Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3242092, 9 pages
https://doi.org/10.1155/2022/3242092

Research Article

Improved Data Security in Cloud Environment for Test Automation Framework and Access Control for Industry 4.0

Pradeep Kumar Tiwari,[1] **Sunil Kr Pandey**,[2] **W. Thamba Meshach**,[3] **Jyoti Parashar**,[4] **Ankit Kumar**,[5] **Majid Altuwairiqi**,[6] **and Daniel Krah**[7]

[1]*Manipal University Jaipur, Jaipur, India*
[2]*Institute of Technology & Science, Ghaziabad, Uttar Pradesh, India*
[3]*Department of Computer Science and Engineering, Prathyusha Engineering College, Thiruvallur, Chennai, Tamilnadu, India*
[4]*Department of Computer Science & Application, Maharishi Markandeshwar (Deemed to Be University), Haryana, India*
[5]*Department of Computer Engineering and Applications, GLA University, Mathura, Uttar Pradesh, India*
[6]*Department of Computer Science, College of Computers and Information Technology, Taif University, Saudi Arabia*
[7]*Tamale Technical University, Ghana*

Correspondence should be addressed to Daniel Krah; dkrah@tatu.edu.gh

Received 8 April 2022; Revised 1 May 2022; Accepted 9 May 2022; Published 25 May 2022

Academic Editor: Kalidoss Rajakani

In analyzing project regressions, automation has emerged as a major agenda in managing changes in software which requires minimum manual intervention. For rapid testing environment, software development processes such as Agile, Scrum, and XP processes depend on continuous integration tools. There is no single tool to handle the project automation, and the main challenge is dependency on multiple tools. The proposed automation tool should support configuration, execution, and debugging facility. Integrating the project automation works such as software configuration management tools Mercurial and Git, job scheduling tools like Jenkins and Apache Continuum, test management tools like TestNG and Selenium need tight integration which is a challenge. The existing PKI infrastructure for access control does not share data among the software tools and processes increasing the complexity when an organization needs to leverage the existing cloud services. The proposed approach optimizes the execution time by taking single CSV with input test case and metadata information and efficiently group and executes the tests automatically. The proposed method includes implementation of security access control mechanism for the jobs execution platform in cloud environment.

1. Introduction

We provide the network telemetry data in a safe manner via approved third parties, while maintaining the ability to search on the encrypted network telemetry while maintaining privacy. We conducted an experimental investigation into the construction of a privacy-preserving search algorithm employing upgraded security algorithms such as ID-PKC and ABE [1].

It is necessary to have a quick development environment for the software that will be distributed on the cloud platform in order to check for flaws in the produced software before providing it. This fast software development necessitates the establishment of a scalable and secure infrastructure that is infallible [2]. However, even while cloud systems allow for the rapid development of products, they still need the assistance of automation tools in order to fully use the build and test environments [3]. With the help of cloud virtualization services, the suggested solution handles the issue of building and testing a framework in a cloud environment [4].

The proposed architecture employs an integrated security framework that makes use of identity-based cryptosystems and ABE to ensure that tasks are executed securely and with greater resistance against vulnerabilities associated with cloud deployment. [5].

It is only via the implementation of appropriate defensive measures that cloud security architecture can be considered effective [6].

When designing a cloud security architecture, it is important to think ahead and anticipate the issues that may arise throughout the security management process.

[7] Security controls are implemented in order to address the issues highlighted by the security management team. It is necessary to have these controls in place in order to safeguard the system from any faults and to minimize the effect of an attack [8]. Despite the fact that there are multiple different types of controls behind a cloud security [9] architecture, they are all susceptible to being exploited. Most of the time, they may be found in one of the following classifications: it is possible to safeguard a system against occurrences by preventing them from happening, which is what preventive controls are designed to do [10]. Minimizing or lowering, if not fully eliminating, certain vulnerabilities, examples include cloud customers who require strong authentication, which reduces the likelihood that unauthorized users will be able to access cloud systems and increases the likelihood that authorized users will be able to access cloud systems when they can be positively identified by the cloud service provider [11]. The goal of detective controls is to detect and react appropriately to any irregularities that may occur [12]. The detective has complete influence over the events that go happen. In the event of an attack, a detective control will notify those responsible for taking preventative or defensive actions. Corrective actions are being implemented in order to resolve the issue [13]. Monitor the security of your systems and networks, including intrusion detection and prevention. Cloud system attacks are often recognized and stopped by the use of detection and prevention processes, which are implemented in the network architecture that facilitates communication. Correlative controls aid in mitigating the consequences of an occurrence, often by preventing them from happening in the first place [14].

Keeping the amount of damage to a bare minimum, they have an influence on the situation either during or shortly after it occurs. Information is stored in the database, which is the backup of the system.

Corrective controls, such as the need to repair a compromised system, are instances of this kind of regulation. The importance of cloud security is widely acknowledged in its many dimensions, with the general consensus being that information security safeguards should be implemented, chosen, and executed according to and in proportion to the risks, which is frequently accomplished through threat assessment [15].

