Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 43 Issue: 06-2024
DOI: 10.5281/zenodo.12529410

ENHANCE CLOUD SECURITY USING IMPROVED RSA WITH XACML TECHNIQUES

ALI ZAHEER AGHA *
Research Scholar, Invertis University, Bareilly, Uttar Pradesh, India.

RAJESH KUMAR SHUKLA
Faculty of Engineering and Technology, Invertis University, Bareilly, Uttar Pradesh, India.

RATNESH MISHRA
Computer Science & Engineering, BIT Mesra, Patna Campus, Patna, Bihar, India.

RAVI SHANKAR SHUKLA
Computer Science, College of Computing & Informatics, Saudi Electronic University, Saudi Arabia.

RATNESH KUMAR SHUKLA
Computer Science & Engineering, Shambhunath Institute of Engineering & Technology, Prayagraj, India.

Abstract

Nowadays, you may find a lot of things online at any time, from any location. Since protection over accessibility, anonymity, and authenticity are essential, this method combined encryption combined with access management. In order to improve total resource admittance security, a much stronger encryption method was included in the suggested architecture. This suggested work encrypts data and maintains credentials using Improved RSA-based role-based access control (RBAC) with extended access connectivity markup language (XACML). By this method, data may be stored on the web computer by utilizing cryptographic concepts and data accessed through a simple admission control system. The encryption technique that combined the traditional homogeneous encryption process with the unstable information distribution approach is used to guarantee the total protection of sensitive data. With the help of this hybrid method, users may benefit from recovered information in a secure way. The suggested work executes far more quickly collectively than other encryption techniques already in use.

Keywords: Admission Control Security, Cloud Computing, Cryptography, Network Security, Privacy, RSA, XACML.

1. INTRODUCTION

Using internet, clients may conveniently access data from anywhere thanks to web technology. Users can obtain data via the web; however administrators must set up infrastructure and other technological requirements. Distributed computing, facilitated by the web, connects anyone anywhere in the globe to a vast array of resources, including applications, computers, and communications. Supplier provides customers with benefits through the same memory, networks, control processing, and other processing power by using cloud computing services. Practically every client utilized a program that runs on an operating system for a computer [1].The content binding encryption procedure is carried out directly on the server using the private key that is stored in the cloud signature mechanism. The challenges of powerful client authentication while gaining access to the private key and safely preserving the private key on the server must be resolved for the secure usage of cloud signatures. One of these solutions is CryptoPro TSS, which employs an HSM to hold the private key and supports Rutoken Web (Strong Two-Factor Authentication) as a component of its authentication choices.

A personal computer provides a virtual droplet framework for exclusive use by the company. Organization is in charge of managing the technology. The entire town may access computer resources thanks to the worldwide internet [2]. An internet provider acting on behalf of a second party is in charge of its upkeep and oversight. A collaborative network is the second cloud distribution paradigm, where several organizations must cooperate on shared resources in order to achieve concurrent goals such as protection. With the use of proprietary technologies and standards, this hybrid cloud business model combines three or more internet infrastructures to enable information mobility.

There are typically three system approaches into which droplet solution may be classified: fog computing, corporate web, and personal computing. Corporate internet is dispersed among users in an operating environment from public computers, particularly inside any large corporate industry [3]. One company is in charge of maintaining and overseeing a commercial network. A unique method in the hybrid design allows it to interface with various environments, including corporate, public, and commercial databases. This hybrid communal architecture makes it feasible for community information to be shared and is utilized by several enterprises in any one location. This infrastructure is funded by the public or private sectors. The current method of access to the internet ensures that unauthorized users can join the network as well. This method prevented unauthorized changes from being made to the network by those with personal access. WiFi was established, but not without challenges, including privacy concerns. These enhancements also offer support for cryptographic techniques. Full-featured browsers that supported encryption started to be available on the marketplace a while ago. Because it enables you to construct safe static WEB clients for machines with stringent security needs, such an approach offers a significant deal of untapped potential [4].

Role-based access control (RBAC), discretionary access control (DAC), and mandatory access control (MAC) are the three distinct kinds of access control strategies. The primary basis for access control in discretionary access control is the customer's identity. Accessibility to information or resources in MAC is granted to clients based on their level of authorization and the data classification label assigned to each resource. The client is assigned a security clearance, and in order to get access, that clearance level must match or exceed the sensitivity designation. The data holder has to determine how sensitive the material is before assigning it a classification label. RBAC required grouping clients into clusters according to the roles that granted them the authority to carry out specific tasks [5].

This paper's primary goal is to offer efficient data preservation with improved security while taking all of the above problems into consideration. A brand-new hybrid cryptography-based encryption technique is put forth that speeds up the secure recovery of stored information by combining RBAC with an expanded language for connection management modeling. The format of the article is as follows: The literature review is covered in Section 2, and the materials and procedures are explained in Section 3.

Section 5 discusses the experimental analysis, whereas Section 4 outlines the suggested methods. Section 6 concludes with a final presentation.

2. LITERATURE REVIEW

Portability is a benefit of the Internet browser. As a result of the accessibility of secure tokens with flash memory, secure options were created whereby the browser is secured in its flash memory and the most critical activities involving the private key are performed on the token's "board". Such a system offers excellent security together with great user-friendliness. The integrity of the database is preserved by a number of methods. Three primary processes—cryptography, backup, and erasing—are used to classify different techniques. Since cryptography lacks actual power over individual data, it greatly conserved data under unstable conditions [6]. The data necessitated novel approaches centered on encryption and access controls that maintain integrity and security. Data is encrypted utilizing a cryptography model in an encryption approach. Elements of cryptography, including security, consistency, client identification, and source identity verification, are related to mathematics [7]. The three primary types of encryption techniques are symmetrical, asymmetrical, and conventional. The information was encrypted in the client using a key, which was subsequently decrypted by the recipient. Two keys are used in asymmetric encryption: a public key and a private key. Commonly available assets called public keys can be used to secure data. After this, a private key which has to be maintained hidden is used for decoding it. Access control and encryption are guaranteed by a complex encryption standard that is integrated into a Single-Sign-On platform using user index accessibility protocols.

