ISSN 2063-5346

ESPP: INVESTIGATING THE EFFECTIVENESS OF SECURE & PRIVACY IN CLOUD ERP SYSTEM

Ekta Sabbarwal[1], Daya Shankar Pandey[2]

Article History: Received: 10.05.2023 Revised: 29.05.2023 Accepted: 09.06.2023

Abstract

As in today's era, everything is moving towards digitalization. Emerging in technology creates every organization has its Enterprise Resource Planning Tools. In India or any country, every data of any organization is controlled by its ERP. As when we deal with the data of any organization, there are many different users and we need to control data privacy to users. We need to control, maintain, and regulate the data as per the user requirements and as per the data authorized to the N user. So one organization needs to focus on the privacy of the data or the services concerning the users. So that no user can either underutilizes the data or services nor over-utilizes the data or services. One user can efficiently use authorized resources and services. As mostly the privacy and security of any organization data or services are disturbed by attacking the system. Usually, the attacks are of two types Active attacks and passive attacks. Usually when someone tries to attack the privacy of the model then security also disturbs. So we can say that security and privacy are hand by hand concerns. In active attacks, the attacker tries to manipulate the data or services whereas in passive attacks the attacker observes the data or the service and uses it in a wrong way. So there are basically two possible places where the attacker can raise the threat one is the communication channel and the second is the server. So need a model which can easily handle these issues to maintain the privacy of any ERP. The proposed model aims to provide an Effective and Secure Privacy-Preserving Technique for Cloud ERP so we named the proposed model as ESPP (Effective and Secure Privacy-Preserving) Model. The proposed model focus on providing an architecture that can't be attacked easily so that it's privacy will remain preserved. The proposed system focus on controlling the user and the data transmission to reduce the threats to privacy.

Keywords: Cloud ERP, Security, Privacy, Active attack, passive attack, ESPP.

[1]Research Scholar, Department of CSE, Sarvepalli Radhakrishnan University, Bhopal, M.P, India, sabbarwalekta19@gmail.com

[2]Professor, Department of CSE, Sarvepalli Radhakrishnan University, Bhopal, M.P, India, dayashankar.rkdfist@gmail.com

DOI:10.48047/ecb/2023.12.9.110

1. INTRODUCTION

Multiple customers are served as a raised area with an innovative solution by the cloud ERP software. ERP hosting, which functions as a third party to support software communications and submission services provided by the cloud environment, may be confused with the idea of cloud ERP. Others characterized cloud ERP as platforms for cloud computing that are utilised to deliver services to organizations so they can conduct their operations more efficiently [1]. SaaS offers cloud computing for organizations with infrastructure capabilities, like ERP systems, as one example [2]. Since cloud computing may quickly adopt the point of view of ERP operation, cloud-based software companies are adept at quickly expanding their functionality. Users of the cloud can quickly and immediately access the offered services. The tragic transition from traditional ERP to ERP cloud has significant problems with superior farm tasks, such as the potential for attacks from the internet environment or the start of the internal and external security consultants of the cloud provider [1]. With the ability to access submission modules through the software as a service (SaaS) delivery model and with submission users having the freedom to build up and commit to a set of application modules based inactive on an architecture known as multi-tenancy, cloud-based ERP is an expansion of integrated industry suites supporting ERP, CRM, and ECommerce. [3]. Security organize harms can be summarized by using cloud ERP, which assists users to steer away of conformist ERP systems, in the red to the higher security issues that cloud providers can carry out. Making sure security controls in software and hardware using IT security specialists, who can be accessed by cloud providers with high levels of security, dispensation control, and storage units, is one of the main difficulties of data security [4]. Finding appropriate ways of authorisation and confirmation due to the service sharing with several tenants via the cloud contributor is another significant difficulty for cloud ERP. Users, third parties, and cloud ERP contributors should all have the legal authority to use their respective responsibilities to enter the cloud ERP application border using their confirmation credentials. There are a variety of access control techniques available in cloud ERP to ensure the secure access of tenants who share resources and services [5] but are not the same.

