication for explicit channels. It is traditionally connected with encryption ways to deal with secure the general transmission. Security targets can be actualized by applying cryptographic devices, for example, encryption or message confirmation plans.

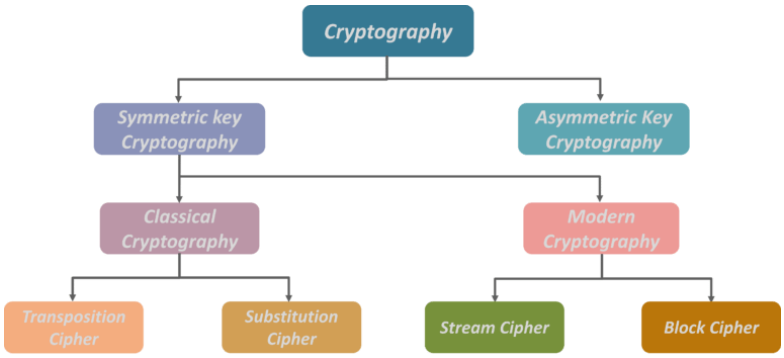

Figure 2: Cryptography Approaches and Related Fragments

3.1 Symmetric Key Cryptography

The symmetric key based implementation is having the integration of same keys that is shared in the channel so that the communication can be made secure, but it might be less integrity aware of the specific scenarios of implementations. Data Encryption Standard (DES) is the most common and prominently used approach of symmetric key based encryption.

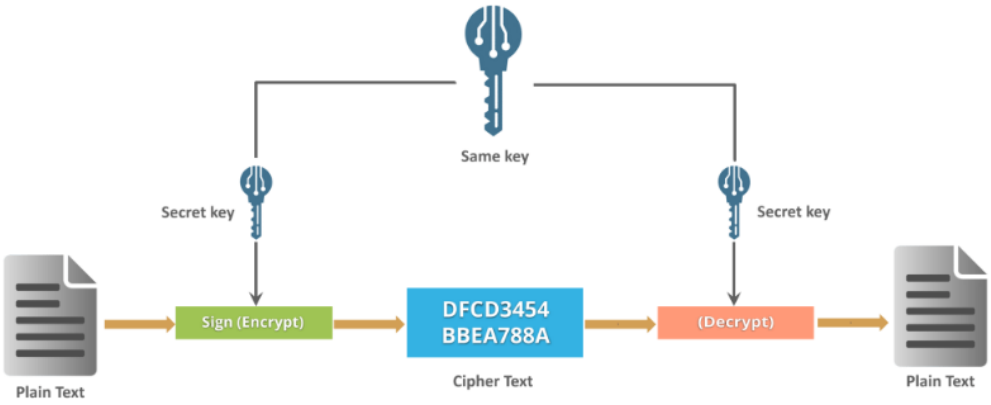

Figure 3: Symmetric Encryption

Transposition Ciphers

The transposition cipher-based implementation of security is the encryption approach whereby transpose operations in the matrix format are implemented and thereby the permutations are generated in the text so that the higher degree of security and integrity can be enforced.

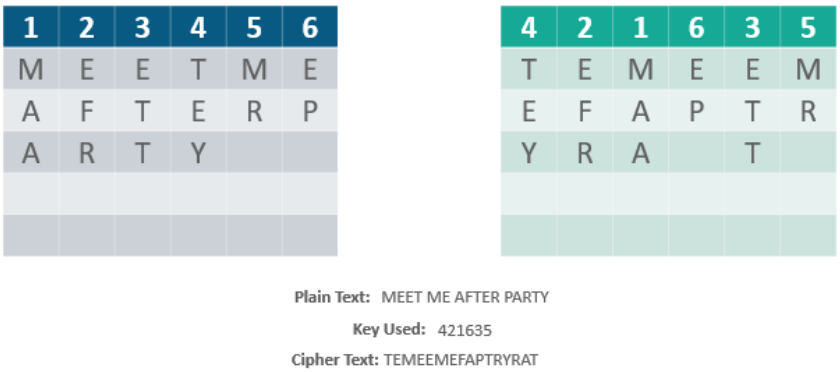

Figure 4: Transposition Ciphers

Substitution Cipher

In this approach, the units of the letters of characters are replaced with the other characters and then the further encryption is done to have the higher degree of security and encryption, but now days it is very common and not fit for the high security implementations.