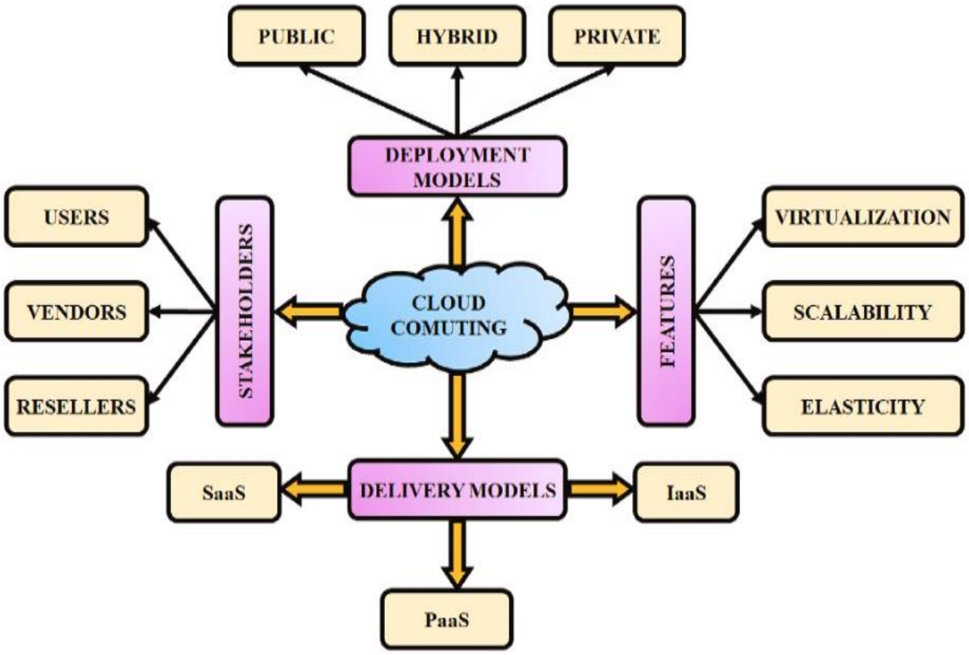


Figure 1: Flow Chart of the Features in Cloud Computing

In cloud computing, confidentiality, credibility, and data protection are major concerns. To safeguard distributed communication, cyber security is employed. The cryptography method that would be used will never be specified by the protocol [8]. The figures 1 are extended with multilayer buffers to increase the overall effectiveness of any privilege control technique.

The process of issuing certifications results in ineffectiveness [9]. Because each collaboration requires a new certification, it throws the organization's processes and many clients into disarray. It is suggested to use distributed RBAC architecture [10] to lessen the authorization demands among individual networks inside a subnet. Every transformer is assigned many localized duties in addition to a single localized function. Inside the Hadoop terminal, an instance with additional site privileges is formed for every power with a different client. The privilege idea used by smart infrastructure networks depends on where a certain obligation falls within a geographical section. As a result, the location entry management model is enhanced to safeguard resources [11].

3. PROPOSED APPROACH

3.1 Preliminaries

Data gathered from pcs and persons is kept on cloud servers. Cloud computing has four key components: privacy, availability, productivity, and sustainability. Access to information is limited to those who have been given authorization by privacy. Online technologies in the modern day require authentication mechanisms to provide safety and prevent client information from being compromised. Integrity is a crucial component of online data, because modifications may only be made by authorized users. In order to preserve content integrity, data stored in cloud systems is concurrently controlled and restricted [12].

The maintenance of online infrastructure is often handled by a different outside business. Verification from users is necessary to preserve information security. If accessibility demands aren't met, clients are unable to find this data in one place; instead, they must obtain it anytime something is being rectified. The client tries to obtain the necessary data. As network operators manage several machines, stability is a problem in online environments.

A company used cyber facilities after taking database backups. In cloud computing, public access monitoring is a fundamental assertion [13]. The cost and capability of cloud services varies, but they all promise high availability, scalability, and flexibility. Businesses are spared from having to spend in the creation of their own approaches, notably the acquisition of pricey cryptographic equipment, even though the services are paid for.

You can increase the range of cryptographic algorithms that the platform supports with the help of the Java cryptography framework. Owing to Java's widespread use, a large number of cryptographic tool developers supply certified JCP providers [14].

3.2 Proposed Techniques

The most popular approach for safeguarding online privacy of data is perhaps cryptography. The suggested method for cloud computing uses an automated access management system and an effective encryption technology to protect and preserve the privacy of sensitive data. When it comes to internet technology, cryptographic techniques ensure that secured data is never compromised since only authorized individuals can access credentials [15]. Theoretically, these can be any size of business that creates or implements applications specifically for the purpose of integrating digital signatures, or that utilizes apps that are previously incorporated.

In circumstances of a compromise of privacy, data security and protection are ensured through the application of cryptographic procedures. According to the security needs and possible hazards, a variety of cryptographic approaches, such as public key cryptography and symmetric key cryptography, may be employed throughout data transfer and storage.

Suppliers of apps or data management systems that wish to incorporate digital stamps or signatures. A different possibility is to offer them to clients as a posh solution which guards against document forgeries. The layout is sufficiently adaptable to accommodate the inclusion of digital signatures as a further layer or extra functionality.

3.3 RBAC with XACML

Web technology uses an admission-based security mechanism to prevent unwanted individuals from connecting to the network. To gain trust, the user is not allowed to perform any unneeded adjustments. When allowing access to users, role-based access control gives login information to occupations and tasks privileges.

RBAC simply verifies the user's identity. RBAC is unable to determine a user's reliability so as to limit login and stop unauthorized access to the network. RBAC and XACML (Extensible Access Control Markup) work together. With XACML, attribute-based access control is the primary technique used.

