International Journal for Rapid Research in Engineering Technology
Vol IX Issue I January 2023
ISSN (Online):- 2455-4723

A Review on Encryption and Decryption Techniques with Multiple Key in Clouds Data

Teena chouhan, Asst. Prof. Ms. Priya Sen
Department of Computer Science & Engineering
Swami Vivekanand College of Engineering
teenachou012@gmail.com, priyasen@svceindore.ac.in,

Abstract: Cloud computing is considered as an on-demand delivery of services in which applications and infrastructure are allocated to users as metered services over networks. Cloud computing services are much cheaper as the user does not have to setup any computing hardware support. It is an emerging technology that delivers computing services such as online business applications and data storage over the Internet. Implementing cloud enables a distributed working environment, where it reduces expenditure of the organization, provides data, information security and so on. Cloud computing has created a paradigm shift in the way information technology resources are provided and consumed by increasing agility and lowering costs. However, cloud-security concerns appear at the top of almost all surveys. Traditional security solutions are having a hard time trying to keep up with the growing security needs of the ever-changing threat landscape in today's cloud environment. This research paper aims to explore the concept of cloud security and its impact on the present day IT environment. We try to classify the security risks in the cloud environment, assess the cost of cloud security, delve into the types of attacks, look for currently available security solutions and arrive at a roadmap for cloud security.. Cloud Server provides storage and search services. To perform efficient searches, the cloud uses verification keys to maintain privacy protection or meet authentication requirements and provide equivalent proof of encrypted documents based on tokens. Most security issues are caused by people deliberately creating malicious or malicious purposes. This Paper reviews and examines some Encryption and Decryption technologies. As a result, the better solution to the symmetric key encryption and the asymmetric key encryption is provided.

Keywords: RSA, Cloud, Encryption, Descrtyption ,Cloud Server, Security

I Introduction

Computer took much space like a big room with exorbitant electronic parts like network devices and processors. These days, small storage devices and costly electronic parts have replaced those large spaces by reasonable network devices. As a result of this improvement, a large distributed system is originated to integrate a vast number of resources in a single unit that can perform highly exhausting tasks. The distributed system has two prominent components, which are clusters and grids. Grid is the design for large heterogeneous and distributed networks, whereas cluster strengthens the amalgamation of homogeneous networks. The grid is most frequently used architecture by operators for creation of servant computational nodes. The cluster is comparatively costlier due to the expensive processing units [1]. As mentioned above, after cluster and grid now cloud computing has evolved as a novel distributed computing model. It provides a professional model for on demand computing services that is focused on cost-as-you-go method that customers can choose any resources, which are needed. In a virtualized manner, they provide a massive amount of computing power with the integration of all the computing resources in a single physical system [2]. Some security loopholes in cloud computing are still remaining as a demanding issue in cloud environment. As several businesses accept cloud technology, cloud computing is rising day by day and it poses many security challenges at the same time. Many enterprises hesitate to handover their sensitive information to cloud environment as many risks are associated with it. Several distinct threats are introduced to the privacy and security of cloud services due to the usage of virtual machine. Another issue is data migration over the Internet. The concept of multi-tenancy is used for sharing cloud resources among multiple users. This idea remains as an obstacle to the development of a fully safe architecture. The cloud provider is hesitant to incorporate security monitoring or intrusion detection and prevention systems due to transparency problems [21].

Data Integrity and Availability- Cloud users (ie data owners) must always be able to check honour of files at all times. To improve storage efficiency, it is best to copy metadata required for file and data integrity checks (such as authentication codes) at the same time. Considering a malicious user on the cloud server, the cloud server must verify that user really owns file before produce a link to his file; user must also confirm that cloud really stores the

file in its storage or must be in the entire lifecycle Review the integrity of the file.The new cloud computing paradigm provides an on-demand purchase of shared configurable computer resource pools and a convenient way to pay for on-demand network access. It requires minimal interaction or management work between service providers. Businesses can now choose to subcontract their data to cloud stowage to reduce the burden of local data storage or condense conservation.[3][4]