1.1. Enterprise Resource Planning (ERP)

ERP (enterprise resource planning) software has emerged as a key area of attention for many firms with the advent of E-Business and the need to impact several sources of in sequence throughout the enterprise. ERP systems are currently concerned with every associational attribute since they offer an incredibly comprehensive justification to satisfy information system requirements. ERP has evolved into a fundamental requirement for businesses of all sizes and importance. Currently, ERP systems are regarded as essential in-sequence systems communications. ERP is a type of software design that makes it easier for information to flow across disparate parts of a project.[6] The sharing of information across directing units and geographical areas is also facilitated by ERP. All of an organization's business operations and assets are managed, documented, set up, and under control using ERP [7]. ERP is used to manage and integrate all business operations in a society, which frequently include a collection of middle-aged business software and tools for financial and cost accounting, equipment management, sales and allocation, production development, human resources, and computer-integrated manufacturing, supply chain, and consumer data. [8]. The successful adoption of ERP systems requires excellent project management on

the part of an organization. The deployment of ERP requires identifying key goals clearly, creating resource and task plans, and closely monitoring the project's progress. Therefore, the project plan should include destructive and doable tasks that are prepared into schedules that help identify necessary and dependent actions. [9].

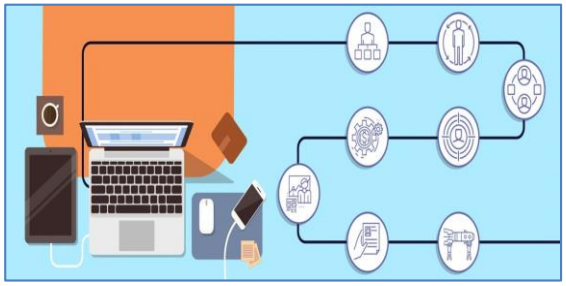

Fig. 1 Cloud ERP

Each ERP has its unique format for data structures and user groups according to the specific organisation. The major problem with physical or offline systems is that scaling them requires a lot of additional resources, but the scalability problems with cloud ERP have been resolved and can now be scaled relatively easily to meet our needs. Users of cloud ERPs only need to be familiar with the system or system's user interface; they are not concerned with where the data or services are physically located. Users can access the Cloud ERP from anywhere in the world with the help of the internet as everything is moving online. Every piece of information was previously only accessible by one person at a time because it was in physical form, but with the aid of cloud ERP, N users can have simultaneous access to the same database. Any company's or ERP's computing requirements can easily be scaled to meet the needs.

Fig. 2 ERP System

The privacy of the data and the use of the services are maintained in large part by all points or ends of the ERP. Since we would lose the privacy of our data and services and any unauthorised user may access our data if either of them were attacked, the ERP's design and security model must be strong enough to maintain both privacy and system security. Attacks against ERP's privacy are typically made either via the server or the communication channel. Therefore, in order to decrease the likelihood of losing privacy, we need effective and reliable models to provide security to the ERP. The model must also be able to authenticate and authorise users in relation to the ERP. Only legitimate users should be able to access the data, according to the security or privacy-preserving model, to prevent unauthorised users or attackers from doing so. Here, we provide an ERP security paradigm to protect privacy so that we may offer safe data access and safety services.

ERP (enterprise resource planning) software has emerged as a key area of attention for many firms with the advent of E-Business and the need to impact several sources of in sequence throughout the enterprise. ERP systems are currently concerned with every associational attribute since they offer an incredibly comprehensive justification to satisfy information system requirements. ERP has evolved into a fundamental requirement for

businesses of all sizes and importance. Currently, ERP systems are regarded as essential in-sequence systems communications. ERP is a software design that makes it easier for information to flow between disparate parts of an enterprise. ERP supports information sharing among administrative units and environmental areas in the same way [7]. ERP is the management, documentation, configuration, and control of all business operations and assets inside an organisation. A set of middle-aged business applications and tools for financial and cost accounting, equipment management, sales, and allocation are frequently included in the business functions that surround an organisation. ERP is used to manage and include all of these business operations, production development, human resources, and computer incorporated manufacturing, supply chain, and consumer information [8]. The successful adoption of ERP systems requires excellent project management on the part of an organisation. The deployment of ERP requires identifying key goals clearly, creating resource and task plans, and closely monitoring the project's progress. Therefore, the project plan should include destructive and doable tasks that are prepared into schedules that help identify necessary and dependent actions. [9].