There were five different policy decision, administration, and information, enforcement, and retrieval points in the XACML authorization model. One aspect of an operating environment's policy enforcement point is access control, which controls the process of authorizing requests and approving or rejecting permission to utilize sources.

Central Policy Decision Point developed the evaluation based on whether or not access has been established. Policies stored at the Policy Retrieval Point are accessible to the Policy Decision Point. The Policy Administration Point is in charge of managing policies. Figure 2 shows the suggested role-based access control using XACML.

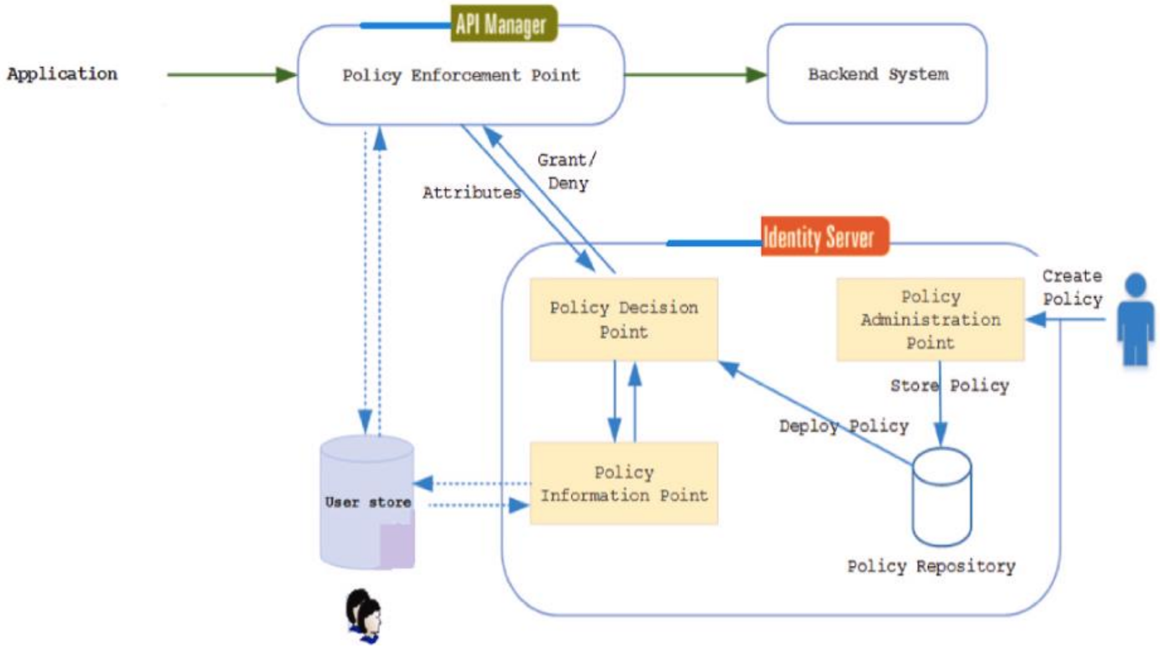


Figure 2: Working Flow Chart of the RBAC with XACML

Digitally signed papers, or seals, were incorporated into business processes by companies, and they were utilized by system integrators in both new and old systems for managing documents. Each company has to choose the DSS solution that best meets the requirements for that project. It considers the scale of the business, the demands of regulatory agencies, and other elements that are frequently particular to each situation.

3.4 Rivest–Shamir–Adleman (RSA)

The Rivest-Shamir-Adleman technique protects data while granting anonymity. A public key stream is encrypted using a pair of input keys in the Rivest-Shamir-Adleman technique [16]. Data that is encrypted is able to be decoded by the owner of the key using a secret key. This approach affects efficiency [17]. The original RSA technique's weakness was fixed by the improved RSA technique. Two source keys were needed: a private key that the file bearer used to encrypt and decode information, and a public key which anybody could employ to access files that were encrypted.

Symmetric encryption encodes every piece of information in cloud computing. It involves key generation and public key cryptography. Symmetric solutions require a "secret code" to safeguard the information that is used by information bearers; however, asymmetrical systems require "two credentials" in order to decode the symmetrical "secret code" that is generated by the asymmetrical "two credentials." The cloud server receives a key pair, resulting in two asymmetric identities. During the first phase, the information owner's secret Cpub and private password Upub were stored on the cloud. The key pair is obtained from a cloud server by the information owner and used to encrypt the symmetric cryptographic key in the second stage [18].

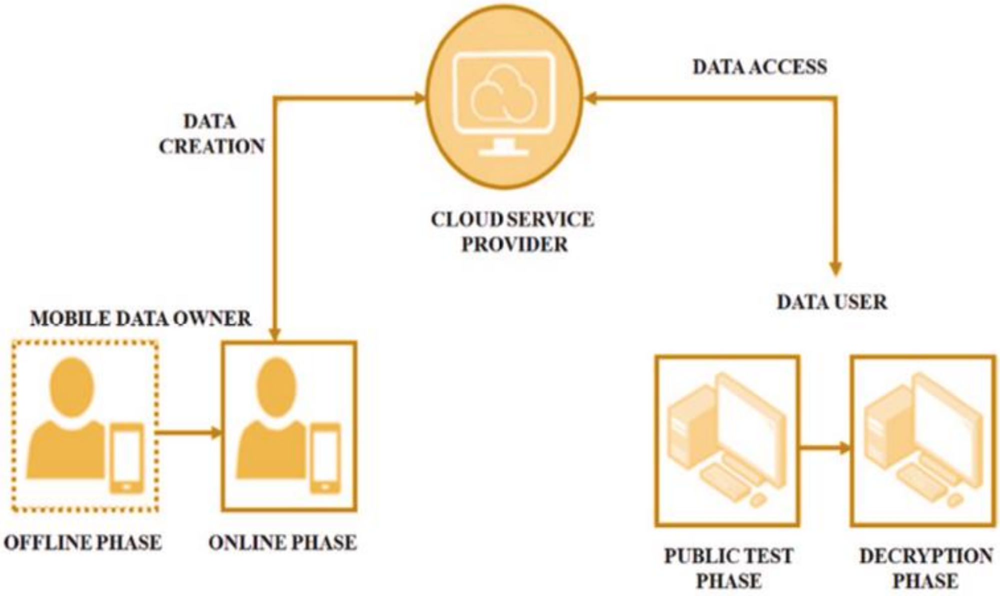


Figure 3: Flow Chart of Phases of the Data Access

Finally, look up KE online. Figure 3 illustrates the Phase of key creation workflow. The next step in the key creation procedure required the encrypted data to be posted on the public internet. The original owner used symmetrical keys to encrypt the material prior transferring it to the public cloud in an unprotected state.