Secured File Transfer-Although the cloud provides limited assistances to data owners, subcontracting data to remote servers and providing data organisation to untrusted cloud service providers can pave the way for losing physical control of data (Wang et al., 2009). Cloud is inherently insecure and reliable for clients, which stances new challenges for integrity, concealment and data obtain ability of cloud computing. Delete e.g. Less commonly received data to provide usable disk space or hide injured or corrupted data to shield organization's standing. Some organizations report that the data on the servers of main cloud substructure providers is corrupted and that there are several cloud service interruptions, such as massive deletion of Gmail emails, Side kick Cloud Disaster, Amazon S3breakdown and Amazon EC2 service interruptions (Crossbow, etc.). 2010). The Clearinghouse for Privacy (PRC) described that more than 535 data cracks occurred in 2011, including breaches of cloud-based email service providers based on Epsilon, Sony Play Station Network, Sony Online Performing or Sony Pictures' Damages, 3, 3 million theft patients' medical data of Sutter Surgeons Services, theft of customers' information on EMC's RSA.[5]

CONCEPTS OF CLOUD SECURITY Cloud security describes set of guidelines, technologies, and controls which are useful for the protection of data and services. Cloud services are affected by the threats and its related attacks. Services of different layers as well as availability, integrity, authentication and confidentiality of the Restrictions apply. Cloud resources can be exploited, which may arise new security concern [2]. The cloud security includes threats, security issues and possible attack preventions. This paper discovers the source of vulnerabilities and threats to understand cloud security. Here, some cloud security concepts that are present in the cloud are discussed [3, 12].

A.Virtualization -The process of utilizing services, computing resources like storage, RAM etc. from the hardware on which they run is known as virtualization. The virtualization elements are the virtual machine (VM) and the virtual machine manager (VMM). VM is an image of large size contents per-image of operating system is known as guest operating system. It is accountable for running multiple tasks on the system. This resource is attainable by VMMs, which is the reason for assigning virtual hardware resources to each VM. Multiple VMs can be linked by VMMs. VMs are linked with virtual switches and are made up of internal and external networks. The main feature of VM image is that it can be easily moved, copied or cloned. Cloud provides highly scalable and available services to their consumer [17].

B. Multi-tenancy- Multi-tenancy introduces the concept of sharing resources or instances, which are shared by multiple operators is called tenants. It gives one or more users the opportunity to share a single cloud network. Multi-tenancy may be used when important user details can be stored in the same physical location. As a result, neighbour VMs or running applications can be accessed by attacker [17].

C. Security controls - Risk can be avoided or minimized with the use of security controls. They also recognize, prevent or understand the security threats. Security plans include a list of countermeasures, how to use them, and other information related to them. It requires unique practices and rules that are used in a system or service for the application of security controls. These controls help us to achieve highest possible security.

D. Security mechanisms- Security mechanism is a defensive framework used for securing the computing resources, services, information and sensitive data. They are narrated in terms of safeguards and countermeasures to increase the security of the cloud.

E. Security policies- The security policy guides and describes the application of the security system's rules and regulations. To recognize the use of security systems and controls, security policies are useful.

F. Data storage mechanism and security- Several security mechanisms are introduced in the OSI model by including the authentication mechanism for data access control and digital signature for integrity control. Data processing is a huge challenge since vast volumes of data are stored in the cloud. Also, it's another aspect is reliable data storage backup policies are also necessary. Even though cloud provider is same, cloud spreads data into multiple data centers.

G. Trust management- In cloud protection, trust remains as an essential factor. Trust is highly volatile and it is highly based on the underlying feature. The trust problem occurs in the cloud, when user data and resources are located remotely and are managed by third parties [20]]

II PROBLEM FORMULATION

To ensure the secure data transmission and storage at minimal cost and searching time. The central goal of cloud computing is to improve computational capacity of the cloud system and to enhance the access levels to the services and resources of the cloud cheaply. Cloud computing defines a remote server that is accessible via Internet, facilitating the use of business applications and features and computer software. This can save users money spent on annual or monthly subscriptions. Due to the benefits of cloud services, more and more personal information is concentrated on cloud servers, such as private videos and photos, individual health records, emails, government documents, company financial data, etc.[8]