1.2. Life Cycle of ERP

Depending on the information system project's quality and the local regulations governing ERP implementation, the four phases of the project life cycle model for ERP implementation—shown in Fig. 3—may be combined into a single, cohesive whole. These phases are: programming; executive; stabilization; and climbing.[7]

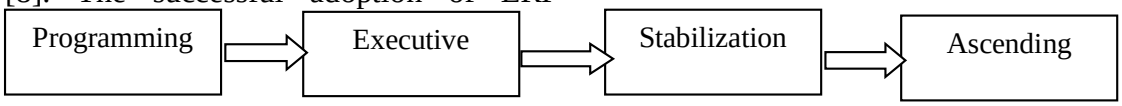

Fig. 3: Implementation life cycle of ERP

- **Programming Phase**

  The first phase of the ERP implementation project is the Programming chapter. Its duty is to set up for the following phase. It involves gathering an ERP, assembling a steering committee, assessing the high-level project capacity and the scope of the implementation, gathering a project team leader, and reserving willpower.

- **Executive Phase**

  In the administrative phase, the main objective is to establish a business development strategy that can satisfy the prospective command of the customer. Other tasks include installing the system, starting the implementation project, training the core team, special-subject conversing, medium-term, and ending test [10]. The level of project management in the phase will determine whether the ERP implementation project succeeds or fails without fail. Set-up, re-engineering, design, arrangement & testing, and installation are the five sub-phases of the phase. A graphic illustration of the project life cycle is shown in Figure 3.

- **Stabilization Phase**

  In the stabilisation phase, the outdated system will be replaced by the new one. Additionally, the data will be distorted throughout this phase, and the end-user will be identified. The system overhaul, extension, and transformation stages are all part of the stabilisation phase, which can last for several years and continues until all end users are able to use the new system technology.

- **Ascending Phase**

  In order to evaluate business advancement level, capacity situation, and system completion, ERP installation success will be compared with the goal that is proposed in the programming sub-phase. The system must be detailed and truthful in order to upgrade software, for example.

2. RELATED WORK

Gupta et al. proposed the SP-MAACS scheme in 2023 as a secure and confidential multi-authority authentication cum authorization system for cloud-based healthcare data sharing. By only disclosing the names of policy attributes, policy privacy is preserved while taking into consideration users from both open and closed domains. The values of the features are not disclosed. A distinctive comparison with similar existing schemes demonstrates how our solution simultaneously offers benefits like multi-authority setup, expressive and adaptable accessible policy framework, safeguarding privacy, and scalability. The results of our performance analysis show that the deciphering expense is reasonable low. In addition, the conventional model proves that scheme is adaptably secure. [11].

In the proposed research of Gayathri S. and Gowri (2023), a significant emphasis is placed on the design of a thin cloud architecture that is capable of securely transmitting medical data without breaching patients' right to privacy. The recommended system develops an effective picture denoising method with a hybrid classification model to guarantee reliable and secure communication. Combining deep learning methods yields the pseudo-predictive deep denoising network (PPDD). The advantage of the recommended approach is that it boosts security in Dark Cloud by using a fresh arranged algorithm. The original data is secured in the deep cloud using the Gaussian noise as a key. The entire packaging and unpacking of medical data is depicted in the manipulated photographs. Cloud data is very secure and protected from malicious users. At the edge devices, the dynamic data is unpacked and the denoise method is applied to lessen storage complexity. Only during the approved access time is data decrypted and available at the edge nodes. Most operations happen on the cloud dynamically, without regard to storage boundaries. The proposed PPDD network model's effectiveness is evaluated using the signal to noise ratio (SNR), similarity index (SI), error rate (ER), and contrast to noise ratio (CNR). The proposed architecture is assessed using up-to-date cutting-edge techniques [12].

Ray and Dutta (2022) concentrated on brand-new techniques for identifying sensitive data. Additionally, non-sensitive qualities are distinguished by the attributes' sensitivity scores, and a domain expert is crucial to this procedure. The system is strengthened and more trustworthy thanks to the design of the security assurance Algo and its accompanying decision tables. The legitimacy of the research effort is amply demonstrated in the results section, which is proven with the aid of graphical representation. In conclusion, the authors may claim that the suggested system's automated sensitive data identification and security assurance functions best in a cloud-based system [13].

