International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

A Review on Clouds Security Based Encryption and Decryption Techniques

Shruti Bhawsar
M.Tech. Scholar
Department of Computer Science and Engineering
Lakshmi Narain College of technology,
Indore (M.P.)

Kushal Joshi
Assistant professor
Department of Computer Science and Engineering
Lakshmi Narain College of technology,
Indore (M.P.)

***Abstract* - Today, large amounts of electronic data have been created, and the work of organizations that need data recovery services can suffer from various natural or man-made disasters, which can lead to huge data losses. Encryption and spatial encryption performance and average response time have been estimated based on the size of the data file. RSA encryption is often used in cloud storage. It allows cloud services to search encrypted data directly. 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.**

***Key words* –RSA, Cloud, Encryption,Descrtyption ,Cloud Server, Security**

I INTRODUCTION

Cloud computing is a distributed community that provides calculating or storage space as services to end users. The architecture / model of cloud computing is that all servers, networks, presentations or other basics connected to the facts centre are accessible to the end users. Cloud computing is upward in attention of technology and business organizations, but this is useful for solving social problems. It can also be beneficial. Cloud computing refers to online operation, configuration and access to applications. It provides online data storage, infrastructure or submissions. Cloud computing allows individuals and businesses to shift the burden by managing large amounts of data or performance processes that require computing for powerful servers. Due to the growing approval of cloud figuring, more or more data proprietors are being encouraged to subcontract their data to cloud attendants in order to provide great convenience and reduce data management costs. Data tenants provide services to many businesses and companies, and they insist on improving data security standards by following a covered method, including following: data encryption, key organization, strong admission controls, or security intellect. The cloud attendant performs query or returns encrypted papers with an additional proof according to the token generated by Data owners. The Data users will receive the result with the corresponding proof so they can verify the correctness and decrypt scrambled leaflets after verification is accurate.

Concepts Of Cloud Computing - Cloud computing is an advantage of information technology / business applications. Any organization can gain this benefit by paying or renting usage. Storage, servers and applications belong to the cloud computing area and are prerequisites for on-demand access. Therefore, unlike traditional methods of building data centers, hardware, applications and applications can be executed in a secure way before concentrating on building / transmitting business solutions. Cloud computing eliminates the need for expensive data centers and management because cloud vendors provide, manage and monitor the health and accessibility of the framework. Registering a cloud is an event on the network that allows administrators to provide versatility, quality of service (QoS) and, in most cases, to ensure custom on-demand and low-cost computing infrastructure. These infrastructures can be simple and access in a universal way. Cloud computing is a model used to authorize expedient, on-demand network admission to a public pool of configurable computing value (such as systems, servers, storage, function, or management). These resources can be managed by negligible or cloud Service-fast configuration and release The term "cloud" for vendor interaction is built from the network and its schematic representation is cloud. It refers to various specific types of services or submission that have been communicated in Internet cloud, and in many cases the devices used to get these products and applications require no special applications.

Cloud Architecture- The rise of cloud computing is rapidly changing business and innovative ideas and having different effects on different individuals. For utilities and IT customers, IT management (ITaaS) - that is, computing, storage and applications is transferred from the central data centre via the Internet. For Internet and software developers, this is the stage of development of web-scale programming. Operating environment For infrastructure providers and administrators, it is a huge distributed data centre infrastructure that is connected to IP networks.

Top layer (application layer): The top application that is delivered as needed according to the software as a service model (SaaS).

Middle layer (platform layer): Middleware provides application services and platform-as-a-service (PaaS) in the runtime environment for cloud applications.

Bottom layer (infrastructure layer): The basic structure of distributed data center services connected via Internet style networks. Figure 1.2 shows a cloud computing system consisting of four deployment models and three service models.