III LITERATURE REVIEW

The following sub-sections give information mined from technical books and IEEE papers. There are many papers related to cloud computing, cloud security, ECC algorithm and Shamir secret distribution. Following the review, the following documents appear to be relevant to the current work of this paper:

The notion of Multi-Key Searchable Encryption (MKSE) enables data owners to outsource their data into a cloud server, while supporting fine-grained data sharing with the authorized users. Note that the traditional MKSE is vulnerable to data leakage. That is, the malicious data owner may collude with the server and recover the search queries of authorized users. Recently, Hamlin et al. (PKC'18) presented a new MKSE construction that can ensure data privacy between data owner and authorized users, where the share key is generated depending on data owner, authorized user and the specific document. However, their scheme cannot support verifiable search in the case of the malicious cloud server. In this paper, we propose a new verifiable MKSE (VMKSE) scheme by leveraging Garbled Bloom Filter, which can simultaneously support verifiability of search result and secure data sharing in multi-user setting. Compared to the state-of-the-art solution, the proposed scheme is superior in efficiency and verifiability. The experiment results demonstrate the efficiency of our scheme

The following sub-sections give information mined from technical books and IEEE papers. There are many papers related to cloud computing, cloud security, ECC algorithm and Shamir secret distribution. Following the review, the following documents appear to be relevant to the current work of this paper:

Than MyoZaw et.al (2019) A database is a collection of organized data. Although there are various types of technologies (such as encryption and electronic signature) that can be used to protect data during cross-site transmission. Data protection refers to the common procedures used to defender safeguard data or data management software against illegal use or threats or malicious occurrences. In this article, we create 6 different ways to store and retrieve data information in a safe and efficient way in a more secure way. Discretion, integrity or accessibility (also known as three-in-one CIA) are models designed to guide information intelligence policies. There are many encryption technologies available, and ECC is one of the most powerful. Users want to store or request data, and users need to be verified. The verified user will receive the key of the main generator, and then the data must be encrypted or decrypted into database. Each key is stored in a large generator or retrieved from the key generator. Use 256-bit AES for high-level extraction, column-level theft, and component level analysis in database. The next 2 methods are to use 521-bit ECC encryption and signaling to encrypt high-level encryption or high-level encryption in the field using 256-bit AES encryption keys. The last technique is safest method in this article. This method uses AES and ECC encryption for component-level encryption to ensure confidentiality and uses ECC signatures for each component in database to ensure authenticity. In addition to translating data at interruptions, it is also significant to ensure that personal data is converted during network traffic to prevent database signatures. The advantage of the element level is difficult to attack, because attacker key will lose only one element. Loss requires thousands of keys to manage.

Feng Shengwu et al. (2018), the level of information security in the cloud computing environment directly affects the data protection issues of users. Using an encryption algorithm with its unique features can compensate for the errors caused by relying on security software security strategies, further convincing them Difficulties and challenges in protecting information. By

examining the basic concepts of elliptic curve encryption algorithm, the encryption algorithm curve based on cloud data protection technology creates a more efficient way to ensure the performance of available systems. safe and effective, and conducts security testing. Built with Matlab 9 software. The outcomes show that cloud-based encryption knowledge based on the ECC algorithm has high security or speed, or can effectively protect safety and security of cloud data.

Mustapha Benssalah et.al (2018) Telemedicine Medical Information System (TMIS) is one of greatest advanced technologies needed to diagnose and treat patients. In this context, special attention has been paid to the importance of exchanging medical data including symbols, images etc. Indeed, since DICOM items contain images and information related to patients 'concerns, their safety issues or privacy should be carefully addressed. In this system, various encryption methods have been introduced in literature to solve problems through a variety of cryptographic solutions, such as chaos-based theory, cryptography (elkiptic). Curve cryptography) (ECC) and other lightweight explanations. In this article, we have conducted a qualified analysis of both ECC encryption and encryption methods. As we know, this is first time that symmetric-based encryption has been compared to EEC-based irregular encryption for image security. The effectiveness of 2 cryptographic systems measured to be evaluated is based on analysis and timing of the security implementation. The results are reassuring and can be used to further examine this search axis.