The data acquisition stage of the proposed study is shown in Figure 3. It found the data that was encrypted and delivered it to the customer along alongside the encoded password. The cloud repository first used its secret keys, Cpriv, to decrypt this symmetrical secret content. Then, it used the client's public secret, Upub, to re-encrypt it. The user uses an asymmetrical passcode to decode the data after encrypting the symmetrical secret using secret Uprivate.

3.4.1. The Effectiveness of Enhanced RSA for Cloud Data Security

There are other ways to ensure the privacy of information, but cryptography has shown to be the most effective. Given that several clients have access to the data in an interconnected environment, this solution is worthless and each client has to be given the secret keys. Administering keys to several customers at once carries a risk, which makes access control extremely difficult to set up.

Figure 4 are shows the availability of data in significantly impacted by the use of asymmetric encryption. These methods of cryptography are among the most practical and effective ways to protect information.

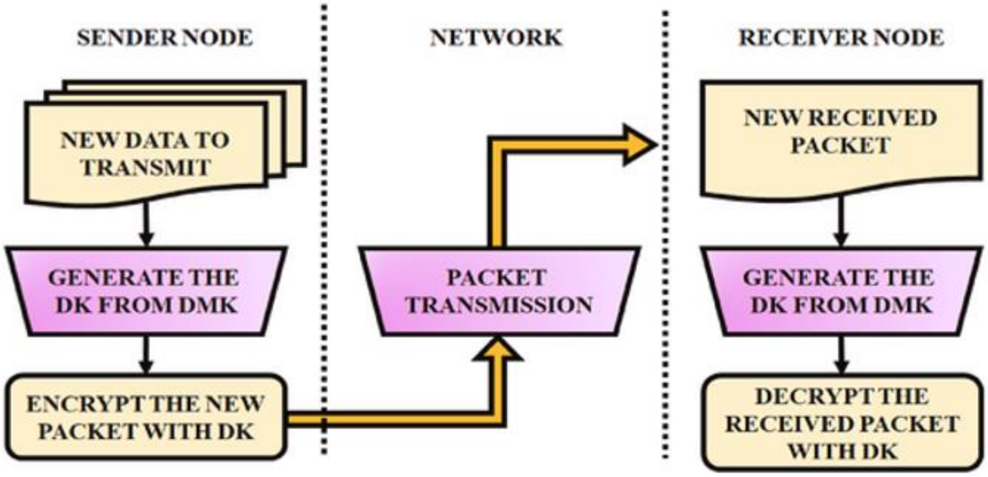


Figure 4: Flow Chart of the Key Generation between Senders and Receivers

It prevents users from encrypting a large volume of data over an extended length of time. It takes technique to recommend striking a balance between system efficacy and safety while preserving data in cloud inter-elements. Figure 5 are adopting higher security, faster data encryption, and suitable and safe information retrieval are all benefits of this RSA technique. a process for allocating uniform keys to cloud servers or authorized users. The data's confidentiality and privacy were preserved by the original procedure.

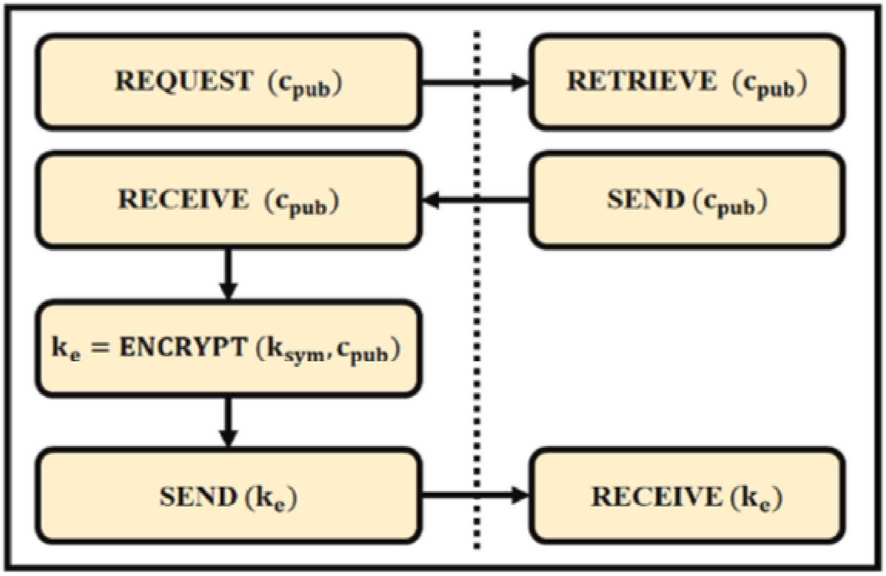


Figure 5: Flow Chart of the Data Storage

3.5 eXtensible Access Control Markup Language

OASIS has standardized XACML, an XML-based language enabling access control. Basic access control needs are expressed in terms of restrictions on elements in the XACML policy language. An attribute can be any property of any Security Related Object

(SRO) that the access request is made for. The version 2 elements (subject, resource, action, and environment) are no longer the only ones available in XACML showing in figure 6. Data types and methods that are predefined are used to alter attributes. Aspects provide the language a great deal of flexibility. In addition, new methods, characteristics, or data types may be added to the XACML language since it is naturally extensible. By orienting the security policy rules using the circumstances features, we make use of XACML. Classification and Aggregation are this version's two most significant enhancements. The primary concept of aggregation is the expression of sets of conditions and rules through abstraction, or being near specifications.