Some of the cloud's numerous service models, such as IAAS, PaaS, and SAAS, are included below, as well as the many deployment options available, which are listed below. Security issues/concerns impact a wide range of organizations, including private, public, hybrid, and community-based organizations that use cloud computing services to operate [16]. However, these difficulties develop as a consequence of the following factors:

There have been concerns made regarding cloud security by both cloud providers (organizations that supply software, platform, or infrastructure as a service through the cloud) and cloud customers (companies or organizations that employ clouds services) [17].

Cloud computing is a technique for hosting programs and storing data in a remote location. It is likely that the major culpability is split between the two parties in this situation. To evaluate whether or not a cloud provider's cloud environment is safe, as well as whether or not their users' cloud environments are safe, we must first assess if the cloud provider's cloud environment is safe [18]. In the case of a cloud-based application or data, all of the associated information and data is safeguarded and transferred to a safe place. Now, the cloud client is generating very strong passwords and performing all of the necessary authentication processes in the background.

Cloud administrators are those who choose to utilize a cloud application that has already been saved in the cloud. When a cloud manager or agency makes the decision to use a cloud application that has already been stored in the cloud, the cloud management or agency is referred to as a cloud administrator [19]. Users upload their data to the public cloud, which is housed inside the data center. A significant amount of potential exists in its manufacturing.

There is the possibility that some attacks may reveal critical and secret information. In the wake of a recent cloud security incident, many attacks on cloud computing infrastructure have been reported, causing widespread worry [20]. It is now the cloud service provider's obligation to ensure that all of the background information with details is accurate. Using cloud computing, organizations may save resources, cut costs, and retain efficiency [21]. Keeping the data of a number of clients on the same server is standard practice among service providers. There is a consequent rise in the possibility that other users will be able to view private information belonging to a single individual as a result of this development (possibly even competitors). It is necessary for cloud service providers to ensure that data segregation and logical storage are effectively implemented segregated in order to cope with sensitive circumstances [22]. It is clear that the extensive usage of virtualization in the development of cloud infrastructure is a major benefit in this context. Customers or tenants of a public cloud service could be concerned about the security of their data. The relationship between the operating system and the underlying hardware—whether it be for computing, storage, or networking—is transformed as a consequence of virtualization [23]. This is the point at which everything starts. An additional layer—-virtualization—must be properly configured, regulated, and maintained in order to be secure. Concerning virtualization software in particular, there is the potential of compromising the program or the danger of data loss in the "hypervisor." However, despite the fact that these concerns are mostly hypothetical, they do exist [24].

Cloud infrastructures are nothing more than a new kind of computer network that is hosted on the internet. This indicates that clouds will have the same characteristics that they have now. Any network infrastructure will be protected to some extent (for example, by intrusion detection and prevention systems). It is up to the cloud to make the decision.

It is the vendor's obligation (whether you or a third party) to determine the level of security that is required. The International Organization for Standardization (ISO) is a nongovernmental organization that sets international standards (ISO). Several information security standards have been created by the International Organization for Standardization (ISO) in the field of information security.

ISO 27001 and ISO 27002 are standards for information security management. The ISO 27001 standard is applicable to all sorts of enterprises. The International Organization for Standardization (ISO) 27002 is likewise tailored to the specific requirements of the business, but it is meant to assist in meeting those criteria. Security risks are assessed by a security risk assessment (ISO (2), 2008) [25]. There is a continuing argument between IT and the rest of the world private clouds that are more secure than public clouds, according to industry experts. Some researchers and experts believe that consequently, there has been no lack of discussion and concern about the security risks associated with public cloud computing [26]. The challenges that computers present are as follows. It is fair to be concerned, particularly if sensitive data and critical applications are in the hands of a third party who is not under your immediate control [27]. Aside from the widely held belief that owning property is a good investment, clouds should be more secure, and there are two types of cloud computing: public cloud computing and private cloud computing. Security Matters 8 discusses some of the fascinating characteristics and aspects of public clouds that should be taken into consideration. The National Institute of Standards and Technology (NIST) is the meaning of the term "public." The term "clouds" refers to information that is made accessible to the general public or a huge industry group [28]. As a result, public cloud service providers are significantly more attractive targets for hackers than private cloud service providers. Public [29] clouds also attract the most qualified security personnel available; the largest and most successful cloud service companies have the most qualified security personnel. They have millions of clients who depend on them. They would almost certainly be picky about who they hired in the first place [30]. Also, the public cloud providers, particularly the bigger corporations such as Google, Amazon, and Facebook, would benefit from this. It is significantly simpler for a small to midsize private corporation to get the most up-to-date security equipment. Concerning public cloud computing, there are many factors to consider [31].