Among others, Bayan O Al-Amri (2020) The massive increase in cloud storage usage over the past few years has created a great demand for a cutting-edge method and powerful tools to make services even more useful and safe. Due to the fact that data privacy in cloud computing has grown to be one of the top concerns for both

consumers and businesses, there is increased demand on cloud service providers to earn their customers' trust. This paper reviews several privacy-preserving methods used in cloud computing and discusses their key features and tools, along with an explanation of their purpose. This research intends to concentrate on the most effective and cutting-edge methods that scientists have developed and examined to date.[14]

With MAMOUN HADIDI and others set to take office in 2020, The enterprise resource planning (ERP) system is one of the most important tools used by organisations of all types, whether they are governmental or private. A range of ERP systems that depend on Internet services have evolved as a result of the quick expansion of Internet services and rising reliance on the infrastructure of companies that provide Cloud services. In addition to the traditional type of ERP system, the most significant ERP types include Web-based ERP and Cloud ERP. As a result, manufacturers of ERP systems like Oracle and SAP are focusing on designing ERP systems based on cloud technology and providing the ERP system as a service for monthly and annual subscription, where the system is external to the organisations and does not need to exist within the organisation. The various ERP system variations will be looked at in this essay, along with the essential differences between conventional and cloud-based ERP. Enterprise resource planning (ERP) systems can be deployed in a variety of ways to help organisations achieve their diverse goals and improve performance by selecting the best application type for the planning system.[15]

D. Soni and M. Kumar (2017) A form of computing technology known as cloud computing allows users to access resources from a central pool of resources. Large-scale resource management is required of the cloud management software. The term "cloud" refers to pervasive computing, which can be found anywhere. In today's technological age, cloud computing has emerged as a substitute for traditional internet access. The two primary entities involved in cloud computing are the cloud user and the cloud service provider. Since a cloud is a collection of several nodes, it can serve a wide range of applications that Clients utilise on a pay-per-use basis. These days, cloud computing is increasingly popular due to its pay-per-use features. However, there are concerns and challenges with cloud computing security, which is turning into a point of competition between different cloud service providers [16]. They provided a thorough examination of security concerns in the cloud computing environment as well as difficulties that are focusing on the various forms of cloud computing in their survey paper. They demonstrated the cloud trust protocol, which is a method for limiting these difficulties and problems. D. Soni et. al. in 2016 discussed about a algorithm called CDM cloud data Mining algorithm. This algorithm discuss how to efficiently use cloud space for different business uses [17].

G. Ananthanath and B. Naresh Kumar (2019) Distributed computing is a way of thinking that enables clients (records owners) to store their information and allows statistics consumers (clients) to access that information from cloud servers. The capability and support value of the information owner are reduced by this mindset. While this is going on, the information owner loses the ability to physically control and own the information, which opens up numerous security issues. Along these lines, it is crucial to examine management to evaluate data reliability inside the cloud [18]. This issue has become a test since the ownership of information needs to be verified while maintaining privacy. This paper suggests the simple and effective privacy-preserving provable

information possession (SEPDP) to overcome those issues. We also extend SEPDP to support a variety of owners, informational components, and cluster affirmation. The most enticing aspect of this strategy is how easily the evaluator may determine who owns certain facts. Devaraju S. et. al. discussed about association base rule mining to detect intrusion based on entropy based feature selection. This is helpful in ERP cloud system also [19].

Soni D. et al. in 2021 discussed about a new paradigm called "cloud computing" enables users to store their data on a reliable and adaptable foundation, and information buyers can access that data via cloud servers. This perspective lowers the information owner's support and stockpiling costs. In the interim, the owner of the information forfeits physical possession and control of the data, creating numerous security risks. Therefore, a data integrity auditing solution is crucial for the cloud. As the possession of data needs to be validated while retaining protection, this problem has increasingly challenging [20]. This paper suggests a safe and efficient security-saving proven information ownership system to address these problems. SEPDP is further extended to handle various proprietors, data dynamics, and clump verification. The reviewer may easily and quickly confirm the existence of the data using this approach, which is its most enticing feature. Dheresh Soni et, al. in 2019 has discussed about framework for secure encrypted communication of textual data in cloud computing through SAAS layer. This framework is applicable for homogenous textual data [21].

Kulwinder Kaurand (2018) Brahmaleen Sidhu discussed an emerging area of information technology is cloud computing. Because it offers services like PaaS (Platform as a Service), SaaS (Software as a Service), and IaaS (Infrastructure as a Service), the cloud is the foundation of information and technology. The big three corporations, Amazon, Microsoft, and Yahoo, all have their own clouds and offer services [22]. Given that the cloud offers all of these important services, cloud security has emerged as a crucial problem. Data is transferred frequently between users and the cloud. Since the information is private, the large amounts of data stored in a cloud environment need to be protected from unauthorised access. The primary goal of this essay is to examine the numerous security measures used to counter the current threats to information security. In 2022 dheresh soni et. al. discussed secure communication in cloud between clients in encrypted way which help in our approach for encryption [23].

