# Response to Cloud Security on Collective Function

**Vipin Kumar Singh[1], Dharamveer Singh[2], Manis Verma[3]**

[1, 2, 3] Deptt. of Computer Science & Engineering, R.D. Engineering College, Ghaziabad, India

**Abstract - Speaking of internet networks, of course, we are now familiar hearing that name, everyone in the world uses the internet for various purposes such as education, company, trade and even a small child even now has a lot use it. Of the many benefits of the internet, there is a huge threat lurk users like Phishing, Sniffing, Hacking, Cracking, Denial of Service Attack, Malicious and other crimes, both for testing or for irresponsible purposes responsibility, such as data theft, misuse of access rights, etc. With the threats - threats of course we as users will feel insecure because they can be a threat at any time it can attack our systems, data, and networks. Therefore in need is the good network security to prevent and handle threats like that. nature of the development of information technology that is now increasingly rapid, the need for network security will continue to increase of course in terms of security in maintaining information, data and network infrastructure, along with the increasing development of knowledge about hacking and cracking problems, even many of its security methods are growing, software and tools that are constantly being developed. Such as IDS (Intrusion Detection System), IDS is a security method that is used to detect events that occur on computer networks. Of course, detection alone is not enough so we need a method that is capable to prevent attacks that threaten unpins informatics study program networks. Consequently, under this scheme, we propose a new approach for intrusion detection based on SQL-Injections, Cross Server Side Scripts, and DDoS using Machine Learning Models (Random Forest and General Regressed Neural Network). Subsequently, we are able to mitigate and perform penetration testing and formulate the attacks on hosts (servers) over the Internet Service Provider (Server Configure on Cloud Infrastructure also) with the accuracy of 69.10% on Mail servers, Database servers, File System, FTP servers etc.**

## 1. INTRODUCTION

Recently, computer technology has grown rapidly with the development of internet technology and its use in many fields. Communication is getting smoother, even in sharing info or data. Basically, a cloud storage system can be thought of as a network of distributed data centers that usually uses cloud computing technologies such as virtualization, and offers several types of services for storing data. In general, all of this is invisible to the user. In its application, the Cloud Computing system has components, namely: servers, storage servers, Cloud Computing programs, security systems, Cloud providers, and users. In summary, the Cloud Computing work system is that users who use Cloud services can access the Cloud system, where they can interact such as storing data, company web systems etc. By placing data in the cloud, users do not have to be in front of a PC (Personal Computer) to access the cloud, but can also go through mobile devices, it is enough just to connect via the internet. The main features of cloud computing are accessibility, availability and scalability.

## 2. LITERATURE REVIEW

At present, computing pursues a model oriented to services that are offered in real time, as well as the services of electricity, water, telephone, gas, etc. In this model the services are provided online for users and are available at the time they are required. In addition, in this model, users use the services without worrying about where these services are running or how they are reaching their computer equipment. Thus, the computing services offered allow all user processes and information storage to be carried out online instead of on a local computer. As a logical consequence, this leads to less sophisticated computer equipment and consequent savings in equipment cost, energy consumption, and application software. Cloud Computing uses applications and / or services over the Internet, for daily use by any user from their workplace or from wherever they are. The most important characteristic of this technology is that the applications are accessed through the Cloud, in which the data of all users and companies could be accessed from anywhere and be available without having to install the necessary devices and software, reaching a considerable reduction in costs. [21-24].

Cloud Computing is a paradigm that allows computing services to be offered over the Internet. Cloud Computing is the development and utilization of Internet-based computational processing capacity (the "cloud"). The concept is a paradigm shift, through which users no longer need to have knowledge, experience or control over the technological infrastructure that is "in the cloud", the same that supports their activities. This concept typically involves the provision of easily scalable and almost always virtualized resources, treated as services over the Internet. The term "cloud" is used as a metaphor for the Internet, based on how the Internet is represented in computer network diagrams and as an abstraction of the underlying infrastructure that it hides. Cloud Computing providers provide online business applications, which can be accessed from internet browsers (Firefox, IE, Opera, Chrome, Safari, etc.), while the software and data are stored on the servers.

These applications are broadly divided into the following categories: Software as a Service (SaaS), Utility Computing, Web Services, Platforms as a Service (PaaS), Managed Service Providers (MSP), Commerce Service (Service Commerce) and Internet Integration (Internet Integration). The name of "Cloud Computing" was inspired by the symbol of the cloud that usually represents the Internet in flow diagrams and networks

The Cloud model allows companies of any size to obtain advantages that are impossible to achieve and to get with the traditional model [21-24].

- Reduction of operating costs and elimination of investments, by avoiding the need to own IT Infrastructure and Software licenses. It does not require a high initial investment in the purchase of Hardware and Software to start working and you do not need to install any type of hardware in your facilities.
- Withstand peak demand, by enabling limitless scalability of your IT infrastructure.
- More flexibly align IT spending to your business needs. 14 Improve the management of IT personnel, by allowing the concentration of its resources in the critical activities of your company while IT operates its infrastructure with the best technology and specialized personnel.
- Improve the "Time to market", by reducing the provisioning and configuration times of servers with compromised delivery times. - Quick implementation of solutions. You don't have to wait weeks or months to have the solution available and start using it.
- Accelerate the launch of new applications and ease the work of development teams by allowing the contracting of the service for short periods of time that avoids the need for investments.
- Enable direct control of your infrastructure through management portals that you can control yourself and that allow you to monitor and manage your environments instantly.
- Ensure service quality with a high availability SLA and multiple delivery commitments.
- Eliminate defects due to mis-configuration or poor hardware sizing by using standardized and reusable configurations.
- Improve your company's IT risk management, ensuring regulatory compliance and high security and IT governance standards for your infrastructure.

**2.1 HISTORY**

In 1961, John McCarthy, inventor of the LISP programming language, envisioned: one day computing will be organized as a public service, later on July 3, 1969, Leonard Kleinrock, one of the scientists in charge of the ARPANET project ( Advanced Research Projects Agency Network), which laid the foundations of the Internet, said: Currently computer networks are in their infancy, but as they grow and become sophisticated, we will likely see the birth of computing services which, like electricity and telephone services, they will reach every home and office around the country. These visions anticipated the emergence of new computing paradigms strengthened by the development of cutting-edge technologies capable of providing never-before-seen measures of performance, efficiency, scalability, distribution, autonomy and ubiquity. These novel computing paradigms include: cluster computing, grid computing, global computing, Internet computing, peer-to-peer computing (P2P), ubiquitous computing, utility computing and more recently cloud computing, derived from the term cloud, used as a metaphor for Complex technological infrastructures whose origin dates back to the 90s, in reference to the already huge ATM (Asynchronous Transfer Mode) networks. In 1999, Marc Benioff, Parker Harris and other partners founded the company Salesforce.com, applying technologies developed by companies such as Google and Yahoo! to various business applications. They strengthened the delivery of on-demand services, particularly SaaS, being supported by thousands of successful customers and businesses. In early 2000, Yahoo! and Google announced the provision of cloud services to four of the largest universities in the United States: Carnegie Mellon University, the University of Washington, Stanford University and the Massachusetts Institute of Technology (MIT). Shortly thereafter, IBM Corp. announced the offering of cloud services, followed by computing giants such as Microsoft, Oracle, Intel, SUN, SAS and Adobe, whose approaches spanned the provision of IaaS, PaaS and SaaS models. However, it is considered that the beginning of cloud computing can be attributed to the appearance of Amazon's Web services (Amazon Web Services), which began production in 2006 offering the IaaS model with basic processing and storage capabilities to through the Internet [23-25]. It was then, towards the end of the 90s, that this concept gained importance with the advent of Grid Computing. The term Cloud is a metaphor expressing similarity to the power grid, in which electricity is produced in large power plants and then disseminated through a grid to end users. Here, the large plants are the Datacenters, the network is most often that of the Internet and electricity corresponds to computer resources. Cloud Computing did not really appear until 2006 with the appearance of Amazon EC2 (Elastic Compute Cloud) [26-30].