Cloud storage is defined as "the storage of data online in the cloud," in which case a company's data is kept in various dispersed and linked resources that make up a cloud and is accessible from anywhere in the world. Cloud storage can provide the advantages of greater accessibility and reliability; rapid deployment; strong protection for data backup, archival, and disaster recovery purposes; and lower overall storage costs as a result of not having to purchase, manage, and maintain expensive hardware [32]. Cloud storage can be used for a variety of purposes, including backup, archival, and disaster recovery, but there is the possibility of security and compliance issues when using cloud storage services.

2. Literature Survey on Automation Frameworks and Secure Jobs Execution

The different phases of software development demand various different automation tools in the cloud environment. For example, to enable automatic job configure, schedule and monitor tools such as Puppet, Juju, Apache Continuum, Jenkins, and Cobbler enable automatic job are used in different phases [33]. To improve quality and address customer issues rapidly, we require a tool which is capable of continuous integration, test-driven development, and debugging.

Based on the project requirement, automation can be triggered in various methods some of them includes [34] the following:

(i) On-demand run: using scripts or user-interface user manually triggers the jobs

(ii) Scheduled run: tests are grouped into test suites and executed as per the schedule

(iii) On event occurrence: these test will run as soon as the build is available or a change set is identified (pushed) in the source repository

It is devised a scheme to measure Cloud Service Level Agreement (SLA) in real time environment and proposed a security management system for monitoring alerts, security of cloud incidents, and vulnerabilities [35].

The primary run time environment is Google Colab which is a part of the google app engine [36, 37].

Cloud computing represents the next step in the growth of the Internet. For coherence to be achieved throughout a network, it is necessary to share resources [38]. In recent years, it has developed as a new computing standard that has implications for a variety of academic domains, including software testing.

There are many different software approaches that may be used to test an application.

It not only alters the method in which computer resources are obtained but it also alters the manner in which computing services, technologies, and solutions are administered and delivered [39]. Meanwhile, it generates new concerns, challenges, and requirements in the field of software testing. Software testing in the cloud may lower the demand for hardware and software resources while also providing a more flexible and efficient alternative to the conventional software testing method, according to the cloud computing community. This paper presents an overview of the latest trends, opportunities, problems, concerns, and requirements in cloud testing and cloud-based application development and deployment [40].

3. Proposed Approach

The proposed methodology includes two major parts. First, for complete testing and validation of cloud software projects, we propose framework for automated jobs execution. The new code change tests are crucial as it allow any project functioning to regressing new source code changes. We

propose an end-to-end approach which scale and run the tests using the cloud resources and as per the configuration (serial or parallel), respectively.

The proposed approach optimizes the execution time by taking single CSV (comma separated file) with input test case and metadata information and efficiently group and executes the tests automatically.

The test configuration information is present in CSV (comma separated) file. Each entry in test definition (CSV) file has test details such as <UNIQUE_ID, TEST_NAME, EXECUTION_MODE, MACHINE_CONFIG ...>.

Later, we propose a security access control mechanism for the jobs execution platform leveraging the cloud environment. The role-based access control policies are integrated, and the security aspects of the tool are experimented.

Dynamical systems with multiscroll are more complex dynamics than chaotic systems with monoscroll attractors. The state-space equation for automatic chaotic system is given by

$$\dot{x}_1 = -ax_1 + bx_2x_3, \tag{1}$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3, \tag{2}$$

$$\dot{x}_3 = ex_3 - fx_1x_2. \tag{3}$$

The above Eqs. (1)–(3) can be adapted using hyperbolic function and modified in Eq. (6).

Equations (4) and (5) are similar to Eqs. (1) and (2).

$$\dot{x}_1 = -ax_1 + bx_2x_3, \tag{4}$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3, \tag{5}$$

$$\dot{x}_3 = ex_3 - fx_1x_2 + p_1 \tan h(x_2 + h). \tag{6}$$

Over the last several years, chaotic systems have been extensively studied in a variety of engineering applications. Using Julia's fractal process, chaotic attractors, and logistic map in a complex set, this work provides a novel chaotic system that may be used in many applications. A number of complex dynamic properties, including equilibrium points, bifurcation, Lyapunov exponents, and the chaotic behavior of the suggested chaotic system, were investigated. Previously, we learned that a single positive Lyapunov exponent demonstrated the chaotic condition. It is shown in the numerical simulation that there are several complicated dynamic behaviors that coexist with an antagonist form that is a mixture of bifurcation and attractor. Afterwards, we provide a chaotic system-inspired picture encryption technique that is both fast and secure. The algorithm is comprised of two major stages: confusion and diffusion, which are interconnected. The experimental findings have shown that the suggested maps employed are more sophisticated and have a key space with a suitable amount of key space to be useful. Comparing the proposed picture encryption algorithm to other current image encryption methods is done by utilizing several security analysis elements such as differential attacks analysis, statistical testing, key space analysis, information entropy test, and running time, among others. Based on the findings, it was determined that the suggested picture encryption approach achieves superior outcomes in terms of both security and speed.