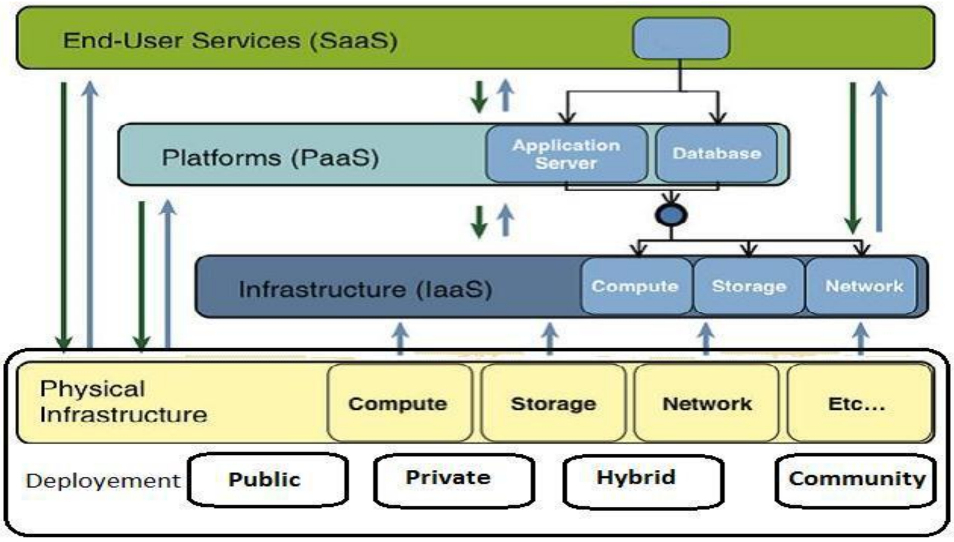

Figure 1 Cloud Computing Systems

Storage Efficiency- One well-known service provided in cloud computing is data storage. Customers do not have to store data on the server, but store their data on the server through a cloud service provider. Customers have to pay for this cloud storage service. Not only does it store tangible and high quality data, but it also provides an advantage to customers who need to pay for the amount of data to be stored over a period of time, without worrying about the hassle of keeping effective way of storing and storing large amounts of data. . In addition to these benefits, customers can easily access their data in any area where the network is easily accessible through a Cloud Service Provider or the Internet .What characterizes the end of this century is the shift of industry information technologies to a model of subscription-based services (called cloud computing). It brings a lot of benefits to the users. There is a lot of data available from day-to-day data distribution or local processing requirements that have led to these changes in technology and business models. Since cloud service providers (CSPs) are different tools in the market, data confidentiality and authenticity are major issues that need to be addressed through cloud computing. Although the service provider has a strong infrastructure and standards or regulations that ensure data protection and stability, thus providing better access, privacy infringement and service interruptions are reported in recent years.

Searching Files From Cloud Storage- Data can be distributed between two storage clouds, so if the opponent is not accessible to the storage cloud, the opponent will not be able to retrieve contents of data .Relying on multiple data storage and retrieval service providers may not prevent service providers from conspiring. Cloud users cannot find out if their information has been retrieved completely from service provider without knowing it. Boneh (1998) proved the threat of collaborating with service providers. We assume that there are two customers (C1) of cloud service providers who want to store their data securely. He divides the data into two parts (D1 and D2), which are divided into two available CSPs (CSP1 and CSP2). The two cloud service providers can link to each other the data stored by consumer on his server is exchanged and the entire data is reconstructed without being perceived by the user. It provides a decision model for cloud computing users to provide better reliability and accessibility by allocating data among multiple cloud service providers. Therefore, no service provider can successfully download and use them.

II PROBLEM DEFINITON

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. The main challenges are

- Consistency
- Limited scalability
- Data replication
- Trust,security,and privacy
- Unreliable availability of cloud
- resources
- Portability

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.