It was in 2009 that the real explosion of the Cloud occurred with the arrival on the market of companies like Google (Google App Engine), Microsoft (Microsoft Azure), IBM (IBM Smart Business Service), Sun (Sun Cloud) and Canonical Ltd (Ubuntu Enterprise Cloud). According to a study conducted by Forrester [31], the cloud computing market was around 5.5 billion dollars in 2008, it is expected to reach more than 150 billion by 2020, as shown in figure 1.1.


| | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BPaaS ($) | 0.15 | 0.23 | 0.35 | 0.53 | 0.80 | 1.26 | 1.95 | 2.93 | 4.28 | 6.00 | 7.66 | 9.08 | 10.02 |
| SaaS ($) | 5.56 | 8.09 | 13.40 | 21.21 | 33.09 | 47.22 | 63.19 | 78.43 | 92.75 | 105.49 | 116.39 | 125.52 | 132.57 |
| PaaS ($) | 0.05 | 0.12 | 0.31 | 0.82 | 2.08 | 4.38 | 7.39 | 9.80 | 11.26 | 11.94 | 12.15 | 12.10 | 11.91 |
| IaaS ($) | 0.06 | 0.24 | 1.02 | 2.94 | 4.99 | 5.75 | 5.89 | 5.82 | 5.65 | 5.45 | 5.23 | 5.01 | 4.78 |

Figure 2.1: Forecast of the size of the public cloud computing market.

3. **PROPOSED METHODOLOGY**

### 3.1 PROBLEM STATEMENT

In spite of the way that Protection, Seclusion and Trust matter subsist since the improvement of the cloud computing,. Any client that transmits data in the cloud is presented to a natural altitude of threat in radiance of the actuality that redistributed organizations avoid the physical, reasonable and staff controls of the customer however using cryptography will verify the proportionate to secure the data while data is in transition or inside the cloud repositories and between the applications or apps. When securing data on the cloud, one should need to guarantee if the data is viably secured and can be recouped later. As the proportion of data set away by the cloud for a client can be titanic, it is nonsensical (and may similarly be in all regards excessive) to recoup all of the data, if one's inspiration is just to guarantee that it is secured adequately. In this manner there is a need to give such affirmations to a client to ensure that the sender and the gatherer and on shielding resource model for security reason. Subsequently, it is huge for together the cloud contributor and the client to have imparted trust to the ultimate objective that the cloud provider can be ensured that the customer isn't some noxious software engineer and the customer can be ensured of data consistency, data amassing and the model he/she is running isn't harmful. In this manner the requirement for making trust models is mentioning.

#### a. WHAT NEEDS TO BE DONE TO SOLVE THIS PROBLEM

Both the customer and the cloud provider event must guarantee that whatever requests/response they get is from a trusted in source by surveying the exactness of the data that they get. This should be conceivable by realizing a trust-based mechanism that continues running between the customer and the case before they start moving any veritable requesting/responses. The model will choose the trust at both the wraps up by testing each other with challenges and a while later pick whether the far edge is credible to manage requesting/give responses using the new hashing technique incorporating digital signatures with Role Based Security for secured, effective and efficient work model in cloud based application or apps.

#### b. FLOW OF WORK

The principle thought of the planned framework is accustomed to observing of the users, refreshes their restorative records quickly and stores this data in distributed storage using cloud infrastructure, simultaneously it gives the security and protection using enhanced augmented proposed security technique depicted in figure 3.1 to the users venerable records. The Proposed System utilizes mobile app based fundamental thought of the structured framework is accustomed to checking of the users, refreshes their restorative records promptly and stores this data in distributed storage simultaneously it gives the security and protection of the users record using the enhanced secured hashing model with RBS (Role Based Security Model).

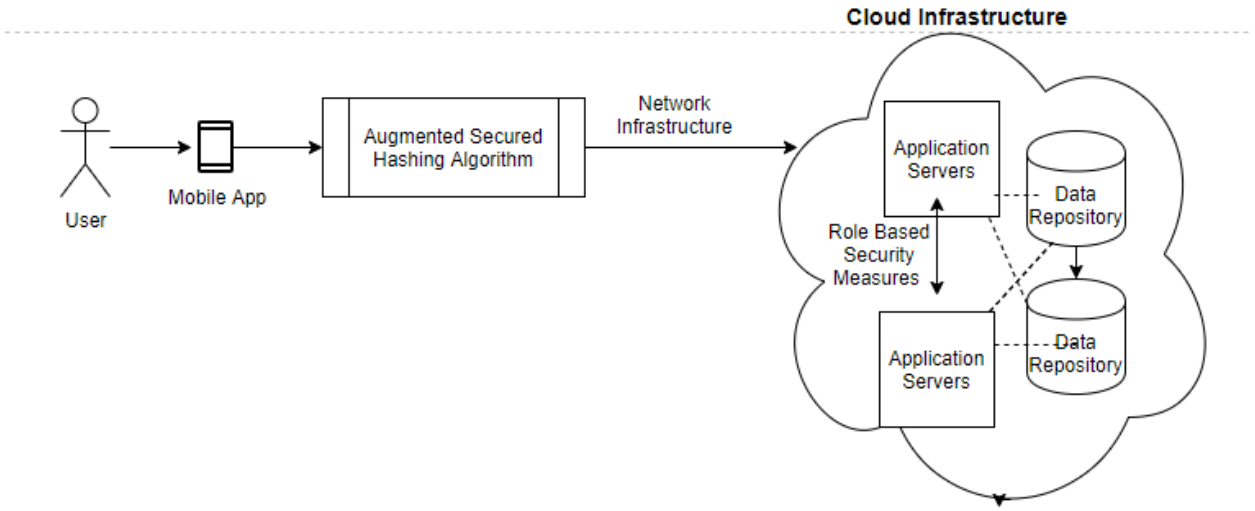



Figure 3.1: Proposed Scheme depicting the Mobile Based App using Augmented Security Measure in Cloud Infrastructure.

#### c. PROPOSED ALGORITHM

This proposed scheme and investigation address a cloud-assisted augmented protection system with insurance sparing the sensitive data especially in medical institutions. The Cloud development and security technique are used to give a positive condition to fabricate the adequacy and exactness with the assurance using the mobile application. The proposed scheme or approach fuses a cautious appraisal of the framework and recognized the potential perils, the addition of preparation security principles, and execution of framework security advancements. Proposed methodology to decide organize security-relevant issues on the proactive and reactive measures i.e. mobile app and central cluster in cloud using Role based Security. Using the proposed models can decrease database weight, and customers to get to data capably; the insurance control framework empowers customers to store data securely.

Proposed Algorithm:-

**Steps for Encryption:**

**i. Establish Numeral for Encryption:**

1. Choose indiscriminate number is formed amid the Range i.e. 8 and 65536
2. Determine the length of number is resolute.
3. Total of Unicode value (message) of number are evaluated a converted values.

Therefore, Random Number Value = Length + Sum of Unicode value as digits.