3. PROPOSED METHODOLOGY

Our main goal is to protect the cloud ERP's privacy. So, for the Cloud ERP System, we have proposed an Effective and Secure Privacy-Preserving Technique. Additionally, we have named the model we have suggested as the ESPP Model. The following name's entire form is provided below,

E-Effectiveness and S-security, P - Protecting p - Privacy

We can label the model for our job using acronyms. A name for the model aids in identifying it when we combine unique elements or frame something novel. We have suggested a privacy-preserving method whose primary goal is to offer excellent security so that privacy can be maintained. Our suggested system consists of numerous parts. But before this let's take a look at the basic ERP system without a security model.

3.1. Working of Cloud ERP

The basic operation of the ERP is depicted in the diagram below, in which the user requests data from the services provided by the ERP and receives a response. When security and privacy of the data or the services are disregarded, the system looks like this, where users can request services and receive responses. But in the modern era, the data are private, and only a select group of authorised users are permitted access to the data or the system's services. The system must have a strong security system in place to prevent outsiders from attacking it. It must also be able to manage fraudulent users that are present in the system and limit the access of undesired and invalid users.

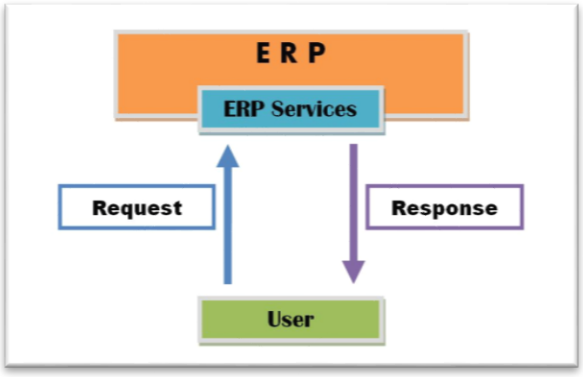

Fig.4. Basic ERP Working

So, this is a very simple request and response architecture of the ERP showing that how a user request and the Cloud ERP response to the following request.

3.2. Layout of proposed System

Having no security model or privacy-preserving with Cloud ERP can cause a big issue to the organizations having the ERPs. So, we need a security and privacy-preserving model in the whole working process so that we can use the data and services efficiently and properly. Also, this will lead to access to the ERP in a valid manner by valid users.

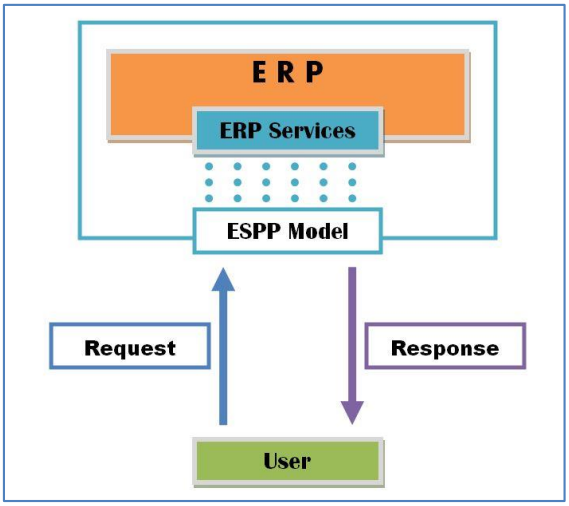

Fig. 5: Basic Layout of Proposed ESPP Model

Before using the privacy-preserving model over the process we need to fame out the ends where it is required the most. We need to control, maintain, and regulate the data as per the user requirements and as per the data authorized to the N user. Organization needs to focus on the privacy of the data or the services concerning the users. So that no user can either underutilizes the data or services nor over-utilizes the data or services. One user can efficiently use authorized resources and services. As mostly the privacy and security of any organization data or services are disturbed by attacking the system. Usually, the attacks are of two types Active attacks and passive attacks.

Usually when someone tries to attack the privacy of the model then security also disturbs. So we can say that security and privacy are hands by hand concerns. In active attacks, the attacker tries to manipulate the data or services whereas in passive attacks the attacker observes the data or the service and uses it in a wrong way. So, there are basically two possible places where the attacker can raise the threat one is the communication channel and the second is the server. So need a model that can easily handle these issues to maintain the privacy of any ERP.