Chaotic attractor is obtained when $a = 2$, $b = 6$, $c = 6$, $d = 3$, $e = 3$, $f = 1$, $p_1 = 1$, and $h = 2$, and the preferred initial conditions include $(x_1[0], x_2)([0], x_3[0]) = (0.1,0.1,0.6)$. Once the hyperbolic function is activated with the parameter, $h = -3$, and for the initial conditions generated, Figure 1 illustrates various conditions of hyperbolic function. The second phase is initiated with the parameters $p_1 = -1$ and $h = 3$ with the newly defined initial conditions as $[0.1,-0.1,-0.6]$. Figure 2 illustrates the function regarding the new initial condition values. In the third phase, the parameters $p_1 = 1$ and $h = 3$ and initial conditions are similar to the initially chosen values $[0.1,0.1,0.6]$. This is demonstrated in Figure 3 which shows a single scroll. From the models, it is evident that the scheme is multiscroll property.

Cryptography has been around for a long time. The exchange of a secret key, which was used both for encryption and decryption, required two parties to employ a secure channel in the early phases of the technology's development. This kind of encryption is referred to as private or symmetric key cryptography. Although such a technique was somewhat secure, there were flaws in its implementation. In addition, a secure route is not always accessible, which is why we want an encryption technique in the first place in the first place. The use of public key cryptography may help to mitigate these disadvantages. When two communicating parties agree on a shared secret key, they may exchange it without having to exchange their secret keys themselves via the communication channel. Instead, it is generated from a set of parameters, none of which are publicly available. When Whitfield Diffie and Martin Hellman presented an algorithm for key exchange in 1976, they were inspired by Ralph Merkle's work on public key distribution. The approach used exponentiation on a finite field, which was later refined by others. Diffie Hellman is a cryptographic algorithm that is utilized in a number of protocols and applications today. As opposed to a batch transfer from one sender to another, it is utilized in interactive transactions between two parties. The algorithm is utilized when data is encrypted on the web using SSL or TLS, as well as in virtual private networks (VPNs).

The newly derived models include

$$\begin{aligned}
\frac{d^q x_1}{dt^q} &= -ax_1 + bx_2x_3,\\
\frac{d^q x_2}{dt^q} &= -cx_2^3 + dx_1x_3,\\
\frac{d^q x_3}{dt^q} &= ex_3 - fx_1x_2 + p_1 \tan h(x_2 + g).
\end{aligned} \tag{7}$$

As a result, its safety is of the highest significance. Although it is more secure than other security algorithms, it is still subject to a variety of attacks, such as plaintext assaults and man in the middle attacks. Consequently, we suggest a version of the original technique that is more tolerant and secure due to the use of a random parameter in the

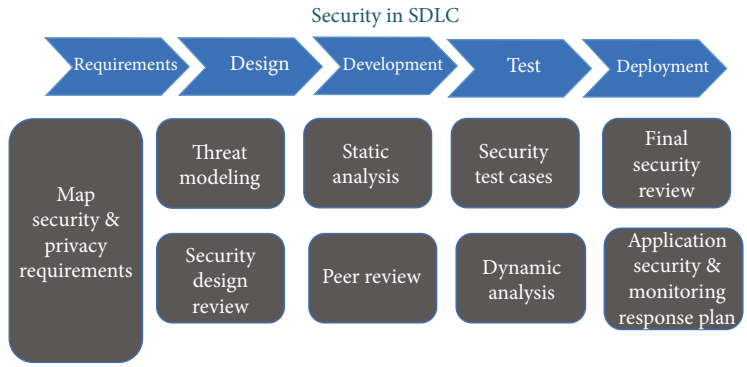

Figure 1: Secure software development life cycle.

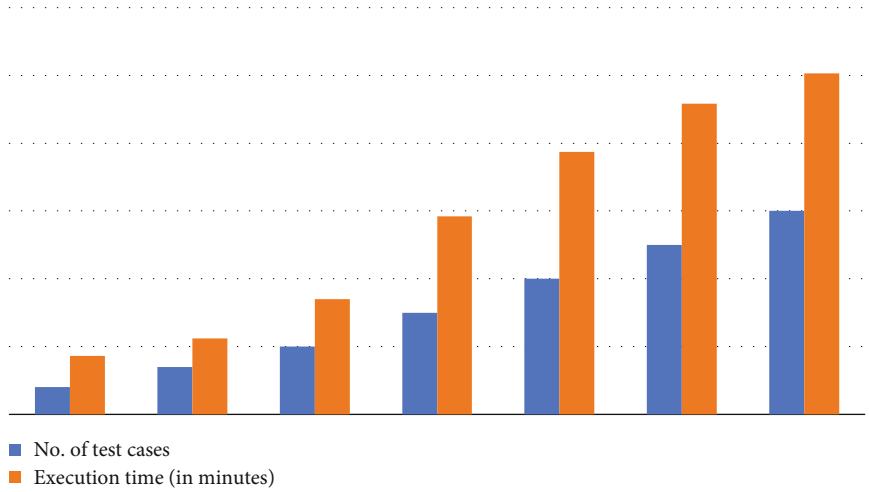

Figure 2: Tests execution using one virtual machine (x-axis: number of test cases vs. y-axis: execution time in minutes).