**ii. Determine Tz0, Tz1, Tz2 and Tz3 variables:**

- Tz0= Total of Numbers at odd random number
- Tz1= Total of Numbers at even random of magic-value number
- Tz2= Multiplication of Tz0 and Tz1
- Tz3= (random of from the range of Tz0 to Tz2) modulus (256)

**iii. Determine Tx0, Tx1,Tx2 and Tx3 variables:**

Whereas in respected to calculate the variables Tx0, Tx1, Tx2 and Tx3 values, encryption factors TsecBox [4][4] are required which are computed using Table below:

**Encryption Parameters ( Trn=random number )**

| TsecBox[4][4] | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | Tz0 ^ Tz1 | Trn + 15 | Tz2 ^ Tz3 | Trn * 15 |
| 1 | Tz0 ^ Tz2 | Trn + 25 | Tz1 ^ Tz3 | Trn * 25 |
| 2 | Tz0 ^ Tz3 | Trn + 35 | Tz1 ^ Tz2 | Trn * 35 |
| 3 | Tz2 ^ Tz3 | Trn + 45 | z1 ^ z3 | Trn * 45 |

Tx0=TsecBox[0][0]*TsecBox[0][1]^TsecBox[0][2]*TsecBox[0][3]; (1)
Tx1=TsecBox[1][0]+TsecBox[1][1]^TsecBox[1][2]*TsecBox[1][3]; (2)
Tx2=TsecBox[2][0]/TsecBox[2][1]*TsecBox[2][2]^TsecBox[2][3]; (3)
Tx3=TsecBox[3][0]*TsecBox[3][1]*TsecBox[3][2]^TsecBox[3][3]; (4)

**iv. Determine Tv0,Tv1,Tv2,TTv3 variables:**

Tv0=((TsecBox[2][0]^ TsecBox[2][1])*Tz0)+Tx2; (5)
Tv1=((TsecBox[1][0]^ TsecBox[1][2])*Tz1)+Tx1; (6)
Tv2=((TsecBox[0][0]^ secBox[0][3])*Tz2)+Tx0; (7)
Tv3=((TsecBox[3][1]^ TsecBox[3][2])*Tz3)+Tx3; (8)

**v. Evaluate replacement box (Secured-box) values using below table**

**Table Secured-Box values**

| TsecBox[4][4] | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | (TsecBox [0][0]^Tv0) *v0 | (TsecBox [0][1]^Tv1) *v0 | (TsecBox [0][2]^Tv2) *v0 | (TsecBox [0][3]^Tv3) *v0 | (secBox[0][4]^Tv 3) *v0 | (secBox [0][5]^Tv3) *v0 |
| 1 | (TsecBox [1][0]^Tv1) *Tv1 | (TsecBox [1][1]^Tv1) *Tv1 | (TsecBox [1][2]^Tv1) *Tv1 | (TsecBox [1][3]^Tv1) *Tv1 | (TsecBox [1][4]^Tv1) *Tv1 | (TsecBox[1][5] ^Tv1) *Tv0 |
| 2 | (TsecBox [2][0]^Tv2) *Tv2 | (TsecBox [2][1]^Tv1) *Tv2 | (TsecBox [2][2]^Tv2) *Tv2 | (TsecBox [2][3]^Tv3) *Tv2 | (TsecBox [2][4]^Tv3) *Tv2 | (TsecBox[2][5] ^Tv3) *Tv2 |
| 3 | (TsecBox [3][0]^Tv3) *Tv3 | (TsecBox [3][1]^Tv1) *Tv3 | (TsecBox [3][2]^Tv2) *Tv3 | (TsecBox [3][3]^Tv3) *Tv3 | (TsecBox [3][4]^Tv3) *Tv3 | (TsecBox[3][5] ^Tv3) *Tv3 |

**vi. Evaluate or Determine the Confidential-parameter:**

Confidential-parameter = Random Number (acquired vide step i) + erratically engendered input between 8 and 65536 + and random values obtained using Tz0, Tz1, Tz2 and Tz3 constraint (achieved in step ii) + Sum of Tx0, Tx1, Tx2 and Tx3 parameters (acquired in step iii) + Sum of Tv0, Tv1, v2 and Tv3 constraint (acquired in step iv)

**vii. Message or Data Encryption vide Hash Based Model**

- Knock over the plain-text (value/parameter) to be encrypted to attain Inequitable Meaning Encryption 1 .
- Execute Exponential TsecBox [index] (obtained in step 2) procedure to Inequitable Meaning Encryption 2.
- Execute Exponential Message parameter (obtained in step 3) procedure to compute Inequitable Meaning Encryption 3.
- Overturn Long values prearranged value of to calculate Inequitable Meaning Encryption 4 which will lead to consequential encrypted text.

**viii. Asymmetric Encryption of Message Parameter After Hash after Encryption 4**

- Form Manual Key Comprising of 16 Bit of Range Value from Unicode Character Set.
- Exponential Generation of Message Parameter based on Hash Values.
- Combine the Value in List Set and Pass as Strong Encrypted Text to Recipient.

More mathematically speaking, these three terms can be summed up using exponential values by comparing the best known attacks on these properties with optimal generic attacks. The length of the hash output is a key security parameter because it determines the overhead of generic attacks. For the minimum required security level of 120 bits in this scheme, because of the paradox for a hash function H: {0, 1} ^ {0, 1} n at least the condition rn = 8 between 65536. It is not necessary to make a case distinction according to the time of use of the method because the hash methods recommended in this scheme have digest length of rn = $2^8$ to $2^{64}$.

### 3.2 COMPARISON TABLE OF PROPOSED SCHEME WITH OTHER SECURITY ALGORITHMS BASED ON VARIOUS ATTRIBUTES AND FEATURE SELECTION

| Comparison Analyses of Proposed Algorithm | | | | | |
|---|---|---|---|---|---|
| **Characteristics** | **Blow Fish** | **RSA** | **DES** | **AES** | **Proposed** |
| Platform | Cloud Computing | Cloud Computing | Cloud Computing | Cloud Computing | Cloud Computing |
| Size | 32-448 bits | 1024 bits | 56 bits | 128,192,256 bits | 256 bits |
| Preliminary Vector Volume | 64 bits | 1024 bits | 64 bits | 128 bits | 64 Bits |
| Security | Users and providers are secure | Only users are secure. | Users and providers are secure. | Users and providers are secure. | Users and providers are secure. |
| Memory Usage | Execute in lower than 5 kb | Highest memory usage algorithm | Higher than AES | Low RAM | High Memory |
| Scalability | Scalable | Not scalable | Scalable | Scalable | Scalable |
| Information Encryption Capacity | Lower than AES | Encryption of small data | Lower than AES | Encryption of huge amount of data | Encryption of huge amount of data |
| Execution Time | Lower than AES | Maximum time | Same as AES | Faster than DES/RSA | Faster than rest |
| Key Used | One key for encryption and decryption. | Private key for decryption. Public key for encryption | One key for encryption and decryption. | One key for encryption and decryption. | Two key for encryption and decryption. |

Table 3.1 Comparative Analysis between various Security Algorithm and Proposed Scheme used in Cloud Computing

## 4. SIMULATION AND RESULTS

Above Signatures Scheme is a new enhanced hashing algorithm that usage security endeavors to ensure the made correspondence between two to progressively parties, resources, and structures using Shielded Virtual Resource in Cloud Computing. The decision motivation behind the mix of front-line confirmation or inscriptions is ensuring the suffering quality and flexibility of data correspondence among resources and frameworks. This assessment was pivoted around hash-based encryption systems; we have used sandbox-based substitution with displacing the joining descriptor key inside in the encryption structure, which ensures the flexibility of mechanized stamps and better execution. Supplementary prospect effort is to position our new anticipated strategy estimation into veritable firmware and framework correspondence structures with security. Regardless of how that we have secluded how the anticipated computation progress with the whole execution of security systems, the information has worn in our evaluation is made and might not be descriptive of this present reality conditions. We mean to complete a strong securing structure and use varying planning estimations during it to discover how our booking figuring can improve this present system's presentation and the projected plan can be used in firmware as expanded fortification using the robotized supporting or checks for assessing reason.