All over our motto is to secure the medium or communication channel and the server or the cloud ERP, cause these two are the only ends where attacking can be done. So our proposed model ESPP Model deals with securing the cloud as well as the medium so that we can reduce the chances of privacy leak. Providing security to the cloud deals with giving access to only the valid user and valid interfaces. Securing the communication medium means securing the data when it travels from Either the Cloud to the user-end or from user-end to the cloud. This kind of security can be provided with the help of encryption techniques. So let's Dive into and try to understand the proposed architecture properly.

3.3. Proposed Model

The main objective behind the proposed model is to preserve the privacy of the model so that the ERP's data and services become more secure. The main focus of the proposed system is to secure two Ends properly in which one is the Services of the ERP and another is the medium of communication between the User and the ERP.

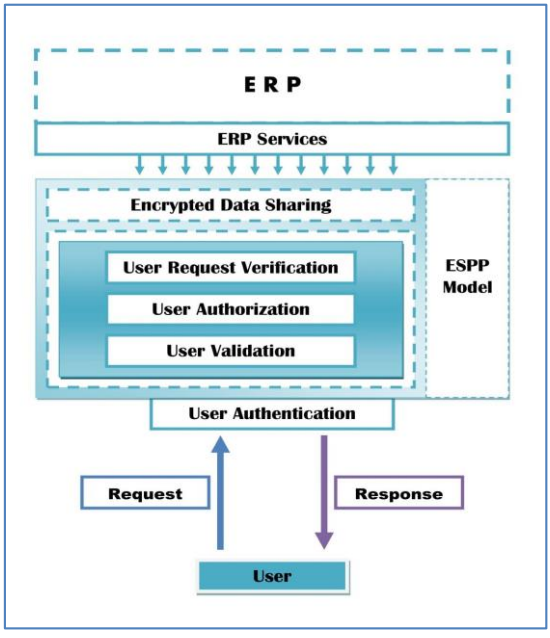

Fig. 6 –ESPP Model

The recommended model's primary goal

1. The safety and confidentiality of cloud-based services.

2. Safeguarding the medium of transmission.

The suggested design consists of numerous parts. As a bridge among the user and the cloud ERP services, the recommended ESPP model functions. For the purpose of maintaining privacy, the model offers an effective and secure paradigm to ERP. The proposed ESPP model mainly concentrates on the system's component in greater detail. We can apply any particular kind of algorithm depending on the ERP's processing capability, space constraints, and storage needs. The Proposed ESPP Model consists of the following elements. Let's look at the names first, and then we'll learn more about how each one functions.

A Elements of the Suggested ESPP Model

1. Verification of users
2. Authorization of users
3. Authentication of users
4. Confirmation request of users
5. Sharing of Encrypted Data / Flow of Encryption data

The ESPP Model's constituent parts are as follows. Every element of the model is essential to maintaining the cloud ERP's privacy and assisting the system in achieving a higher level of security. Let's examine each element in detail so that we can comprehend them with the aid of the process flow.

3.3.1. Authentication of users

Login verification is crucial for any enterprise resource planning system. It is the process of determining whether or not a user is a legitimate user. Another way to put it is that this cloud only recognises the user's identity. It's a technique where we assign each user a set of credentials, and

anytime a user requests access, the credentials are always needed to confirm the person's reliability and authenticity. To prevent anyone from the admin side from seeing the safe credentials directly, the server stores all of the safe credentials in an encrypted format. When the building represents the ERP, authentication is like the door. So, using the credentials, we must pass via the first door if we need to access the building. The owner of the ERP can choose from a variety of authentication methods to utilise the desired and cost-effective one. Every time a user wants to access the Cloud ERP, they must first authenticate themselves. So, this has to do with system user authentication. Although it is the most necessary step, authentication is a relatively straightforward process. Simply said, it filters out all of the typical undesirable users.

3.3.2. Authorization of users

In the Cloud ERP, authorization is the second-most important step. It serves as a security measure of sorts. Simply providing and denying access to the various users to the Cloud ERP's resources and services sums up the entire procedure. Typically, this information describes the access that is permitted according on the user's position within the company. For instance, when discussing any organization's cloud ERP, the receptionist only has a limited number of portal visits that are specifically linked to their job. Every user in the ERP has their own necessary and allowed access to the Cloud ERP services since each clerk in the same firm has a different level of access to resources. When users attempt to access the ERP after the model has confirmed that they are authorised through authentication, the ESPP model checks to see if they are authorised to use the service they are attempting to access. If it is accepted, the user can continue; otherwise, they are simply prevented from doing so and their session will collapse. If a user tries to access any undesirable data or services that are only available to that specific user, they are directed back to the authentication page. The access control process in ERPs or other systems typically combines these two processes, with the exception that the first step is authentication and the second step is authorisation.