Figure 5: Substitution Encryption

Stream Cipher

The stream cipher is more dependent on the time span based analytics of the characters and then to have the encryption. In this approach, the plaintext or byte is encrypted in different time spans with the association of the security keys for the encryption.

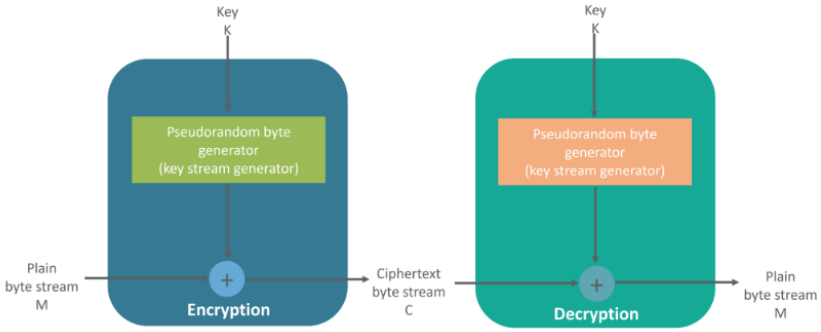

Figure 6: Stream Encryption

Block Cipher

The approach of block cipher makes use of the deterministic approach of algorithm thereby with the integration of symmetric key and to have the integration of block-based encryption rather than the security in the character streams in character by characters.

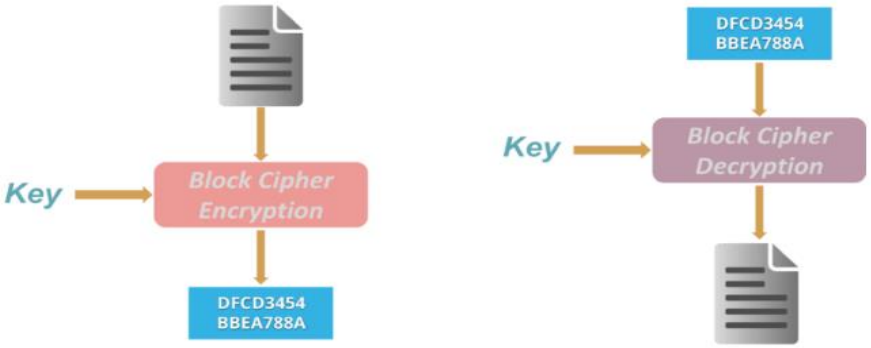

Figure 7: Block based Encryption

3.2 Asymmetric Key Encryption (or Public Key Cryptography)

In this approach of asymmetric key, mathematical formulations and functions are used with the association of different keys. In addition to this, the mathematical functions with the fuzzy association are done. RSA based cryptography is one of the broadly used asymmetric key cryptography approach.

RSA Algorithm

- RSA stands for the originators of this algorithm - Rivest, Shamir, and Adelman
- If one key is declared as public, then alternate key will be private and vice versa
- The key length is optional (512bits/1024 bits/2048 bits)

Figure 8 depicts the RSA based key generation and encryption process.