Pratibha Chaudhary et al. (2019) can calculate in the form of collected data - this is the content of homomorphic writing. Homomorphic encryption solves security problems by storing data on third party systems (e.g., cloud or unreliable computers, service providers, etc.). The most important category of homomorphic encryption is complete homomorphic encryption. It allows unlimited operation of data in encrypted form, and the system exits cipher text space. This article provides basic information about homomorphic encryption and its various categories, namely homomorphic encryption, homomorphic encryption and full homomorphic encryption. Its main features are complete homomorphic encryption and the study of complete homomorphic encryption schemes. These tables use lattices, integers, error analysis and elliptic curve cryptography.

PreetiGoyal et.al (2019) In field of computer science, cloud computing has become a well-known paradigm that allows you to start services, such as storing and editing data over Internet instead of the hard disk drive of a computer. Cloud also offers various services such as Iaas, Paas and Saas. With the popularity of the cloud, access to the hidden files of various cloud users began to interfere with its process. There must be a system that provides the necessary protection. To achieve security, cloud services use various security rules, such as privacy, access control, integrity, presence etc. In today's work, all of these moralities are applied to the environment through algorithms such as ECC to improve discretion of data. In this case, MD5 maintains integrity of data on server side and enforces access control through RBAC technology. As a result, the proposed architecture provides a high level of protection for cloud atmosphere.

Based on an analysis of the vulnerabilities of wireless communication networks (WSNs), **YueTongxu et al. (2019)** combined high-encryption efficiency of symmetric coding algorithms with high strength of asymmetric coding algorithms, and proposed a method based on Wireless Network Sensor. The algorithm overrides the simple block by sorting simple messages, using Advanced Encryption Standard (AES) with symmetric encryption algorithm or Elliptic Curve Encryption (ECC) of different algorithms asymmetric, or then uses data transfer knowledge to obtain the cipher block, the MAC address or AES key hidden by the ECC to create a complete ciphertext communication. By defining and applying algorithm, the results show that algorithm can decrease encryption time, encryption time or complexity of running time without losing safety.

IV CRYPTOGRAPHIC SYSTEMS:

Cryptographic Systems can be divided into deterministic and probabilistic encryption scheme [7]. Deterministic encryption scheme allows the plaintext is encrypted by using keys that always provide the same ciphertext, but the encryption process is repeated many times. In this scheme, every plaintext has one to one relationship with the keys and ciphertext otherwise it will produce more than one output of particular plaintext during the decryption process. Probabilistic Encryption Scheme shows the plaintext has different ciphertext with the different keys. The probabilistic encryption scheme is significantly secure than the deterministic encryption scheme because it makes difficult for a cryptanalyst to access any sensitive information regarding plaintext that is taken from ciphertext and corresponding key. Furthermore, the

cryptographic algorithms can be further divided into two main categories like keyless cryptosystem and key-based cryptosystem as shown in Fig. 1. In the keyless cryptosystem, the relationship between the plaintext and ciphertext having a different version of the message is exclusively depend on the encryption algorithm [8]. The keyless cryptosystem is generally less secure than key-based systems because anyone can gain access to the algorithm will be able to decrypt every message that was encoded using keyless cryptosystem such as Caesar cipher [9]. The key based cryptosystem can be further categories into symmetric key (secret key) encryption and asymmetric key (public key) encryption based on the type of security keys utilized for the encryption or decryption process [10]-[13]. The detail of the cryptosystems is explained as follows:

RSA Algorithm- RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic- Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. The RSA algorithm (named after the inventors Rivets, Shamir and Adleman) was one of the first cryptographic algorithms that met the requirements for public key systems as stated by Diffie and Hellman [5]. Since then it has reigned supreme as the only widely accepted and implemented general purpose approach to public key systems.[10]

Key Schedule Algorithm: Key schedule algorithm is employed to generate secret keys and plays an important role in the development of encryption and decryption key. The insignificant key generation algorithm generates weak keys that are used for encryption process can easily attack using brute force attack because cryptanalyst continuously trying all possible combinations to get original text using this attack [27]-[29]. All cryptographic algorithms follow the consideration of Advanced Encryption Standard (AES) that must support the key lengths include 128 bits, 192 bits and 256 bits [19]. The number of the round for that key length is 10, 12, 14 respectively and the round keys are taken from the cipher key using key schedule algorithm and utilized in the construction of block cipher. For the development of fully secure block cipher, the multiple numbers of rounds ensure the high diffusion and employed invertible transformation.