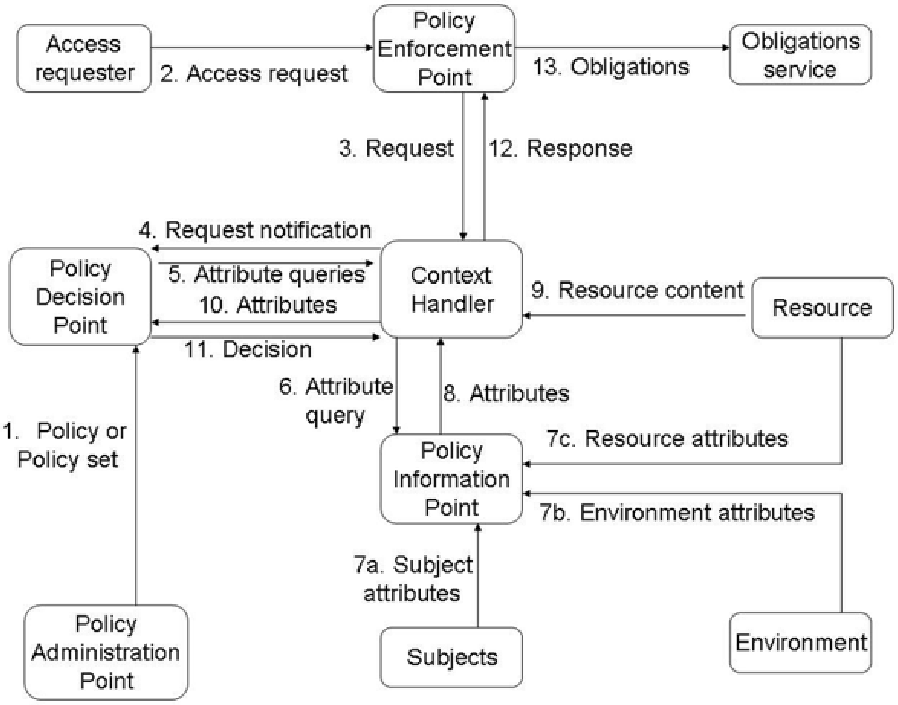


Figure 6: Flow Chart of the Working of XACML.

With the new target section fashion, aggregation is feasible and no longer dependent on the four tuples (Subject, Resource, Action, and Environment). The XACML category feature allows the policy to be targeted to additional attribute categories, such circumstances. In order to connect the scenario attribute to each XACML policy, we define the category that is filled in the target section. Consequently, the Policy Decision Point (PDP) will be directed toward the appropriate set of criteria for evaluation based on the value of scenarios. Consequently, scenarios were used to aggregate rules. Furthermore, the organizational structure provided by XACML (Figure 6) describes each entity and how they relate to the process of making decisions.

In this model step 1 are defined rules drafted by Policy Administration Points (PAP) and sent to the PDP. In the second step, the requester for access submits it to the Policy Enforcement Point (PEP) that forwards it to the context handler. The context-related handler creates a standard XACML demand contexts in phase four and sends it to the

PDP. The PDP can ask the context handler for any additional topic, resource, action, and environment attributes (step 5). The context's handler contacts a Policy Information Point (PIP) in step 6 with an attribute demand. Steps 8 and 7 are retrieving the required attributes, the PIP returns these to the context handler. The context handler sends the required attributes. After assessing the policy, the PDP provides the context handler (steps 9, 10) with a typical XACML response context along with an authorization decision. In step 11, the context handler finally provides the PEP with a response that upholds the PDP's ruling.

3.6 Role-based Access Control Using XACML and RSA

The individual who was in charge of the material employed RSA encryption in the recommended technique to guarantee data security and enable full accessibility. RBAC made use of XACML to give the proper authorization for content access. The content owner protects the data using an improved RSA technique each time a customer seeks access. This method employed two keys: a public key that let external parties to carry out transactions following encryption and a secret key that was used to encrypt or decode the data. A reliable component that links tasks and permissions and ensures that those relationships are constant is essential for cloud computing.

The suggested approach was role-based access utilizing XACML on accounts with authorization constraints. When a user requests access to material, the policy decision point typically grants or denies the request; if permission is denied, the request is denied. This process is initiated by the person in charge who attached the XACML rules to the Policy Administration Point and created them. The created guidelines are stored in the policy repository and forwarded to the policy decision point once they have been authorized by the public. Permission submissions are checked against these rules when a policy is made. The policy decision point carries out a number of regulations.

The API Manager served as the policy enforcement point for the XAMCL paradigm. The policy decision point receives the permission request along with any pertinent attributes if this supervisor gets an access request. When matching demand with the set regulations, the policy decision point collected request and its features. Policy decision point made an effort to contact policy data point for further details as needed. A user role is necessary for the API Manager, which requests usernames and implements rules. The data was obtained from the user store by the policy decision point, which was designated as a policy information point. The response and the rule decision are forwarded to the API Manager if the Policy Decision Point has the data needed to forecast demand.

Credentials were handled by a reputable user. Authorization is subsequently granted, the job is assigned, and the appropriate position is approved. This data is subsequently transported via the cloud. Using the valuations key, the third party executed the program and completed the owner-directed tasks. An outside source delivered the encryption key and the completed encrypted data. Every output was decoded by a client using a secret key. The client can safely perform actions in the cloud thanks to a range of security principles offered by the recommended authorization mechanism.

3.6.1 Privilege

Where consumers have greater flexibility, privilege is crucial—which is significant in any case. In order to gain a privilege, each client in this design fulfilled a number of tasks, each point had several actions that were finished, and each action earned an equal amount of rights. Thus, positions that follow preferred methods are offered by clients. Despite the client's unlimited access, this job still requires authorization in order to complete.

3.6.2 Accessibility

It establishes relationships between computer users and roles as well as between roles, responsibilities, and permissions. When it comes to privacy policy, there are several groups that provide the capacity to allocate authority effectively. It is feasible to transfer assignment rights from one account to another.