### 4.1 WORK FLOW INCORPORATION OF ABOVE MENTIONED SCHEME UNDERBAR CODE BASED CAR PARKING SYSTEM USING CLOUD RESOURCE

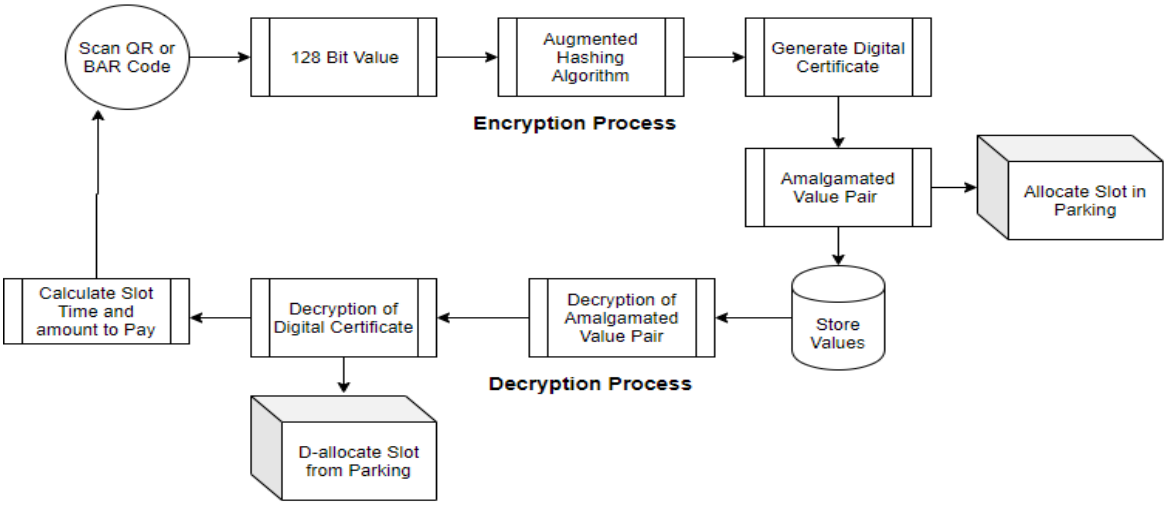



Figure 4.1: Workflow Diagram of Proposed Algorithm and Cloud App on Shielded Virtual Resource using Cloud Resource

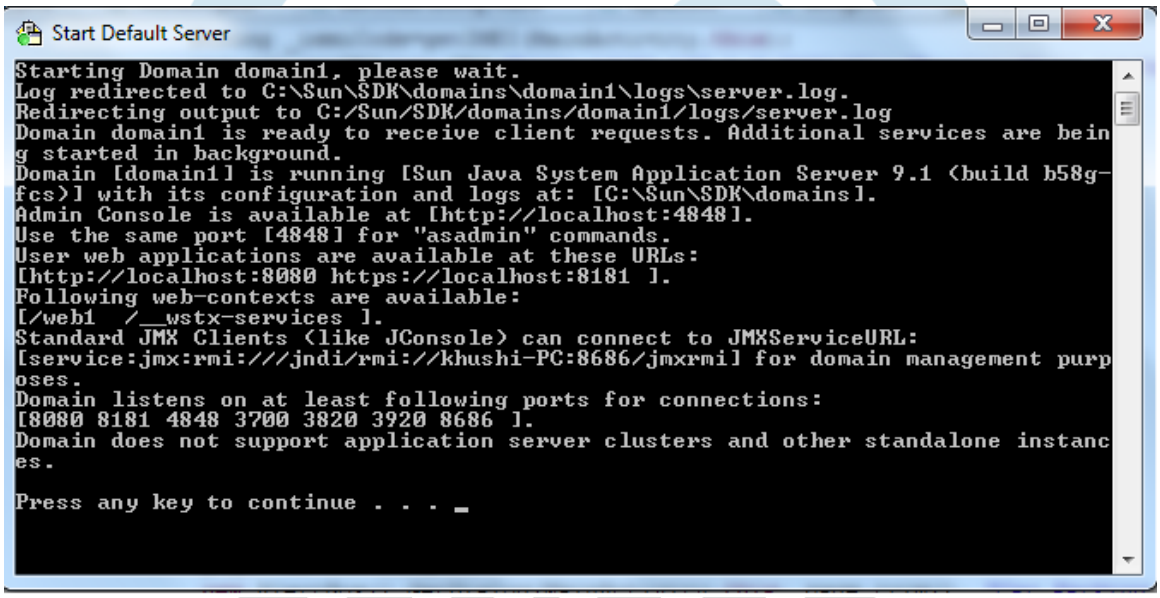



Fig. 4.2: Starting Sun One Web Application Server

Above Application Web Server will communicate with Shielded Cloud Based App and the values captured will be stored in data repository. The server side Java Server Page is responsible to interact with mobile app and storing the values in data vault.

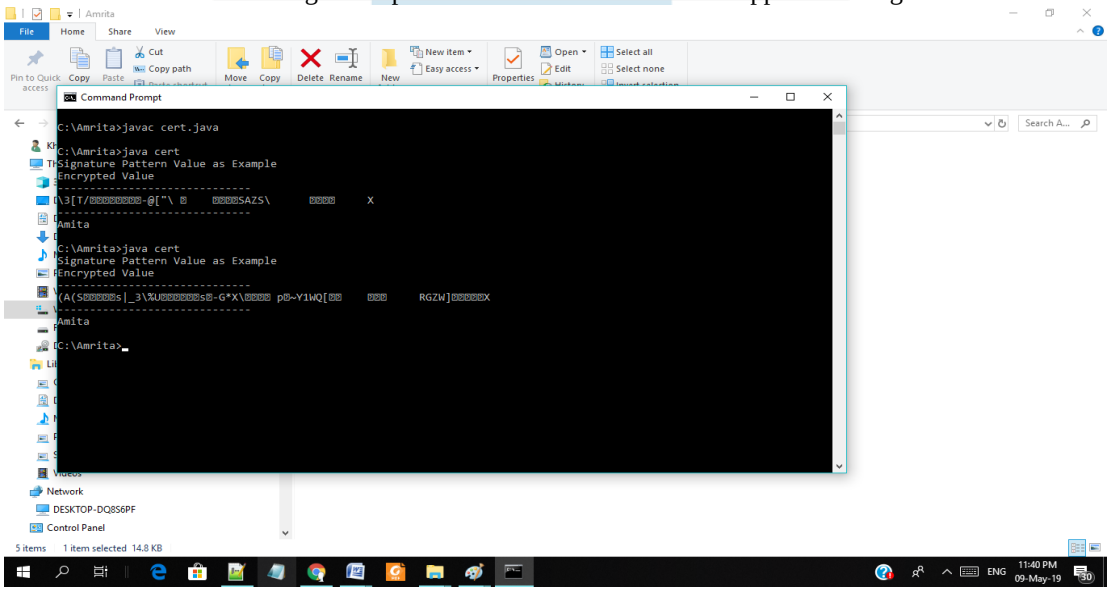


Figure 4.3 Digital Certificate Generated using Proposed Scheme

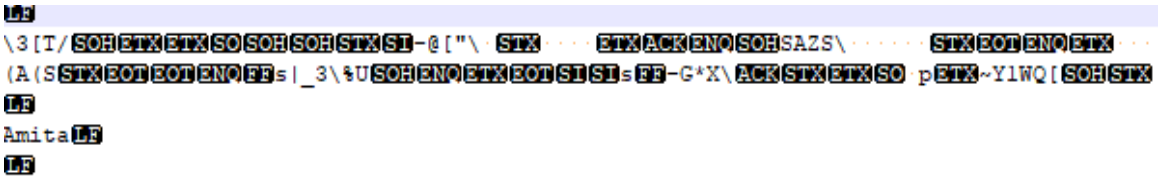



Figure 4..4 Cipher Data Generated using Proposed Scheme


Figure. 4.5: Car or Vehicle Smart Parking App Interface

The above interface will enable user to scan the BAR or QR code and send to central WAS using the proposed scheme.