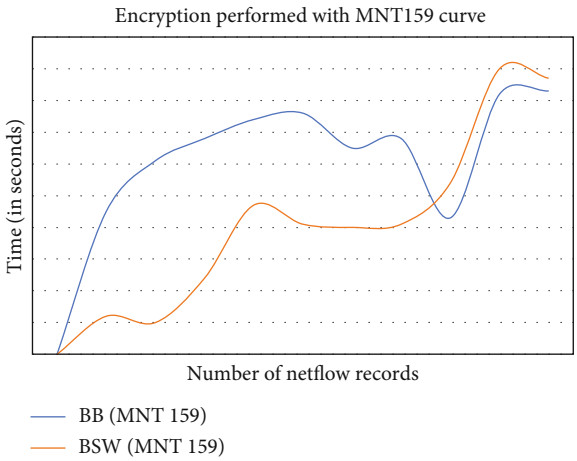

Figure 3: Encryption performed with MNT159 curve.

computation. Plaintext assaults are one of the most widely utilized cryptanalysis techniques today, accounting for around a third of all attacks. The attacker has access to sample plaintext and cypher text, as well as the plaintext itself. From a collection of known plaintext and cypher text, an attacker may extract further critical information, such as secret keys and code books, which can be used against them. The random parameter added in the proposed technique significantly reduces the potential of a known plaintext attack of this kind.

4. Design and Implementation of Fully Automated Test Framework for Cloud

Unlike the on-premise deployments, additional controls are required for development and deployment of software for cloud environment.

Some important changes in the cloud environment included the following: compatibility issues since cloud providers support different ways of managing user data, reduced control over physical cloud data security, compliance to appropriate regulations applicable to data domain, and data security during entire tenure of data (newly created persisted, processed, transit and destroyed).

Cloud software developers should follow Secure Coding Guidelines (OWASP Security Guide) as shown in Figure 1. Security aspects need to be considered in every phase right from requirements to deployment. In the production environment, the execution logs, debug statements, and error messages have very valuable information about the code.

Table 1: Test case results using Single client machine.

No. of test cases	Execution time (in minutes)
40	86
70	112
100	170
150	292
200	387
250	458
300	503

Table 2: Test case results using master-slave architecture.

	No. of VMs		
No. of test cases	10 Execution time (in minutes)	20 Execution time (in minutes)	30 Execution time (in minutes)
40	7	5	3
70	16	11	7
100	22	16	9
150	37	19	10
200	42	22	12
250	47	25	15
300	56	27	18

Static analysis checks code statically, and the dynamic code analysis tools analyze as it executes and checks for possible security vulnerabilities. The dynamic code analysis tool analyzes the runtime code execution paths.

Upon execution, the input is specified in a CSV file with test case information. Later, the result aggregator tool groups the result which generates failure analysis.

User-interface test automation tool, Selenium, is used to run the tests on infrastructure machines depending on configuration with test inputs file in TestNG format. Connected in master-slave architecture, it runs tests in parallel or serial mode on a single host or multiple host.

This user-interface disseminates tests to slave machines of different OS, platform version, and browser versions; then, the results are aggregated in xml format in serial fashion.

4.1. Experimental Results. To experiment and validate the results of automation framework, the user-interface tests are chosen. Generally, the tests are often categorized into back-end tests, database tests, application programming interface tests, and user-interface tests.

The user-interface tests demand different browsers and operating systems and considered to be the most complex due to permutations and combinations of browsers, operating system support, requirement for pre- and postconfiguration of virtual machines, and runtime environment.

Execution of this tests demands careful selection of target machine configuration, and execution takes longer time compared to other tests. The execution time growth was almost linear with number of test cases. The performance measure of a single client machine running all the test case is shown in Figure 2.

When 70 tests cases are executed in a single machine, it took 112 minutes and when the test cases was increased to 200 and 300, it took 458 minutes and 503 minutes, respectively, as shown in Table 1. The speed of execution can increase by adding more number of tests machines as the cloud environment supports easy scalability.

Figure 2 shows the results of Selenium grid-hub environment in master-slave architecture with multiple registered client machines.

One of the host has selenium grid-hub software installed which acts like master and other hosts have slave configuration which register with master for jobs execution.

We could observe from the graph that the time consumed decreased with increasing the number of virtual machines.

For example, the execution time for 200 test cases costs 458 minutes and when the slave machines or test machines are increased to 20 as shown in Table 2, it took 22 minutes to run the same number of test cases; further, the time reduced to 12 minutes when the slave machines are increased to 30 numbers.

4.2. Discussion. We observed that the proposed system provided with sufficient test virtual machines could run any number of test cases. Further we found (after 800 test cases) that framework designed was stable and able to distribute the test across heterogeneous work environment. Running test automation jobs on a cloud ease scaling based on project requirement.