3.6.3. Accountabilities

Reciprocal obligations are required in this strategy in order to complete crucial tasks.

3.6.4. Dependability

Only a user's identity is being authenticated by RBAC. RBAC is unable to monitor a user's reliability in order to restrict login attempts and safeguard the network from unauthorized access. Extensible access control markup (XACML) is paired with RBAC.

3.6.5 Protected data

To guarantee information security and privacy while data is exchanged and kept in the cloud, the improved RSA technique is used. It prevents misuse of Communications Service Providers (CSP) or any danger to cloud-stored data.

Table 1: Response & Execution Time between Encryption & Decryption Techniques

Response Time(s)			Execution Time	
Block Size (bits) (s)	**Encryption**	**Decryption (s)**	**Info. Sent (s)**	**Received Data (s)**
128	0.13	0.32	0.28	0.44
256	0.36	0.37	0.42	0.60

Table 2: Using Encryption Time & Size of Key Generation

Size of Key	AES (s)(bits)	DES (s)	RSA (s)	Proposed RSA
1	0.04	0.05	0.08	0.07
10	0.34	0.34	0.79	0.34
50	1.63	1.91	4.59	2.30
100	4.28	6.63	5.98	5.24

4. RESULTS AND DISCUSSION

Depending on the quantity of files analyzed, this task uses Java technologies. You can increase the range of cryptographic algorithms that the platform supports with the help of the Java cryptography architecture. Owing to Java's widespread use, a large number of cryptographic tool developers supply certified JCP providers. An Intel Core i7 CPU running at 1.70 GHz with 16 GB of RAM is used to do this operation. The total execution time and reaction time for data transmitting, data receiving, decoding, and encryption for different block sizes are displayed in Table 1. And Table 2 contains most of the asymmetric approaches. The resulting encryption time duration is displayed in Table 2. Table 3 shows that information processing, including decryption and secret key release, is faster at different key sizes than current methods. Table 3 makes it evident that the decryption time grows in tandem with the key size.

Table 3: Decryption Time of Using Hybrid Technique.

Description Time(s)				
Size of Key	**AES (s) (bits)**	**DES (s)**	**RSA (s)**	**Proposed RSA**
1	0.04	0.04	0.05	0.05
10	0.24	0.32	2.38	3.44
50	2.86	1.93	4.87	3.23
100	4.99	6.02	3.94	3.12

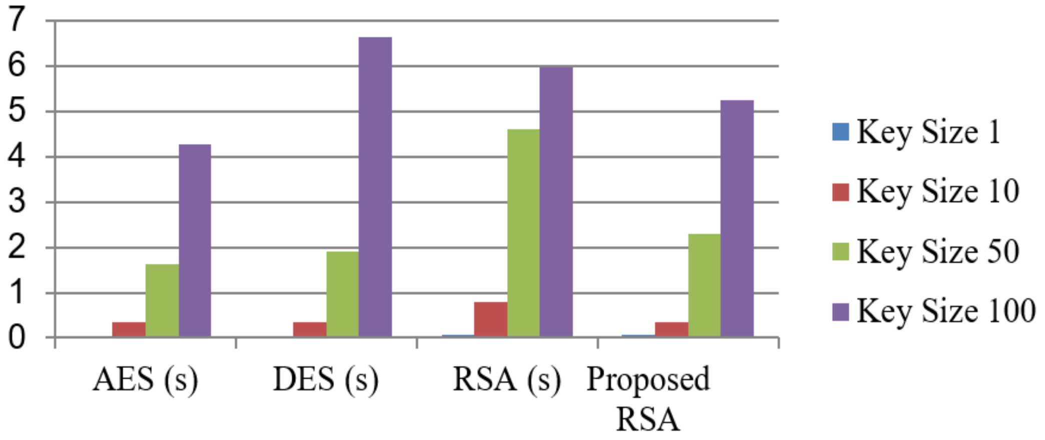
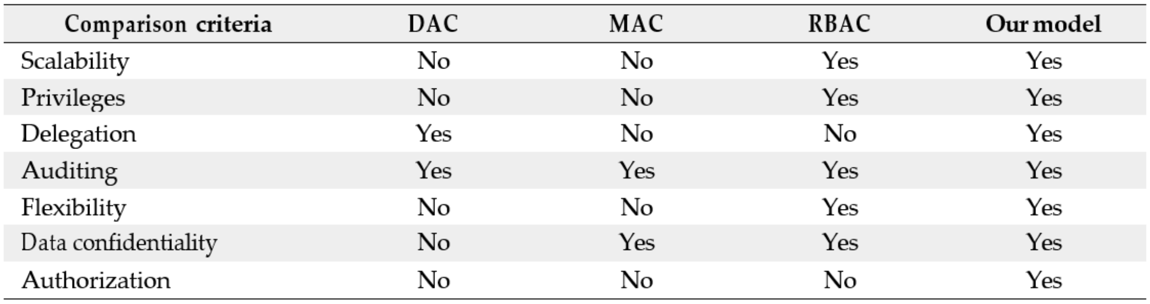


Figure 7: Decryption Time of the Various Techniques

Table 4: Comparison Criteris of the Access Control Models



Comparison criteria	DAC	MAC	RBAC	Our model
Scalability	No	No	Yes	Yes
Privileges	No	No	Yes	Yes
Delegation	Yes	No	No	Yes
Auditing	Yes	Yes	Yes	Yes
Flexibility	No	No	Yes	Yes
Data confidentiality	No	Yes	Yes	Yes
Authorization	No	No	No	Yes

Table 4 provides the timings for AES, DES, RSA, and improved RSA for key sizes of 1, 10, 50, & 100. When comparing the data analyzing rates of DES and RSA, AES is the quickest. Because AES uses symmetric keys, a single key may be used for both encryption and decryption. In contrast, RSA requires the usage of two keys that are uniquely coupled to each other: a public key and a private key. AES keys are composed of simple random bytes. Moreover, RSA is the most asymmetrical technique with the longest secret length, as shown in figure 7 shows how long each of the suggested techniques takes to execute overall. Thus, in order to evaluate the novel technique that results from combining the RSA strategy with the AES algorithms as an asymmetrical approach. Table 4 displays the access control models for DAC, MAC, RBAC, and the suggested paradigm, which includes Delegation, Scalability, Flexibility, Privileges, and Authorization. The methodology ensured data security when storing data on cloud technology by utilizing an enhanced RSA technique. RBAC rules that comply with XACML are considered to be associated with the permission process. The duration of the RSA method for various key sizes is displayed in figure 8 and figure 9.