3.3.3. Verification of users

Typically, when we use the phrase "validation," we want to check something and acknowledge it by sending signals indicating whether it is correct or incorrect. Here, the terms "validation" relate to the backend operation of the user's authentication and permission. Here, the user's physical address is also verified as part of the validation. This indicates that whenever a new user tries to access the ERP and authenticates themselves using a new device for the first time, the user validation portal in the backend sends a request to the server informing it that a device with the specified physical address wants to access the data. The request can be accepted or rejected by the server depending on whether it uses the ESPP Model or the ERP. Most requests that come from real, accurate physical addresses are simply granted by the system. However, the server administrator must perform manual tasks in order to process uncommon physical address requests. The users' devices used to be restricted in some organisations. However, with our system, this process will be completed once for each device. This kind of procedure will assist us in preventing bogus users (with strange physical addresses) from accessing our system and the ERP, as well as aiding in enhancing the security of the latter.

3.3.4. Confirmation request of users

This is identical to user verification, however here the requested resources or services would only be confirmed in relation to the user from the very first time.

In user validation, the proposed ESPP model verifies the physical address. This is the final phase to fulfil the request if any user successfully completes the first three steps. One of the key components of the proposed ESPP model, this also functions in the user's backend. The proposed model automatically raises a request to the admin that this specific user, with this identity and with this physical address wants to access that specific part of our Cloud ERP whenever any user tries to access the particular part of their ERP or any particular portal for the very first time. For each user, this process only needs to be done once. The user can access the necessary and desired resources after the admin gives them permission to do so. The main advantage of this type of portal is that fraudulent users who are unwelcome can be prevented because they are unaware of internal operations and requests. Since ERP is typically used for closed organisations, this approach allows us to keep out undesirable individuals.

3.3.5. Sharing of Encrypted Data / Flow of Encryption Data

As each of the aforementioned 4 elements is primarily contributing to the server's security. The communication channel, also known as the medium of communication, is the second most crucial element in maintaining privacy in any system. The fact that the data is typically transmitted in a format that is easily readable by humans is to blame for the majority of the difficulties identified. Any attacker in the middle can easily read the data there. However, there is a mechanism that encrypts the data that needs to be transported from the origin and decrypts it at the receiving end in the suggested ESPP Model. This only implies that if the user is transferring data to the Cloud ERP, the data will be encrypted at the backend using a random key produced for T seconds. The server only needs to decode the data and carry out the requested action because the destination and key are already shared with the message in a specific pattern when the request reaches it. The addition of such features to ERP may make work a little more difficult, but it will also increase security and privacy to higher levels.

4. RESULT ANALYSIS

This section of research work is briefly explains the experimental results and analysis of proposed methodology among the exiting approach. We have proposed a model as an Efficient and Secure model for Privacy Preservation in Cloud ERPs named as ESPP Model. As the model is itself able to tackle all the security regarding issues. From having its Authentication, system to providing security to the communication channel the Proposed System (ESPP) is capable of taking care of everything and in an efficient way. The Proposed System (ESPP) has a unique workflow as well as there is something new proposed, as every node so that we can make the model more secure and efficient in terms of resources and computational needs. The major focus of the proposed model is to preserve privacy and for this, it is taking the server and the communication channel in reference because these two are the only place where privacy can be attacked. So All over the proposed model is way better than the past models.

4.1. Evaluation and Implementation Results

Implementation Size: It tells about the expected size of the model after implementation. Model having a large size have lower efficiency. In this fig. 7, the graph between proposed and existing model or methodology is shown and it is found that our model has medium implementation size than the existing method.