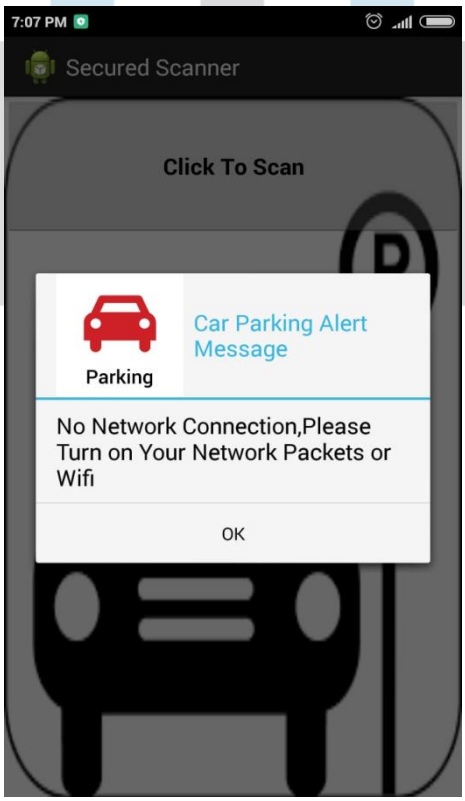



Figure. 4.6 Car or Vehicle Smart Parking Cloud Based App Interface using Above Scheme

The above screen shot depicts that, after scanning the bar or QR code the app will establish the connection with centre Web Application Server using Data Packets or Wire Transfer Agent using WiFi. However, If the network is down or weak the above message will be broadcasted to user via App. Even this will alert the user if the respected services are not been enabled.


Figure. 4.7: Bar Code Scanning System using App

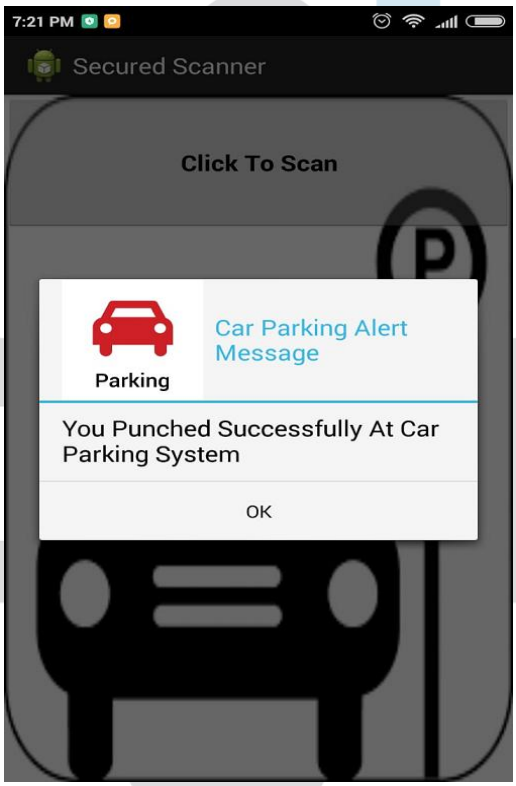
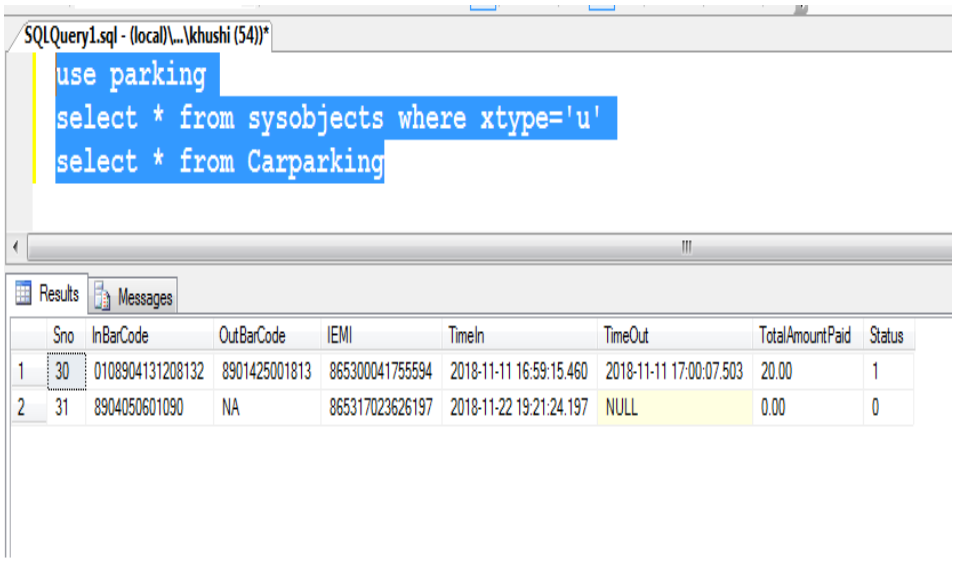



Fig. 4.8: Car or Vehicle Smart Parking App Interface Information Message on Successfully Registration or Entry

The above screen shot depicts that, after scanning the bar or QR code the app will establish the connection with centre Web Application Server using Data Packets or Wire Transfer Agent using WiFi. However, If the network is available the App will punch the current BarCode or QRCode Number along-with IEMEI number in central data repository successfully and revert with above message as confirmation of parking.




| | Sno | InBarCode | OutBarCode | IEMI | TimeIn | TimeOut | TotalAmountPaid | Status |
|---|---|---|---|---|---|---|---|---|
| 1 | 30 | 01089041312081 32 | 8901425001813 | 865300041755594 | 2018-11-11 16:59:15.460 | 2018-11-11 17:00:07.503 | 20.00 | 1 |
| 2 | 31 | 89040506010 90 | NA | 865317023626197 | 2018-11-22 19:21:24.197 | NULL | 0.00 | 0 |

Fig. 4.9: Entry Registration in Central Data Repository

The above screen shot depicts that, after scanning the bar or QR code the app will establish the connection with centre Web Application Server and preserve the BarCode or QRCode information along-with IEMEI number of respective mobile phone in central data repository and punch the time-in of the respected car using Web Application Server.

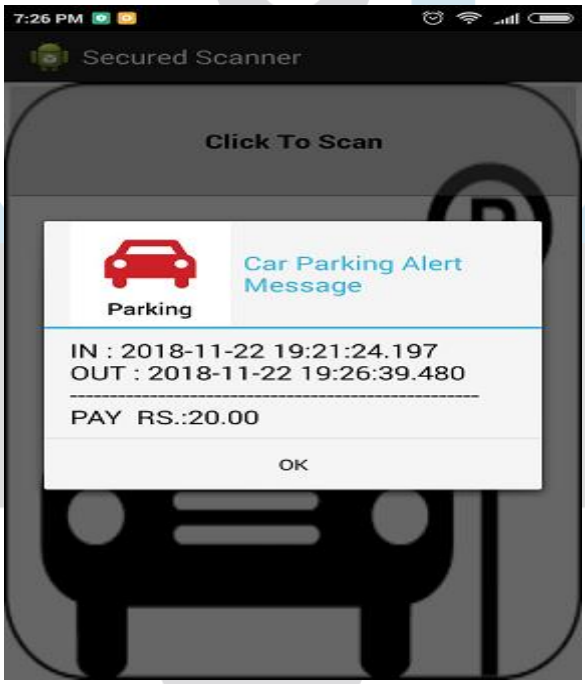



Figure .4.10: Car or Vehicle Smart Parking App Interface Information Message of Bill Payment on Exit

The above screen shot depicts that, after scanning the bar or QR code at the time of Exiting the parking the app will calculate the respective at the time the car is in and the car is out and will calculate the amount in accordance to duration.

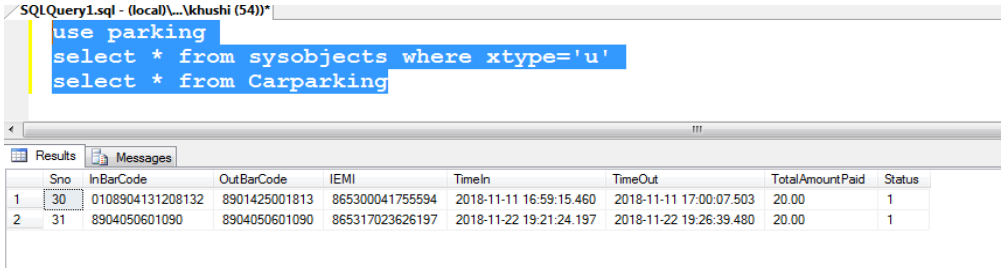



Figure 4.11: Car or Vehicle Smart Parking Central Data Repository Depicting Amount Collected at the Exit of Parking

The above screen shot depicts that what is in time of the vehicle and what is the out time of the vehicle and the amount charged in respect to the duration for the which the parking facility is availed by the user or client.