Recent automation tools like Puppet, Chef help in automation of virtual machine deployment and configuration and can be integrated into the process to improve the efficiency further.

5. To Improve Security in Jobs Execution Platform

We need to ensure security and data confidentiality in automation jobs execution platform (JEP). CSP has large pool of resources (machines) which the user can use to run on JEPs. The type of jobs or test cases depends on the CSP and users.

5.1. Technical Architecture of the System. The job configuration file consists of two parts: job parameters and job configurations.

The job parameters consist of job-name, run-schedule, start-at, and recurring-job which have permissions READ-EXECUTE for normal users and administrator has READ-WRITE-EXECUTE permission. The job configuration includes programming commands, and it processes on data. It can be of any type such as a software program for data analytics operations or script of security forensic tool. The job information comprises of Db_column_list, and Db_result_column is also part of job configuration file.

The JEP computes the data as per the job configuration, and the results are stored back in the database repository.

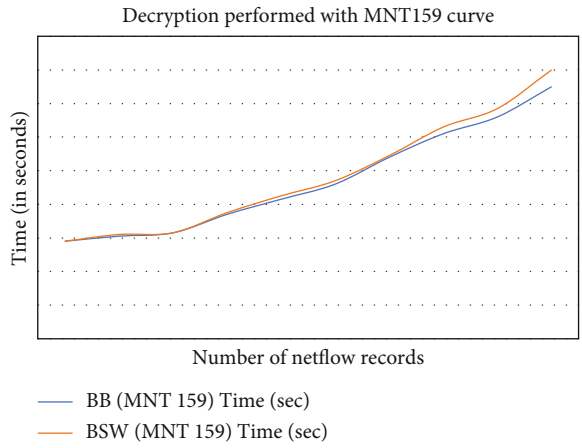

Figure 4: Decryption performed with MNT159 curve.

Using the ID-PKC encryption algorithm, the job configuration file is encrypted using identity information, security identifiers, and access structure as inputs.

The jobs execution platform retrieves the job file from the database and checks for user signature. If the user signature is verified using a public key component, the secret key is validated. If the verification is successful, then the corresponding job file is obtained. From the obtained job file, the corresponding JEP finds the operations to be carried out and fetch the relevant data from the underlying database, and the computation is done accordingly.

It has become common for cloud computing to incorporate platforms for developing and executing bespoke applications, a notion referred to as "platform as a service" (or PaaS). This strategy might be seen of as the next step beyond the SaaS model, where on-demand distribution includes not just the particular piece of software that is needed but also the customers' operating system and browser. When it comes to running apps over the Internet, PaaS offers the whole infrastructure required. When it comes to delivery, it is similar to that of a utility like electricity or water.

Users just "tap in" and take what they need; all of the complexity are concealed behind the scenes of the application. As with any utility model, PaaS is based on metering or subscriptions; so, customers only pay for what they use. The delivery channel in this model is the "Cloud," as is the case with any other utility model.

5.2. Example Policy Settings

5.2.1. Policy String Protecting Job Metadata.

$$\{\text{role} = \text{Administrator OR } (\text{role} = \text{Engineer AND mode} = \text{READ})\}. \quad (8)$$

5.2.2. Policy String Protecting the Job Script Contents.

$$\{\text{role} = \text{Administrator OR } (\text{role} = \text{JEP\_Admin and mode} = (\text{READ or EXECUTE}))\}. \quad (9)$$

There are new automated test methods for cloud interoperability. Because both cloud and SaaS apps provide connection protocols and APIs, test engineers should ensure the interoperability quality of cloud applications.

The data required for job execution is fetched from underlying data repository and processed.

The results from the processed job operations are encrypted and delivered in the user site. The results arrived at the user site is then decrypted using specific secret key, public parameters, and policy string by the decryption algorithm. In this methodology, we concentrated only the time spends on cryptographic techniques for various job executions. This paper does not considered the time spends on data computation before encryption and decryption techniques. Here, the proposed security framework, ID-PKC algorithms, namely, Boneh-Boyen [7] and Bethencourt, Waters, and Sahai [9] model, is evaluated for implementing access control. We used network telemetry dataset of size 2,000 to 20,000 records, and bilinear pairings are generated using MNT159 asymmetric curves. Data encryption [13] includes ciphering the job configuration file and the actual network telemetry as shown in Figure 3.

Data encryption task using BB scheme has consumed more time when compared to the BSW scheme, and this is due to the fact that earlier scheme requires one pairing operation in addition [36].

For example, to execute 11000 NetFlow records, BB scheme took 0.72 seconds, whereas the BSW took only 0.4 second.

Decryption task involves CEK key decryption and later, a symmetric key algorithm for actual content decryption, and took same time for both the schemes as shown in Figure 4.

Cloud engineers will be unable to construct a cost-effective cloud test environment with the existing cloud technology since there are no supporting solutions available for it. The results of a study conducted by Gao and colleagues revealed that many of the published articles have explored performance testing and solutions.