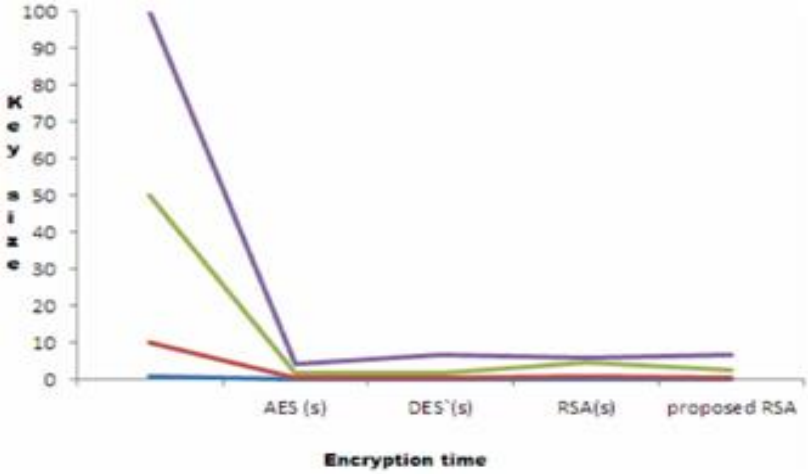


Figure 8: Different Techniques' Encrypting Times with Different Key Sizes

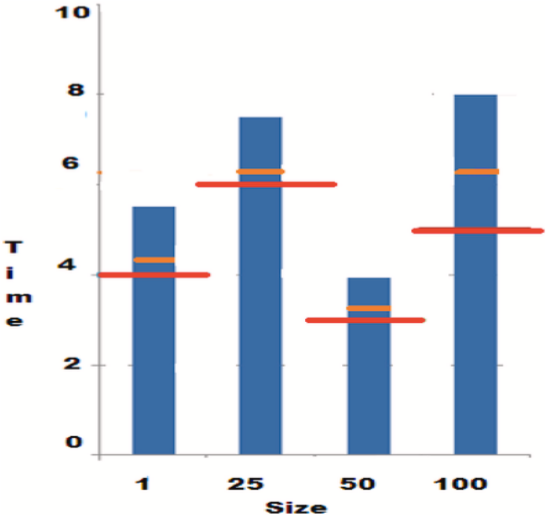


Figure 9: Analysis of the RSA's Execution Time for Different Sizes

Additionally, the outcomes of the time variations determined by the encryption and decryption of RSA as well as our suggestion are shown in Figs. 10(a) and 10(b). The system we use simulates the use of encryption for sending private information to a cloud server, as shown in figure 10(a) and 10(b). The results of the data showed that the strategy we used performed quicker than the conventional RSA procedure. Figure 11 displays the results of the study according to various data sizes with mean throughput traditional and proposed method.

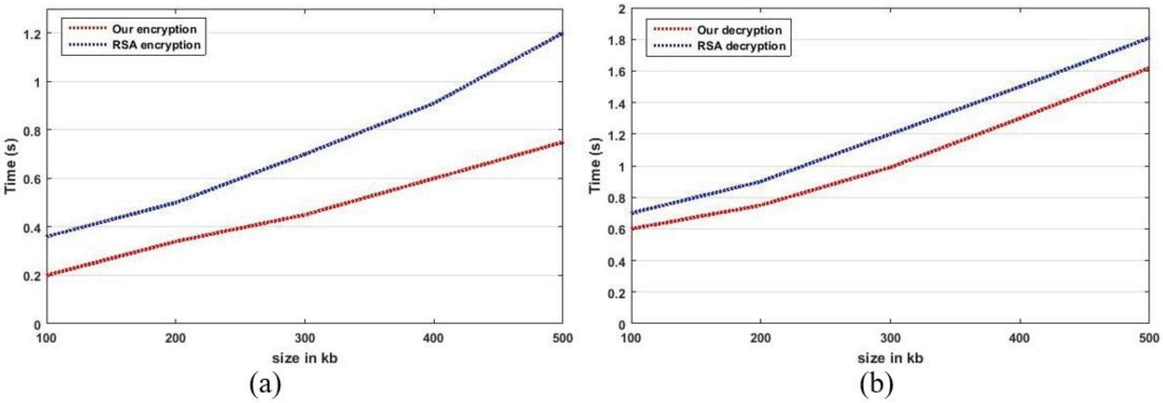


Figure 10: Our Encryption and the Original RSA are compared: The Processes of (a) Encryption and (b) Decryption

Table 5: Difference in Mean Throughputs.