Symmetric Key Encryption: The symmetric key (secret key) encryption is employed similar key for the encryption and decryption of a message. Encryption and decryption keys are keeping secret and only known by authorized sender and recipient who want to communicate. The allocation of different keys to the different parties increases the overall message security. The strength of the symmetric key encryption is depending on the secrecy of encryption and decryption keys. The symmetric encryption algorithms can be classified into block and stream cipher on the basis of the grouping of message bits [14], [15]. In a block cipher, a group of messages characters of a fixed size (a block) is encrypted all at once and sent to the receiver. Moreover, the block cipher can be further divided into binary and non-binary block cipher based on the final results of the message, keys and ciphertext. The message bit size for the binary block cipher is 64, 128, 192, and 256 and the non-binary block cipher has not defined the standard that depends on the cipher implementation.

Asymmetric Key Encryption The asymmetric key encryption is commonly referred to as public key encryption in which different keys are employed for the encryption and decryption of the message. The encryption key is also said as the public key and can be utilized to encrypt the message with the key. The decryption key is said to as secret or private key and can be used to decrypt the message. The strength of the asymmetric key encryption is utilized with digital signature then it can provide to the users through message authentication detection. The asymmetric encryption algorithm includes RSA.

Public key -The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the private (or decryption) exponent d, which must be kept secret. p, q, and $\lambda(n)$ must also be kept secret because they can be used to calculate d. In fact, they can all be discarded after d has been computed. In the original the Euler totient function $\varphi(n) = (p - 1)(q - 1)$ is used instead of $\lambda(n)$ for calculating the private exponent d. Since $\varphi(n)$ is always divisible by $\lambda(n)$ the algorithm works as well. That the Euler totient function can be used can also be seen as a consequence of Lagrange's theorem applied to the multiplicative group of integers modulo pq. Thus any d satisfying $d \cdot e \equiv 1 \pmod{\varphi(n)}$ also satisfies $d \cdot e \equiv 1 \pmod{\lambda(n)}$. However, computing d modulo $\varphi(n)$ will sometimes yield a result that is larger than necessary (i.e. $d > \lambda(n)$). Most of the implementations of RSA will accept

exponents generated using either method (if they use the private exponent d at all, rather than using the optimized decryption method based on the Chinese remainder theorem described below), but some standards such as FIPS 186-4 may require that $d < \lambda(n)$. Any "oversized" private exponents not meeting that criterion may always be reduced modulo $\lambda(n)$ to obtain a smaller equivalent exponent

Data Encryption Standard (DES) DES is the earliest symmetric encryption algorithm developed by IBM in 1972 and adopted in 1977 as Federal Information Processing Standard (FIPS) by the National Bureau of Standard (NBS). The NBS is currently the National Institute of Standards and Technology (NIST) that evaluate and implement the standard encryption algorithm. It includes 64 bits key that contains 56 bits are directly utilized by the algorithm as key bits and are randomly generated. The remaining 8 bits that are not used by algorithm because it is used for the error detection as set to make a parity of each 8- bit byte [17], [37], [38]. DES utilized the one secret key for encryption and decryption process and key length is 56 bits and performs the encryption of message using the 64 bits block size. Similarly, the decryption process on a 64 bits ciphertext by using the same 56 bits key to produce the original 64 bits block of the message

Key distribution-Suppose that Bob wants to send information to Alice. If they decide to use RSA, Bob must know Alice's public key to encrypt the message and Alice must use her private key to decrypt the message. To enable Bob to send his encrypted messages, Alice transmits her public key (n, e) to Bob via a reliable, but not necessarily secret, route. Alice's private key (d) is never distributed.

Encryption-After Bob obtains Alice's public key, he can send a message M to Alice. To do it, he first turns M (strictly speaking, the un-padded plaintext) into an integer m (strictly speaking, the padded plaintext), such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c, using Alice's public key e, corresponding to This can be done reasonably quickly, even for very large numbers, using modular exponentiation. Bob then transmits c to Alice.