In terms of scalability and performance testing, they are only concerned with metrics and methods for evaluating scalability in parallel and distributed systems. In the present state of metrics development, frameworks, and solutions, aspects such as dynamic scalability are not supported.

Regression testing is complicated by software problems and bug fixes, which creates issues and obstacles for regression testing. The cloud testing services that are available on demand should be able to solve a wide range of difficulties and concerns.

Providing suitable test models and criteria for cloud testing, test engineers should be supplied with adequate test models and criteria that are effective in cloud computing.

Continuous validation and regression testing solution are as follows: if software has been modified as a result of bug fixes or feature updates, test engineers must offer automated retesting methodologies that handle the multitenancy aspect of cloud computing environments.

Test engineers should ensure the interoperability quality of cloud applications since both cloud and SaaS apps provide connection protocols and APIs. There are new automated test solutions for cloud interoperability.

6. Conclusion

Fast software product development demands flexible infrastructure. The elasticity provided by cloud environment can be leveraged to build such products. The existing cloud environment should be equipped with automation of build and test environments to develop swift products. Security is paramount when it comes to cloud and data computations. This methodology is targeted in proposing a scheme for the secure cloud environment.

This method discussed the need of data encryption while accessing public cloud services such as auditing, computation, and security forensics. This work also highlighted importance of secure SDLC for scalable test automation framework build on top of the cloud environment.

Functional testing makes extensive use of hardware and software to replicate human activities, and it is becoming more sophisticated. When compared to functional testing, nonfunctional testing allows for the measurement and association of the testing of nonfunctional characteristics of software systems. Few benefits and testing issues associated with cloud computing have been recognized so far, according to experts. Testing is a recurring operation, and for each project, new requirements must be defined and documented.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

All authors declared that they do not have any conflict of interest.

References

[1] K. Beck, M. Beedle, A. Van Bennekum et al., *Manifesto for Agile Software Development*, Agile Alliance, 2011.

[2] P. Samarati, "Data Security and Privacy in the Cloud," in *Information security practice and experience*, X. Huang and J. Zhou, Eds., Springer, Cham, 2014.

[3] P. Donadio, G. B. Fioccola, R. Canonico, and G. Ventre, "Network security for hybrid cloud," in *2014 Euro Med Telco Conference (EMTC)*, pp. 1–6, Naples, Italy, 2014.

[4] N. K. Rathore, N. K. Jain, P. K. Shukla, U. S. Rawat, and R. Dubey, "Image forgery detection using singular value decomposition with some attacks," *National Academy Science Letters*, vol. 44, no. 4, pp. 331–338, 2021.

[5] N. Garigipati and R. V. Krishna, "A study on data security and query privacy in cloud," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 337–341, Tirunelveli, India, 2019.

[6] P. K. Shukla and M. Dixit, "Cloud-based image fusion using guided filtering," in *Handbook of Research on Emerging Perspectives in Intelligent Pattern Recognition, Analysis, and Image Processing*, N. K. Kamila, Ed., pp. 146–165, IGI Global, Hershey, PA, 2016.

[7] P. K. Shukla, V. Roy, P. K. Shukla et al., "An advanced EEG motion artifacts eradication algorithm," *The Computer Journal*, 2021, bxab170.

[8] R. Buyya, C. Vecchiola, and S. T. Selvi, *Mastering Cloud Computing: Foundations and Applications Programming*, Newnes, 2013.

[9] C. Yang, B. Song, Y. Ding, O. Jiangtao, and C. Fan, "Efficient data integrity auditing supporting provable data update for secure cloud storage," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 5721917, 12 pages, 2022.

[10] G. G. Rajput and R. Chavan, "improved LSB based image steganography using run length encoding and random insertion technique for colour images," *World Scientific News*, vol. 112, pp. 180–192, 2018.

[11] D. Parwani, A. Dutta, P. K. Shukla, and M. Tahiliyani, "Various techniques of DDoS attacks detection and prevention at cloud: a survey," *Oriental Journal of Computer Science and Technology*, vol. 8, no. 2, pp. 110–120, 2015.

[12] A. Sarkar and S. Karforma, "A new pixel selection technique of LSB based steganography for data hiding," *International Research Journal of Computer Science (IRJCS)*, vol. 5, no. 3, pp. 120–125, 2018.

[13] H. Deng, Z. Qin, Q. Wu et al., "Achieving fine-grained data sharing for hierarchical organizations in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, p. 1, 2022.

[14] J. Shen, H. Yang, P. Vijayakumar, and N. Kumar, "A privacy-preserving and untraceable group data sharing scheme in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 114, 2021.

[15] G. Khambra and P. Shukla, "Novel machine learning applications on fly ash based concrete: An overview," *Materials Today: Proceedings*, pp. 2214–7853, 2021.

[16] K. Bahwaireth, L.'a. Tawalbeh, E. Benkhelifa, Y. Jararweh, and M. A. Tawalbeh, "Experimental comparison of simulation tools for efficient cloud and mobile cloud computing applications," *Journal on Information Security*, vol. 2016, no. 1, p. 15, 2016.