User requests	Mean throughput (kr/s)	
	Traditional RBAC	Our proposal
5	29	30
7	40	42
9	48	50
11	49	53
13	45	47
15	43	44

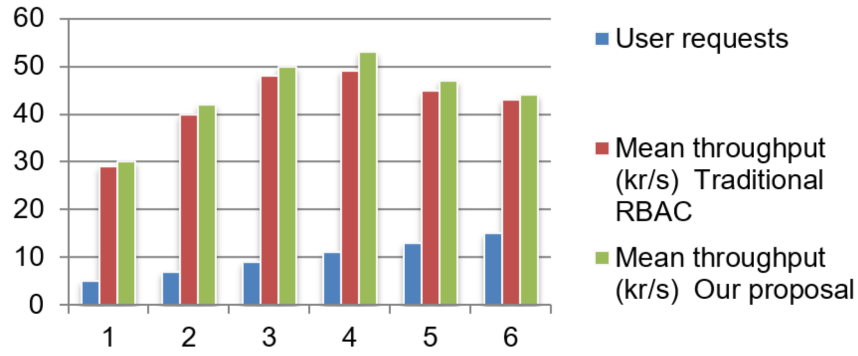


Figure 11: Comparison Chart of the Mean throughput Traditional and Proposed Method

Various key sizes are used to get the findings from experiments. It is therefore utilized to immediately safeguard user-provided data. The amount of information that a system can handle in a specific amount of time is known as throughput. It is measured in terms of requests per unit of time. The throughput variations among RBAC and RBAC with enhanced RSA and XACML which were examined in the current research are shown in Table 5. From the start of request 1 until the conclusion of request 10, the throughput is calculated. It demonstrates how customer information housed in the cloud is better protected by the suggested accessibility model then by RBAC.

5. CONCLUSION

To enhance privacy and safeguard communication, the suggested architecture is built with RBAC and enhanced RSA techniques combined with XACML. According to the study, there are greater benefits to using this suggested accessibility approach than traditional RBAC. Due to its rapid processing of data, the AES asymmetrical approach is far more cost-effective in a virtual environment than other techniques. Because of the total secret size, the RSA approach is more durable than others. The enhanced RSA algorithm is created by combining the AES and RSA algorithms. Two varieties of symmetrical and unsymmetrical decryption systems are examined at various data inputs in cryptography techniques. The encryption and decryption of information with varying bit sizes took a shorter period with these approaches. Due to its fundamental approach to leadership, it is also trustworthy and safe. In order to give an encrypted secret to every authorized individual while requiring a cloud server, new key management techniques will be developed as time goes on.

References

1) C. Butpheng, K.H. Yeh, and H. Xiong, “Security and privacy in IoT-cloud-based e-health systems a comprehensive review,” *Symmetry*, vol. 12, no. 7, July 2020, 1191.

2) R. K. Shukla, A. K. Tiwari, and A. R. Mishra, “Face Recognition Using LBPH and CNN” *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, vol. 17, no. 5, pp. 48-58, 2024.

3) S. Mishra, S.K. Sharma, and M.A. Alowaidi, “Analysis of security issues of cloud-based web applications,” Journal Ambient Intelligent Human Computer, vol. 12, no. 7, pp. 7051–7062, July 2021.

4) P. K. Tripathi, R. K. Shukla, N. K. Tiwari, B. K. Thakur, R. Tripathi, and S. Pal, “Enhancing Security of PGP with Steganography,” *In 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pp. 1555-1560, December 2022, IEEE.

5) R. K. Shukla, A. S. Sengar, A. Gupta and N. R. Chauhan, “Deep Learning Model to Identify Hide Images using CNN Algorithm,” *In 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pp. 44-51, December 2022. IEEE.

6) D. Jang, M. Shin and D. Pathirage, “Security Fault tolerance for access control,” *In 2020 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C)*, pp. 212–217, 17 Aug 2020, IEEEE.

7) M. Shakir, M. Hammood and A.K. Muttar, “Literature review of security issues in saas for public cloud computing: a meta-analysis,” International Journal of Engineering & Technology, vol. 7, no. 3, pp. 1161-1171, 2018.

8) N. R. Chauhan, R. K. Shukla, A. S. Sengar and A. Gupta, "Classification of Nutritional Deficiencies in Cabbage Leave Using Random Forest," *In 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pp. 1314-1319, December 2022. IEEE

9) A.G. Khan, S. Basharat and M.U. Riaz, "Analysis of asymmetric cryptography in information security based on computational study to ensure condentiality during information exchange," *Int. J. Sci. Eng. Res.*, vol. 9, no. 10, pp. 992–999, Oct 2018.

10) R. K., Shukla and A. K. Tiwari, "Masked face recognition using mobilenet v2 with transfer learning," *Computer Systems Science & Engineering*, vol. 45, no. 1, 2023.

11) G. Batra, V. Atluri, J. Vaidya, and S. Sural, "Deploying ABAC policies using RBAC systems," *Journal of Computer Security*, vol. 27, no. 4, pp. 483–506, Jan 2019.

12) R. K., Shukla, A. K. Tiwari and A. K. Jha, "An Efficient Approach of Face Detection and Prediction of Drowsiness Using SVM," *Mathematical Problems in Engineering*, vol. 2023, no. 1, 2023, 2168361.

13) H. Al-Samarraie and N. Saeed, "A systematic review of cloud computing tools for collaborative learning: opportunities and challenges to the blended-learning environment," *Computer Education, vol.* 124, pp. 77–91, Sep 2018.

14) M.M. Sadeeq, N.M. Abdulkareem, S.R. Zeebaree, D.M. Ahmed, A.S. Sami, and R. R. Zebari, "IoT and Cloud computing issues, challenges and opportunities: a review," Qubahan Acad., J. vol. 1, no. 2, pp. 1–7, Mar 2021.

15) N.Mansouri, R.Ghafari and B.M.Zade, "Cloudcomputingsimulators:acomprehensive review," *Simulating Modeling Practise Theory*, vol. 104, Nov 2020, 102144.

16) M.N. Birje, P.S. Challagidad, R.H. Goudar and M.T. Tapale, "Cloud computing review: concepts, technology, challenges and security," *International Journal of Cloud Computing*. Vol. 6, no. 1, pp.32–57, 2017.

17)] K. Jiao, G. Ye, Y. Dong, X. Huang and J. He, "Image encryption scheme based on a generalized arnold map and RSA algorithm," *Security Communication Network*, June 2020.

18) S. Shamshirband, M. Fathi, A.T. Chronopoulos, A. Montieri, F. Palumbo and A. Pescap`e, "Computational intelligence intrusion detection techniques in mobile cloud computing environments: review, taxonomy, and open research issues," Journal Information Security. Application, vol. 55, Dec 2020102582.