**4.2 TEST ENVIORNMENT**

To test the proposed conspire we have plotted the below mentioned ecosystem for calculation and evaluation.

| Machines | Processing Speed | Cache Memory | Processors | RAM | Bit | Processor Description | Virtual Machine |
|---|---|---|---|---|---|---|---|
| 1 | 2.1 GHZ | 1.4 MB | 4 | 4 GB | 32 | i3 | NO |
| 2 | 2.5 GHZ | 2.4 MB | 4 | 8 GB | 64 | i3 | NO |

Table 4.2: Resources Used for Performance Evaluation

| Resource | Processing Time in Seconds |
|---|---|
| 1 | 1.127 |
| 2 | 0.723 |

Table 4.3 : CPU Time in Seconds using under Different Virtual Resources

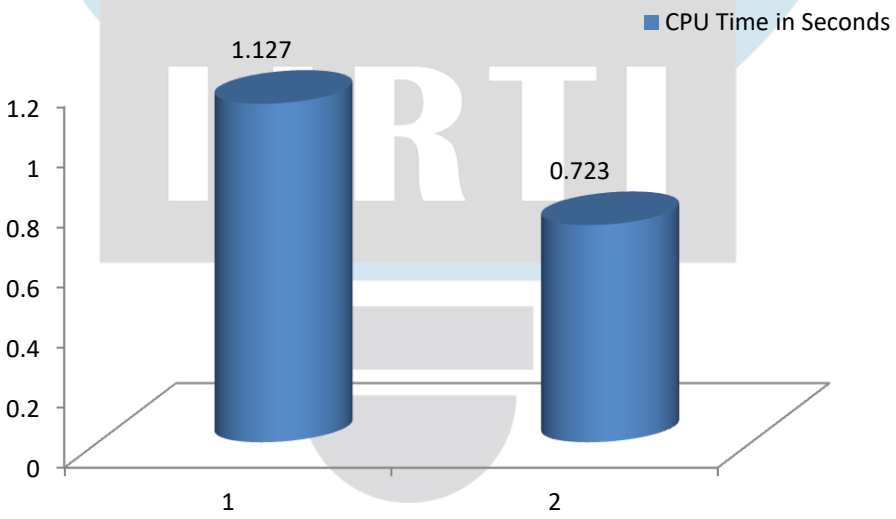



Chart 4.1: Results Depicted using Bar Graph

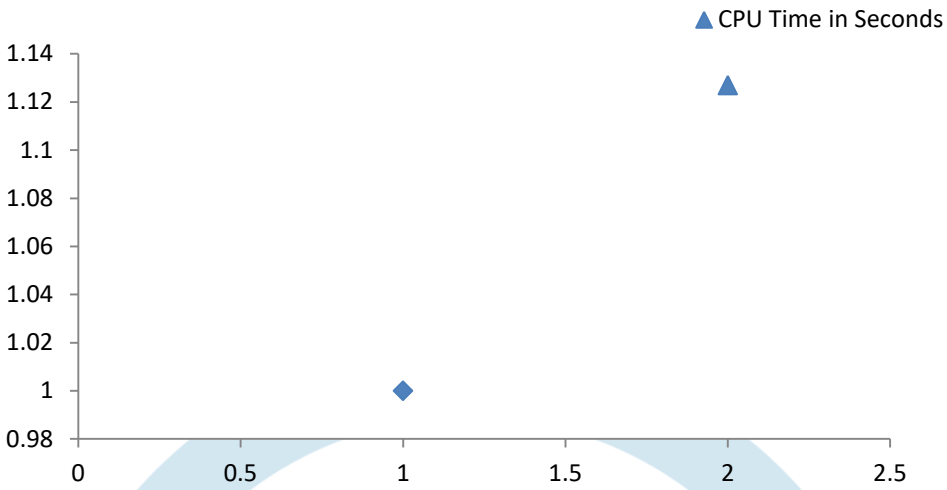



Chart 4.2: Results Depicted using Surface Model

From a theoretical point of view, one of the major problems evokes in many articles is to find a scheme for securing data stored, and guaranteeing confidentiality in the Cloud environment and which is secure in the standard model. Another problem is to design diagrams which allow data integrity to be checked. It would then be interesting to study the cryptography based on digital signatures, fingerprints, hashing, so it's theoretically possible to use it to guarantee and to facilitate the data is not distorted. In this way, one could hope to obtain a scheme which is more effective. For the third part: the above scheme that we have proposed is articulated on XOR based hashing algorithm. It is interesting to build achieving the proposed enhanced security paradigm, this will make more difficult for malicious people or resources to compromise the system. It will be a prospect desirable to have the result of a fully encrypted application in the SaaS level of Cloud.

## 5. CONCLUSION AND FUTURE SCOPE

### 5.1 Conclusion

This thesis focused on the challenges related to the security of data in transition between various resources over cloud resources either which is inside the system or outside the system and data stored in the Datacenters of the Cloud provider. We studied cryptography as well as its use for the realization of secure data storage on data servers. This conclusion is an opportunity to recall the different contributions of this thesis and to give some perspectives for future research. In the first chapter, we are focused on the concept of Cloud Computing we presented the objective and general definition of the concept of cloud computing, Then we described the system architecture, the deployment model, and the characteristics essential. We also clarified the conditions, opportunities, and challenges that exist in its development, as well as the obstacles that hinder the adoption of this new solution by professionals where the main concern security is focused on the contextual level. In the second chapter, we presented the literature survey, and existing security scenarios available in the Cloud architecture, the security standards and strategies are even emphasized.. Then, we proposed our approach concerning security in Cloud Computing allowing and ensuring data security and the availability of the service with integrity and confidentiality while transiting data from one resource to another or others (inside/outside). Consequently, the proposed hashing algorithm based encryption will become more essential for cloud services to improve system performance and security over communication. Hashing encryption in the cloud is still relatively young and is only being adopted at a slow pace. The proposed scheme will make it more difficult for attackers (outsiders/insiders) to compromise the system and to access the confidential data.

### 5.2 Future Scope

For the future scope, the proposed scheme can be inculcated as firmware in cloud architecture for better security parameters for authorization and authentication.

**References**

[1] National Research Council. 1999. Funding a Revolution: Government Support for Computing Research. Washington, DC: The National Academies Press. https://doi.org/10.17226/6323.

[2] Qi, Lianyong&Khosravi, Mohammad & Xu, Xiaolong& Zhang, Yiwen& Menon, Varun. (2021). Cloud Computing. 10.1007/978-3-030-69992-5.

[3] Beri, Rydhm& Singh, Jaspreet. (2020). Cloud computing.

[4] P, Krishna Sankar& N P, Shangaranarayanee&Saravanan, K.. (2020). CLOUD COMPUTING.

[5] Manvi, Sunilkumar&Shyam, Gopal. (2021). Cloud Computing: Concepts and Technologies. 10.1201/9781003093671.

[6] Kumar, Abhishek &Sanjeevikumar, P. &kumar, vishal. (2021). Blockchain Security in Cloud Computing. 10.1007/978-3-030-70501-5.

[7] P, Krishna Sankar& N P, Shangaranarayanee&Saravanan, K.. (2020). CLOUD COMPUTING.

[8] https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france

[9] FRAUD THE FACTS 2019 | THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD

[10] John Gantz and David Reinsel, THE DIGITAL UNIVERSE IN 2020: Big Data, Bigger Digital Shadow s, and Biggest Grow th in the Far East, https://www.cs.princeton.edu/courses/archive/spring13/cos598C/idc-the-digital-universe-in-2020.pdf

[11] https://www.cloudtp.com/doppler/cloud-economics-getting-bigger-picture/

[12] https://www.vxchnge.com/blog/different-types-of-cloud-computing

[13] Hayes, Patrick & Morgenstern, Leora. (2007). On John McCarthy's 80th Birthday, in Honor of His Contributions. AI Magazine. 28. 93-102. 10.1609/aimag.v28i4.2063.