[17] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic review of security vulnerabilities in Ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.

[18] G. Xu, M. Lai, J. Li, L. Sun, and X. Shi, "A generic integrity verification algorithm of version files for cloud deduplication data storage," *EURASIP Journal on Information Security*, vol. 12, no. 1, 2018.

[19] S. Mehdi and F. Richard Yu, "Attribute-based data access control in mobile cloud computing: taxonomy and open issues," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991–3005, 2016.

[20] C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: challenges and opportunities," *Vehicular Communications*, vol. 10, pp. 13–28, 2017.

[21] A. Motwani, P. K. Shukla, and M. Pawar, "Novel framework based on deep learning and cloud analytics for smart patient monitoring and recommendation (SPMR)," *Journal of Ambient Intelligence and Humanized Computing*, 2021.

[22] J. Zhou, Z. Cao, X. Dong, and X. Lin, "TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems," in *34th IEEE Annual Conference on Computer Communications and Networks, IEEE INFOCOM 2015*, pp. 2398–2406, Hong Kong, China, 2015.

[23] V. Bhandari, S. Tamrakar, P. Shukla, and A. Bhandari, "A new model of M-secure image via quantization," in *Data, Engineering and Applications*, R. K. Shukla, J. Agrawal, S. Sharma, and G. Singh Tomer, Eds., Springer, Singapore, 2019.

[24] "Open Web Application Security Project (OWASP)," http://www.owasp.org/.

[25] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," in *Advances in Cryptology - EUROCRYPT 2004. EUROCRYPT 2004*, C. Cachin and J. L. Camenisch, Eds., vol. 3027, Springer, Berlin, Heidelberg, 2004.

[26] H. Qiao, J. Ren, Z. Wang, H. Ba, and H. Zhou, "Compulsory traceable ciphertext-policy attribute-based encryption against privilege abuse in fog computing," *Future Generation Computer Systems*, vol. 88, pp. 107–116, 2018.

[27] M. Kaur, D. Singh, V. Kumar, B. B. Gupta, and A. A. Abd El-Latif, "Secure and energy efficient-based E-health care framework for green internet of things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1223–1231, 2021.

[28] H. Bhardwaj, P. Tomar, A. Sakalle, T. Singh, D. Acharya, and A. Bhardwaj, "Future aspects and research perspectives of the internet of things," in *Integration and Implementation of the Internet of Things through Cloud Computing*, P. Tomar, Ed., pp. 1–18, IGI Global, Hershey, PA, 2021.

[29] L. Gupta, R. Jain, A. Erbad, and D. Bhamare, "The P-ART framework for placement of virtual network services in a multi-cloud environment," *Computer Communications*, vol. 139, no. 1, pp. 103–122, 2019.

[30] N. Jain, S. Rathore, and P. K. Shukla, "Designing efficient optimum reduced order IIR filter for smoothening EEG motion artifacts signals," *Design Engineering*, pp. 5080–5101, 2021.

[31] S. Stalin, P. Maheshwary, P. K. Shukla, A. Tiwari, and A. Khare, "Fast chaotic encryption using circuits for mobile and cloud computing: investigations under the umbrella of cryptography," in *Soft-Computing-Based Nonlinear Control Systems Design*, U. P. Singh, A. Tiwari, and R. K. Singh, Eds., pp. 252–277, IGI Global, Hershey, PA, 2018.

[32] M. Wazid, A. K. Das, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: survey and outlook," *Journal of Systems Architecture Volume*, vol. 97, pp. 185–196, 2019.

[33] A. Akella, "Experimenting with next-generation cloud architectures using CloudLab," *IEEE Internet Computing*, vol. 19, no. 5, pp. 77–81, 2015.

[34] Y. Vijay, S. Goyal, R. Sharma, and U. Mamodiya, "Green building design and security system," *Journal of Web Engineering & Technology*, vol. 6, no. 2, pp. 10–14, 2018.

[35] R. K. Gupta, K. K. Almuzaini, R. K. Pateriya, K. Shah, P. K. Shukla, and R. Akwafo, "An improved secure key generation using enhanced identity-based encryption for cloud computing in large-scale 5G," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 7291250, 14 pages, 2022.

[36] N. Newalkar, S. Silakari, and P. K. Shukla, "Comparative analysis of co-operative MAC schemes," in *2012 International Symposium on Cloud and Services Computing*, pp. 42–48, Mangalore, India, 2012.

[37] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, CA, USA, 2007.

[38] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.

[39] P. Patidar and A. Bhardwaj, "Network security through SSL in cloud computing environment," *International Journal of Computer Science and Information Technologies*, vol. 2, no. 6, 2011.

[40] F. Xingbing and Z. Wu, "Ciphertext policy attribute based encryption with immediate attribute revocation for fine-grained access control in cloud storage," in *2013 International Conference on Communications, Circuits and Systems (ICCCAS)*, pp. 103–108, Chengdu, China, 2013.