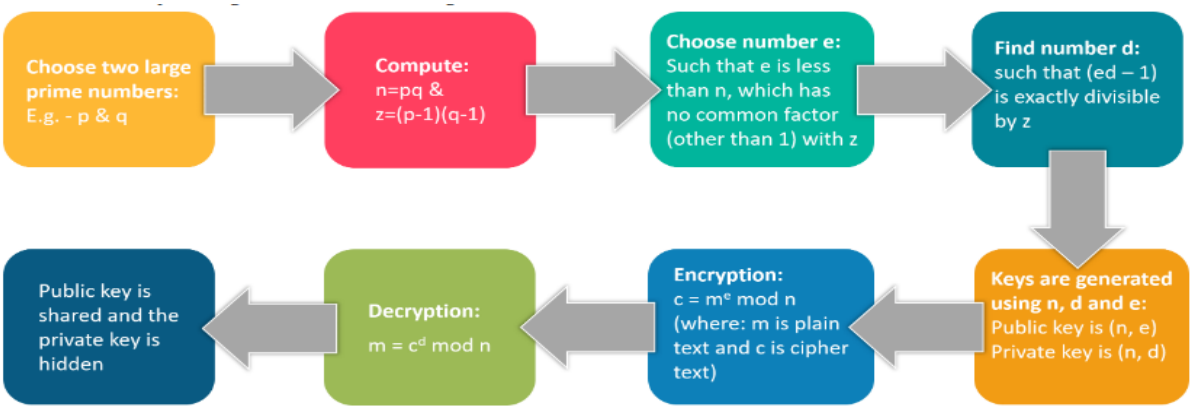

Figure 8: RSA based Encryption

Following are the taxonomy of the cryptography-based approaches:

Classical Cryptography includes the manipulation among the characters and the digits, Based on Security using Obscurity Approach, entire crypto-system is communicating with confidentiality. In contrast, Contemporary Cryptography includes Binary Operations and Bit-Wise Manipulations, Usage of Data Science and Mathematical Functions and Integration of Secret Key. There is another approach titled Steganography that is associated with the security and integrity in enormous scenarios. Following are the key differences between cryptography and Steganography.

Table 3: Comparative Evaluation of Key generation and exchange

Implementation	ECDH	DH	DSA	RSA	ElGamal	NTRU	DSS
Botan	1	1	1	1	1	0	1
Bouncy Castle	1	1	1	1	1	1	1
Crypto++	1	1	1	1	1	0	1
Libgcrypt	1	1	1	1	1	0	1
Libsodium	0	1	1	0	0	0	0
Nettle	0	0	1	1	0	0	0
Cryptlib	1	1	1	1	1	0	1
OpenSSL	1	1	1	1	0	0	0
wolfCrypt	1	1	1	1	0	1	1

Table 3 presents the cryptography-based approaches on assorted parameters with the key features and the availability of specific secured implementations. The availability of specific feature is depicted as ‘1’ and non-availability is presented as ‘0’ in the tabular data.

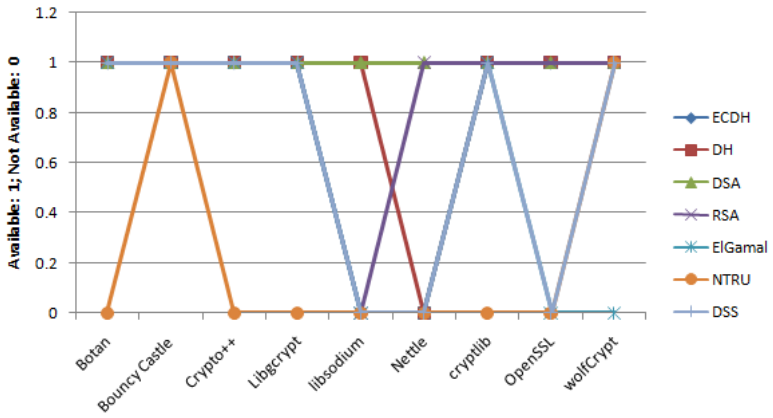

Figure 9: Open Source Cryptography Libraries and Features

Table 4 presents the assorted public key cryptography implementations with the standards which are quite prominent for the cumulative performance in multiple scenarios.

Table 4: Public key cryptography standards in the Cryptography Implementations

Implementation	PKCS#1	PKCS#5	PKCS#8	PKCS#12	IEEE P1363	ASN.1
Botan	1	1	1	0	1	1
Bouncy Castle	1	1	1	1	1	1
Cryptlib	1	1	1	1	0	1
Crypto++	1	1	1	0	1	1
Libgcrypt	1	1	1	1	1	1
Libsodium	0	0	0	0	0	0
Nettle	1	1	0	0	0	0
OpenSSL	1	1	1	1	0	1
WolfCrypt	1	1	1	1	0	1

Table 5 is having the cavernous evaluation of cryptography implementations with the security-based hashing approaches. The hash-based approaches are used to provide the higher degree of security and integrity in the network environment as well as overall communications.