[14] David W Cearley, Cloud Computing: Key Initiative Overview, Gartner Report, 2010

[15] Peter Mell and Tim Grance, The NIST Definition of Cloud Computing, version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory, www.csrc.nist.gov, 7 Oct 2009

[16] Dustin Amrhein and Scott Quint, Cloud Computing for the Enterprise: Part 1: Capturing the Cloud, DeveloperWorks, IBM, 8 Apr 2009

[17] John Rhoton, Cloud Computing Explained: Implementation Handbook for Enterprises, Recursive Press, 3 May 2010

[18] Kartit, Zaid &Azougaghe, Ali &Idrissi, H. & El marraki, Mohamed & Mustapha, Hedabou&Belkasmi, Mostafa & Ali, Kartit. (2016). Applying Encryption Algorithm for Data Security in Cloud Storage. 10.1007/978-981-287-990-5_12.

[19] Saichyshyna, Nataliia. (2020). ELGAMAL ENCRIPTION. 10.36074/11.12.2020.v2.02.

[20] Mohit, Prerna& Biswas, G.. (2021). Modification of ElGamal Cryptosystem into Data Encryption and Signature Generation. 10.1007/978-981-33-4788-5_10.

[21] https://cloudnine.com/ediscoverydaily/electronic-discovery/according-to-idc-big-data-is-only-getting-bigger-ediscovery-trends/

[22] MihailDimitrov, Ibrahim Osman, The Impact of Cloud Computing on Organizations in Regard to Cost and Security, Department of informatics, https://www.diva-portal.org/smash/get/diva2:728880/FULLTEXT02

[23] Bennett, David & Mason, Jeffrey. (2014). Secure cloud computing infrastructure.

[24] Komarek, Ales &Pavlik, Jakub &Sobeslav, Vladimir. (2017). Performance Analysis of Cloud Computing Infrastructure. 303-313. 10.1007/978-3-319-65515-4_25.

[25] Britannica, The Editors of Encyclopaedia. "John McCarthy". Encyclopedia Britannica, 20 Oct. 2020, https://www.britannica.com/biography/John-McCarthy. Accessed 1 April 2021.

[26] Piper, Ben & Clinton, David. (2019). Amazon Elastic Compute Cloud and Amazon Elastic Block Store. 10.1002/9781119560395.ch2.

[27] Vohra, Deepak. (2016). Using the Amazon EC2. 10.1007/978-1-4842-1830-3_15.

[28] Acuña, Pablo. (2016). Amazon EC2 Container Service. 10.1007/978-1-4842-2415-1_4.

[29] Bhise, Vidya& Mali, Ajit. (2013). Cloud resource provisioning for Amazon EC2. 1-7. 10.1109/ICCCNT.2013.6726565.

[30] McGilvary, Gary & Barker, Adam & Atkinson, Malcolm & Lloyd, Ashley. (2011). Performance and cost variability of Amazon EC2.

[31] Dilma Da SilvaQingyangWangLiang-Jie Zhang, Cloud Computing – CLOUD 2019, 12th International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings

[32] Gong, Chunye& Liu, Jie& Zhang, Qiang& Chen, Haitao& Gong, Zhenghu. (2010). The Characteristics of Cloud Computing. Proceedings of the International Conference on Parallel Processing Workshops. 275-279. 10.1109/ICPPW.2010.45.

[33] Vidosav, Majstorovic&Stojadinovic, Slavenko. (2020). Cloud Computing. 10.1201/9780429055621-5.

[34] Ayyappa, Sanneboina. (2020). cloud computing..

[35] Farwick, Matthias & Schmidt, Tobias &Trojer, Thomas. (2020). Cloud Computing. 10.3139/9783446462809.007.

[36] Natrajan, Nidhi. (2020). Cloud Computing.

[37] Bhowmik, Sandeep. (2020). Popular Cloud Services. 10.1017/9781316941386.021.

[38] Baldwin, Paula. (2017). Cloud Services. 10.1007/978-3-319-32001-4_37-1.

[39] Alves Ferreira, Anderson & Bastos-Filho, Carmelo. (2013). Cloud services. 59-64. 10.1109/LatinCloud.2013.6842224.

[40] Hill, Richard & Hirsch, Laurie & Lake, Peter &Moshiri, Siavash. (2013). Cloud Services. 10.1007/978-1-4471-4603-2_5.

[41] Cambron, G.. (2012). Cloud Services. 10.1002/9781118394519.ch7.

[42] Schaper, Joachim. (2010). Cloud Services. 91 - 91. 10.1109/DEST.2010.5610668.

[43] Chauhan, Sidhartha& Cuthbert, Dave & Devine, James &Halachmi, Alan &Lehwess, Matt & Matthews, Nick &Morad, Steve & Seymour, Steve & Walker, Dave. (2018). Service Requirements. 10.1002/9781119549000.ch11.

[44] Campbell, David &Kakivaya, Gopal & Ellis, Nigel. (2010). Extreme scale with full SQL language support in microsoft SQL Azure. 1021-1024. 10.1145/1807167.1807280.

[45] S. P. T., Krishnan & Gonzalez, Jose. (2015). Google Cloud SQL. 10.1007/978-1-4842-1004-8_7.

[46] Sabharwal, Navin& Edward, Shakuntala. (2020). Hands On Google Cloud SQL and Cloud Spanner: Deployment, Administration and Use Cases with Python. 10.1007/978-1-4842-5537-7.

[47] Balamurugan, Balamurugan&Abirami, R &Kadry, Seifedine&Gandomi, Amir. (2021). NoSQL Database. 10.1002/9781119701859.ch3.

[48] Martins, Pedro & Tomé, Paulo &Wanzeller, Cristina &Sá, Filipe &Abbasi, Maryam. (2021). NoSQL Comparative Performance Study. 10.1007/978-3-030-72651-5_41.

[49] Franklin, Curtis & Chee, Brian. (2019). Private Cloud. 10.1201/9780367259433-13.

[50] Beach, Brian &Armentrout, Steven & Bozo, Rodney &Tsouris, Emmanuel. (2019). Virtual Private Cloud. 10.1007/978-1-4842-4850-8_5.

[51] Collins, Lauren. (2016). Virtual Private Cloud. 10.1201/9781315372211-9.

[52] Franklin, Curtis & Chee, Brian. (2019). Public Cloud. 10.1201/9780367259433-12.

[53] Sehgal, Naresh & Bhatt, Pramod&Acken, John. (2020). Features of Private and Public Cloud. 10.1007/978-3-030-24612-9_4.

[54] Serhane, Yassine&Sekkaki, Abderrahim&Abid, Mehdi. (2020). Cost Effective Cloud Storage Interoperability Between Public Cloud Platforms. International Journal of Communication Networks and Information Security. 12. 440-449.

[55] Shah, Nirav. (2019). Survey in data security of public cloud.

[56] Khan, Amin &Freitag, F. & Navarro, Leandro. (2016). Community Clouds. 10.1002/9781118821930.ch4.

[57] Marinos, Alexandros & Briscoe, Gerard. (2009). Community Cloud Computing.. 472-484.

[58] kavita, Dr. (2014). cloud computing book.

[59] Franklin, Curtis & Chee, Brian. (2019). Hybrid Cloud. 10.1201/9780367259433-14.

[60] Chatterjee, Rithik. (2021). Red Hat Hybrid Cloud Infrastructure. 10.1007/978-1-4842-6434-8_2.

[61] Missbach, Michael &Staerk, Thorsten & Gardiner, Cameron & McCloud, Joshua &Madl, Robert &Tempes, Mark & Anderson, George. (2016). The Hybrid Cloud. 10.1007/978-3-662-47418-1_7.

[62] Manduri, Afzal & Ghani, Anwar &Daud, Ali &Chronopoulos, A. & Jalal, Ateeqa. (2020). Revenue Maximization Approaches in IaaS Clouds: Research Challenges and Opportunities.