Decryption- Alice can recover m from c by using her private key exponent d by computing given m, she can recover the original message M by reversing the padding scheme

V Conclusions

Cloud computing offers the benefit of rapid deployment, cost savings, massive storage space, and easy-to-access anywhere and anytime to the system. It aims to empower the user by providing a seamless and rich functionality, regardless of the resources. So, it is evident that cloud computing is a swiftly evolved technology and broadly accepted computing environment around the globe. Cloud computing have many advantages over conventional environment and have the ability to handle most sudden peaks in application or service that demand on the cloud infrastructures. However, there are several privacy and security concerns that act as a barrier to the acceptance of cloud computingCloud Computing is still a rapidly evolving landscape; and one that requires us to stay current or fall behind. Still, we must not be complacent. Just as security professionals have done for ages, we must continue to evolve our processes, methods, and techniques in light of the opportunities that Cloud Computing brings to our industries. This evolution is critical to our long-term success as we find new ways to improve the efficacy and efficiency of our security enforcement and monitoring capabilities. Cloud Computing isn't necessarily more or less secure than a traditional environment. As with any new technology, it creates new risks and new opportunities. In some cases moving to the cloud provides an opportunity to rearchitect older applications and infrastructure to meet or exceed modern security requirements. At other times the risk of moving sensitive data and applications to an emerging infrastructure might exceed our tolerance

References

1. Than MyoZaw Min Thant S. V. Bezzateev Database Security with AES Encryption, Elliptic Curve Encryption and Signature 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) Year: 2019 ISBN: 978-1-7281-2288-5 DOI: 10.1109/IEEESaint-Petersburg, Russia, Russia
2. Feng Sheng WuResearch of Cloud Platform Data Encryption Technology Based on ECC Algorithm2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)Year: 2018 ISBN: 978-1-5386-8031-5 DOI: 10.1109/IEEEChangsha, China
3. Mustapha Benssalah Yasser Rhaskali Mohamed Salah AzzazMedical Images Encryption Based on Elliptic Curve Cryptography and Chaos Theory2018

International Conference on Smart Communications in Network Technologies (SaCoNeT)Year: 2018 ISBN: 978-1-5386-9493-0 DOI: 10.1109/IEEEElOued, Algeria

4. Pratibha Chaudhary Ritu Gupta Abhilasha Singh PramatheshMajumderAnalysis and Comparison of Various Fully Homomorphic Encryption Techniques2019 International Conference on Computing, Power and Communication Technologies (GUCON)Year: 2019 ISBN: 978-93-5351-098-5 IEEENCR New Delhi, India, Indi
5. PreetiGoyalHemantMakwanaNilima KarankarMD5 and ECC Encryption based framework for Cloud Computing Services 2019 Third International Conference on Inventive Systems and Control (ICISC) Year: 2019 ISBN: 978-1-5386-3950-4 DOI: 10.1109/IEEECoimbatore, India, India
6. Rupesh Raj Karn;Prabhakar Kudva;Ibrahim Abe M. ElfadelvDynamic Autoselection and Autotuning of Machine Learning Models for Cloud Network Analytics IEEE Transactions on Parallel and Distributed Systems Year: 2019 DOI: 10.1109/TPDS.2018.2876844
7. Marouane Hachimi;Georges Kaddoum;Ghyslain Gagnon;Poulmanogo Illy Multi-stage Jamming Attacks Detection using Deep Learning Combined with Kernelized Support Vector Machine in 5G Cloud Radio Access Networks 2020 International Symposium on Networks, Computers and Communications (ISNCC) Year: 2020
8. Song Xia;Meikang Qiu;Hao Jiang An adversarial reinforcement learning based system for cyber security 2019 IEEE International Conference on Smart Cloud (SmartCloud) Year: 2019 DOI: 10.1109/ IEEE Tokyo, Japan
9. Sumanth Gowda;Divyesh Prajapati;Ranjit Singh;Swanand S. Gadre False Positive Analysis of Software Vulnerabilities Using Machine Learning 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) Year: 2018
10. Dharitri Tripathy;Rudrarajsinh Gohil;Talal HalabiDetecting SQL Injection Attacks in Cloud SaaS using Machine Learning 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) Year: 2020