Table 5: Implementation details of various Hashing Algorithms

Implementation	MD5	SHA-1	SHA-2	SHA-3	RIPEMD-160	Tiger	Whirlpool	GOST	Stribog	BLAKE2
Botan	1	1	1	1	1	1	1	1	1	1
Bouncy Castle	1	1	1	1	1	1	1	1	1	1
Cryptlib	1	1	1	1	1	0	1	0	0	0
Crypto++	1	1	1	1	1	1	1	1	0	1
Libgcrypt	1	1	1	1	1	1	1	1	1	1

Libsodium	0	0	1	0	0	0	0	0	0	1
Nettle	1	1	1	1	1	0	0	1	0	0
OpenSSL	1	1	1	1	1	1	1	1	0	1
wolfCrypt	1	1	1	1	1	0	0	0	0	1

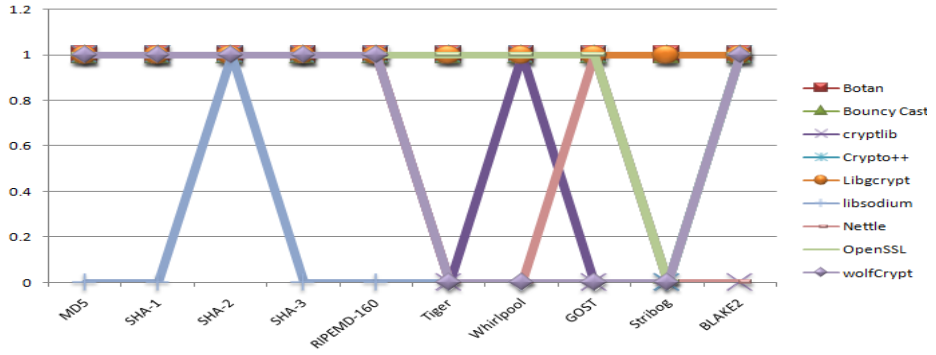

Figure 10: Open Source Cryptography Libraries and Features

The following Table 6 is having the comparative evaluation on the availability aspects with the support for SIM, HSM and Smartcard in the Implementations so that financial and banking with block-chain based implementations shall be effective.

Table 6: Support for SIM, HSM and Smartcard in the Implementations

Implementation	PKCS #11	PC/SC	CCID
Libsodium	0	0	0
Bouncy Castle	1	0	0
Cryptlib	1	0	0
wolfCrypt	1	0	0
Crypto++	0	0	0
Botan	1	0	0
Libgcrypt	1	1	1
OpenSSL	1	0	0

Table 7: Evaluation of Cryptography Hash Approaches in Network Environment

Algorithm	Rounds	Word size	Internal state size	Block size	Output size (bits)
GOST	32	32	256	256	256
HAVAL	5	32	256	1024	128
MD2	18	32	384	128	128
MD4	3	32	128	512	128
MD5	64	32	128	512	128
PANAMA	32	32	8736	256	256
RIPEMD	48	32	128	512	128
RIPEMD-128/256	64	32	128/256	512	128/256

RIPEMD-160	80	32	160	512	160
RIPEMD-320	80	32	320	512	320
SHA-0	80	32	160	512	160
SHA-1	80	40	160	512	160
SHA-256	64	56	256	512	256
SHA-3	24	64	1600	3200	512
SHA3-224	24	64	1600	1152	224
SHA3-256	24	64	1600	1088	256
SHA3-384	24	64	1600	832	384
SHA3-512	24	64	1600	576	512
Tiger2	24	64	192	512	128
WHIRLPOOL	10	8	512	512	512
BLAKE2b	12	64	1024	512	512
BLAKE2s	10	32	512	256	256