[63] Gomathi, Ms. (2020). A Study on Cloud Computing Architecture and Research Challenges on Cloud Computing. International Journal for Research in Applied Science and Engineering Technology. 8. 947-955. 10.22214/ijraset.2020.32341.

[64] Silva, Paulo & Monteiro, Edmundo &Simoes, Paulo. (2021). Privacy in the Cloud: A Survey of Existing Solutions and Research Challenges. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3049599.

[65] Cuadrado, Félix &Navas, Álvaro &Dueñas, Juan & Vaquero, Luis. (2014). Research challenges for cross-cloud applications. Proc. of the IEEE INFOCOM Workshop on Cross-cloud Systems (CrossCloud 2014), Toronto, Canada. 19-24. 10.1109/INFCOMW.2014.6849162.

[66] Keshavarzi, Amin &Haghighat, Abolfazl&Bohlouli, Mahdi. (2020). Research Challenges and Prospective Business Impacts of Cloud Computing: A Survey.

[67] https://www.csoonline.com/article/2123964/cisco-ceo--cloud-computing-a--security-nightmare-.html

[68] Krishnamurthy, Sandeep. (2005). Amazon.com - A Comprehensive Case History.

[69] Oualline, Steve &Oualline, Grace. (2018). Using Google Docs. 10.1007/978-1-4842-3075-6_16.

[70] Oualline, Steve &Oualline, Grace. (2018). Using Gmail. 10.1007/978-1-4842-3075-6_15.

[71] Owens, Kenon. (2007). Virtualization/VMware..

[72] K, Arthi&Vijayalakshmi, R. & v, Vijayalakshmi. (2013). Cloud Linkup: Scrutinizing Among Cloud Applications for Business Perspective to Desire the Technological Shift in Miniature Dealings. 6. 64-67.

[73] Georgiou, Dimitra &Lambrinoudakis, Costas. (2015). Cloud Computing Security Requirements and a Methodology for Their Auditing. 10.1007/978-3-319-27164-4.

[74] Iankoulova, Iliana &Daneva, Maya. (2012). Cloud computing security requirements: A systematic review. Proc. 6th Int. Conf. Research Challenges in Information Science (RCIS 2012). 1-7. 10.1109/RCIS.2012.6240421.

[75] Fazil, Shivan. (2012). Cloud Computing Security. 10.13140/RG.2.1.2499.2407.

[76] Bordak, Lukas. (2019). Cloud Computing Security. 87-92. 10.1109/ICETA48886.2019.9040043.

[77] Samani, Raj & Honan, Brian & Reavis, Jim. (2015). Chapter 8. Cloud Security Alliance Research. 10.1016/B978-0-12-420125-5.00008-X.

[78] Sen, Amartya & Madria, Sanjay. (2018). Data Analysis of Cloud Security Alliances Security, Trust, and Assurance Registry. 10.1145/3154273.3154343.

[79] Rajan, Sreeranga & Ginkel, Wilco & Sundaresan, Neel &Bardhan, Anant & Chen, Yu & Fuchs, Adam &Kapre, Aditya & Lane, Adrian & Lu, Rongxing & Manadhata, Pratyusa & Molina, Jesus &Cardenas, Alvaro & Murthy, Praveen & Roy, Arnab & Sathyadevan, Shiju & Shah, Nrupak. (2013). Cloud Security Alliance report on the Top Ten Challenges in Big Data Privacy and Security. 10.13140/RG.2.1.1744.1127.

[80] Manvi, Sunilkumar&Shyam, Gopal. (2021). Cloud Security. 10.1201/9781003093671-11.

[81] Yao J., Zimmer V. (2020) Cryptography. In: Building Secure Firmware. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6106-4_19
[82] Stein LD (1998) Web security: a step-by-step reference guide. Addison-Wesley, Boston Google Scholar .
[83] Kaeo M (1999) Designing network security. Cisco Press, Indianapolis Google Scholar.
[84] Stallings W (1999) Cryptography and network security: principles and practice, 2nd edn. Prentice Hall, Upper Saddle River Google Scholar
[85] A.Kizza J.M. (2020) Cryptography. In: Guide to Computer Network Security. Texts in Computer Science. Springer, Cham. https://doi.org/10.1007/978-3-030-38141-7_11 Kerckhoffs. La cryptographiemilitaire. University Microfilms, 1978. 21
[86] Aruljothi, S. &Venkatesulu, iM. (2010). Symmetric Key Cryptosystem Based on Randomized Block Cipher. 2010 5th International Conference on Future Information Technology, FutureTech 2010 - Proceedings. 1 - 5. 10.1109/FUTURETECH.2010.5482692.
[87] Tamura, Shinsuke. (2012). Encryption and Decryption. 10.4018/978-1-4666-1649-3.ch002.
[88] Rashidi, Bahram. (2019). Cryptographic algorithms. 10.1049/PBSE009E_ch4.
[89] Schneier, Bruce. (2015). Cryptographic Algorithms. 10.1002/9781119183471.part3.
[90] Daemen, Joan &Rijmen, Vincent. (2020). The Design of Rijndael The Advanced Encryption Standard (AES): The Advanced Encryption Standard (AES). 10.1007/978-3-662-60769-5.
[91] Klima, Richard &Sigmon, Neil &Stitzinger, Ernest. (2015). The Advanced Encryption Standard. 10.1201/b19010-10.
[92] Miah, Md. (2014). Advanced Encryption Standard.
[93] Robertazzi, Thomas. (2012). Advanced Encryption Standard (AES). 10.1007/978-1-4614-2104-7_10.
[94] Altigani, Abdelrahman& Hasan, Shafaatunnur& Barry, Bazara&Shamsuddin, SitiMariyam. (2018). Key-dependent Advanced Encryption Standard. 10.1109/ICCCEEE.2018.8515761.
[95] Afifah, Nur&Fanani, Aris& Farida, Yuniar&Intan, Putroue. (2018). Image Cryptographic Application Design using Advanced Encryption Standard (AES) Method. 247-254. 10.5220/0008905502470254.
[96] Gary C. Kessler, An Overview of Cryptography, 16 December 2020. https://www.garykessler.net/library/crypto.html
[97] Daemen, Joan &Rijmen, Vincent. (2020). Cryptanalysis. 10.1007/978-3-662-60769-5_10. (2020). Cryptanalysis Attacks and Techniques. 10.1007/978-1-4842-6367-9_19.
[98] Mihailescu M.I., Nita S.L. (2021) Implementation and Practical Approach of Cryptanalysis Methods. In: Pro Cryptography and Cryptanalysis. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-6367-9_24
[99] Banik, Subhadeep&Bossert, Jannis& Jana, Amit & List, Eik& Lucks, Stefan & Meier, Willi & Rahman, Mostafizar&Saha, Dhiman& Sasaki, Yu. (2019). Cryptanalysis of ForkAES. 10.1007/978-3-030-21568-2_3.
[100] Xin, Wenqian& Liu, Yunwen& Sun, Bing & Li, Chao. (2019). Improved Cryptanalysis on SipHash. 10.1007/978-3-030-31578-8_4.
[101] Roman'kov, Vitaly. (2020). Algebraic cryptanalysis and new security enhancements. Moscow Journal of Combinatorics and Number Theory. 9. 123-146. 10.2140/moscow.2020.9.123.
[102] Dobraunig, Christoph &Eichlseder, Maria & Mendel, Florian &Schofnegger, Markus. (2020). Algebraic Cryptanalysis of Variants of Frit. 10.1007/978-3-030-38471-5_7.
[103] Lu, Jinyu& Liu, Yunwen& Ashur, Tomer& Sun, Bing & Li, Chao. (2020). Rotational-XOR Cryptanalysis of Simon-Like Block Ciphers. 10.1007/978-3-030-55304-3_6.
[104] Horáček, Jan. (2020). Algebraic and Logic Solving Methods for Cryptanalysis.
[105] Padate, Roshni et al. “Encryption and Decryption of Text using AES Algorithm.” (2014).