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:

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 signalling 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.[1]

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.[2]

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 (elliptic). 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.[3]

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.[4]

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), [5]

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.[6]

Mustapha Benssalah et.al (2020) Currently, medical imaging information as part of the Telemedisin Information System (TMIS) plays an significant role in the treatment of assisting medical staff in the identification of effective diagnostics. Therefore, regarding number of horrific attacks perpetrated by cybercriminals, security issues and the confidentiality of medical broadcast medical images must be addressed. This paper introduces a new medical imaging strategy, which combines cryptography (elliptic curve cryptography) (ECC), Hill cipher, Arnold cat graphics (ACM) and linear congruential generator (LCG). Through Arnold's Cat and LCG imagery, the confusion and scattering of images is transmitted through hidden health images. Compared to the latest technology, it has been found that encryption strategies are robust to various tactics and provide better security.[7]

The Network Vehicle Ad Hoc Network (VANET) by **Pragathi Yellanki et al. (2020)** provides secure protection through unstructured links. One of the unique features of the VANET system is that it transmits data to a limited amount of security data in a continuously moving topology. The wireless mode of the VANET system facilitates the attack by reading the protocol control message. Therefore, it is necessary to send a VANET protocol message safely. Researched various cryptographic algorithms, and developed a secure state-of-the-art protocol (S-OLSR) for the VANET. Elliptical wing cryptography (ECC) uses the characteristics of elliptic curves, while RSA uses decomposition of primary numbers to obtain encryption key. From results, you will see that the S-OLSR using ECC delivers best encryption for protocol emails with very low latency.[8]

Mohita Jaiswal et al. (2019) With the continued development of the global Internet, information security has become more severe. Many wicked articles can retrieve respected information through unreliable media. In this regard, elliptic curve cryptography (ECC) has been widely recognized has become an beautiful option for new entrants. Many investigators have examined safety of the ECC or it is considered one of most reliable encryption algorithms. This article converses enterprise or implementation of ECC-encrypted encryption in the 192-bit digital format of FPGAs. The micro-ECC recording model or 192-bit decryption were developed by Verilog and upgraded to Xilinx Vivado 2016.2. In this article, the FPGA selected here is the AC-701, which is an assessment board founded on Xilinx's Artix-7 FPGA. In addition, this work demonstrates the use of resources and power consumption in the encryption or decryption models offered in FPGAs. The authors also offer a case study analysis of various event designs.[9]

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 λ(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 CONCLUSION

Text data plays an important role in lives and they are used in many applications in our day to day lives. Therefore it is necessary to affirm the integrity and confidentiality of the data that being transmitted. Some of the encryption techniques are discussed that plays an important role in data transmission. In this paper a survey of some important cryptography algorithm is provided in last decades. These encryption methods are studied and analysed well to promote the performance of encryption methods. Each technique is unique in its own way and this make it suitable for its many application. Everyday new techniques are evolving hence fast and secure conventional encryption techniques work with high security rate. This survey provide a way to design and invent a new and fast encryption algorithm compare with the existing algorithm

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] TongxuYue Chuang Wang Zhi-xiangZhuHybrid Encryption Algorithm Based on Wireless Sensor Networks2019 IEEE International Conference on Mechatronics and Automation (ICMA)Year: 2019 ISBN: 978-1-7281-1699-0 DOI: 10.1109/IEEETianjin, China, China

[7] Mustapha Benssalah Yasser RhaskaliA Secure DICOM Image Encryption Scheme Based on ECC, Linear Cryptography and Chaos 2020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP)Year: 2020 ISBN: 978-1-7281-5835-8 DOI: 10.1109/IEEEEL OUED, Algeria, Algeria

[8] PragathiYellanki M.V.S PhaniNarasimhamSecure Routing Protocol for VANETS using ECC2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)Year: 2020 ISBN: 978-1-7281-5830-3 DOI: 10.1109/IEEEGunupur, India, India

[9] MohitaJaiswalKusumLataHardware Implementation of Text Encryption using Elliptic Curve Cryptography over 192 bit Prime Field2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)Year: 2018 ISBN: 978-1-5386-5314-2 DOI: 10.1109/ IEEEBangalore, India

[10] D. Oppenheimer, A. Ganapathi, and D. A. Patterson, "Why dointernet services fail, and what can be done about it?" in USITS'03: USENIX Symposium on Internet Technologies and Systems, 2003.

[11] J. Gray, "Why do computers stop and what can be done about it?" in Symposium on Reliability in Distributed Software and Database Systems, 1986, pp. 3–12.

[12] "AWS Elastic Compute Cloud (EC2)," http://aws.amazon.com/ec2/, accessed: 2015-06-02.