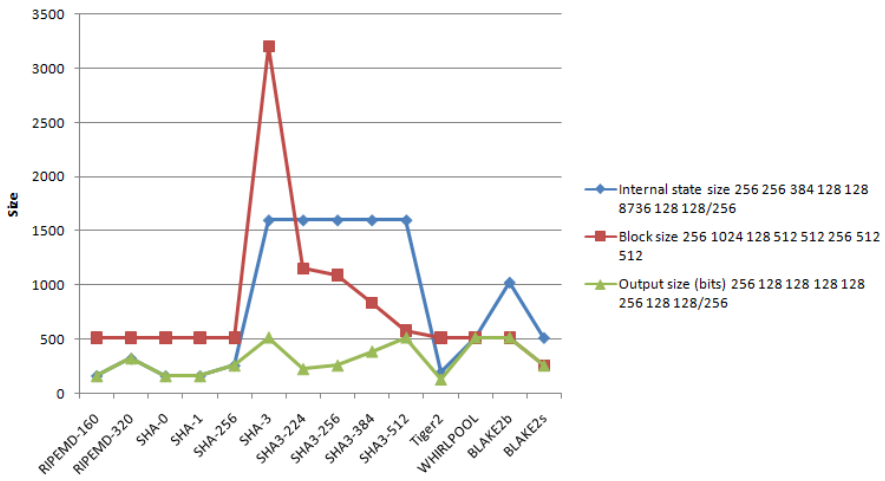

Figure 11: Evaluation of Traditional Cryptography Hash approaches

The tabular and graphical view in the Table 8 and Figure 11 presents the parameters Rounds, Word size, Internal state size, Block size, Output size (bits) which are the paramount aspects in the performance of cryptography approaches.

4. Conclusion

This paper focuses on the empirical review of the cryptography approaches in the advance wireless scenarios of the Internet of Things (IoT) whereby the assorted approaches are used and evaluations on the diversity of research manuscripts is done so that the detailed comparative evaluation of the work done can be presented. Multiple different approaches and algorithms are discussed in this paper. The SHA-256 is the best technique that can be used for a secured communication and will return higher degree of accuracy and cumulative performance parameters.

References

1. B. L. Srinivas, A. Shanbhag, and A. S. D. Souza, "A comparative performance analysis of DES and BLOWFISH symmetric algorithm," International Journal of Innovative Research in Computer and Communication Engineering, 2(5), 2014, pp. 77-88. 16.
2. M. A. Hameed, A. I. Jaber, J. M. Alobaidy, and A. Alaa, "Design and simulation DES algorithm of encryption for information security," American Journal of Engineering Research, 7(4), 2018, pp. 13-22. 17
3. S. Ramanujam, and M. Karuppiah, "Designing an algorithm with high avalanche effect," Int. J. Comput. Sci. Netw. Secur., 11(1), 2011, pp. 106-111. 18.
4. R. Divya, and M. Kumar, "Enhanced digital assessment of examination with secured access," International Journal of Advanced Studies in Computers, Science and Engineering, 3(10), 2014, pp. 33-37. 19.
5. M. M. Al-Laham, "Reducing security concerns when using cloud computing in online exams case study: General Associate Degree Examination (Shamel) in Jordan," Int. J. Comput. Sci. Inf. Technol., 7(6), 2015, pp. 131-144. 20.
6. N. Singhal, and J. P. S. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," Int. J. Comput. Trends Technol., 2(6), 2011, pp. 177-181.
7. “Cloud computing security”, Wikipedia, Wikimedia Foundation, 4 March 2021, https://en.wikipedia.org/wiki/Cloud%20_ computing%20security.
8. A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” J. Netw. Comput. Appl., vol. 79, pp. 88–115, 2017.
9. H. Wu, Y. Ding, C. Winer, and L. Yao, “Network security for virtual machine in cloud computing,” in 5th International Conference on Computer Sciences and Convergence Information Technology, 2010, pp. 18–21.
10. A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” J. Netw. Comput. Appl., vol. 79, pp. 88–115, 2017, (ISSN: 1084-8045), http://doi.org/10.1016/j.jnca.2016.11.027.
11. J. Wu, et al., “Cloud storage as the infrastructure of cloud computing,” in 2010 International Conference on Intelligent Computing and Cognitive Informatics, IEEE, 2010.