Table 1 Comparison of Implementation Size

Systems	Implementation Size
Existing System (CSP)	90
Proposed System (ESPP)	50

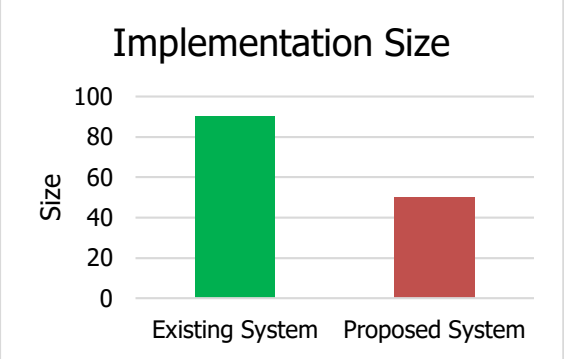

Fig. 7: Implementation size comparison between proposed and Existing System (CSP)

Implementation Complexity: It tells about the expected Complexity which we will face while implementation. Model having a large complexity have lower efficiency. Here fig. 8 shows the implementation complexity of proposed and exiting model and it is analyzed that the implementation complexity of our proposed model is medium while the other (exiting) model has very high implementation complexity.

Table 2 Comparison of Implementation complexity

Systems	Implementation Complexity
Existing System (CSP)	97
Proposed System (ESPP)	58

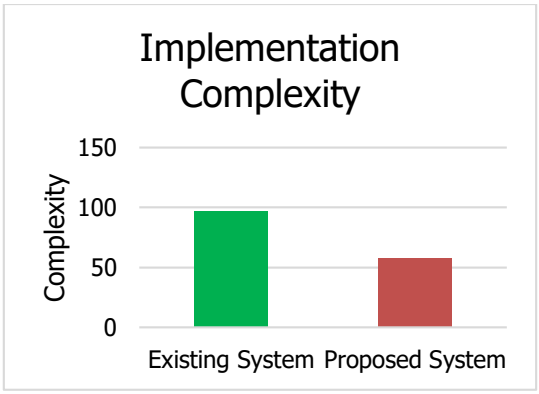

Fig. 8: Implementation complexity comparison between proposed and Existing System (CSP)

Implementation Time: It tells us about the time we need to implement the model. Model having a large implementation time have lower efficiency with respect to the time taken to implement. Here fig. 9 shows the time taken in the execution or implementation of model for proposed and Existing System (CSP) in which our Proposed System (ESPP) requires less implementation time than the existing.

Table 3 Comparison of Implementation Time

Systems	Implementation Time
Existing System (CSP)	95
Proposed System (ESPP)	63

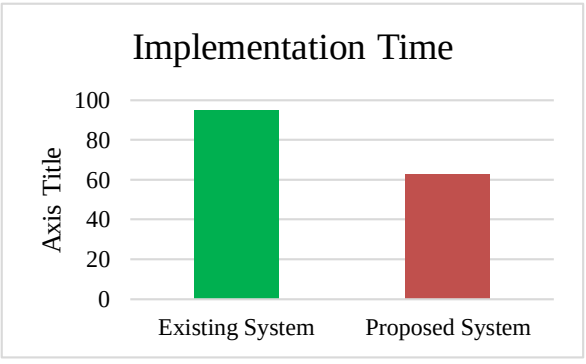

Fig. 9: Implementation time comparison between proposed and existing model

Solution Complexity: It tells about the expected Complexity which we will face while providing any kind of solution with a particular model. Model having a large complexity have lower efficiency. It means those models which has high implementation size and requires high implementation time then that model will also have high solution complexity. The solution complexity of proposed and existing model is shown in fig. 9 and found that our model has medium solution complexity than the existing model.

Table 4 Comparison of Implementation Time

Systems	**Solution Complexity**
Existing System (CSP)	91
Proposed System (ESPP)	65

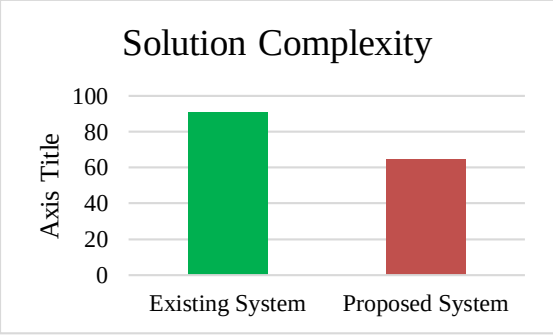

Fig. 10: Solution complexity comparison between proposed and existing model

Capital Cost: It tells about the cost we need to implement the model. Model having a large capital cost have lower efficiency about affordability. Here fig. 5.11 shows the comparison graph of proposed and existing model for capital cost in which the capital cost of our model is less than the existing model.

Table 5 Comparison of Capital Cost

Systems	**Capital Cost**
Existing System (CSP)	97
Proposed System (ESPP)	71

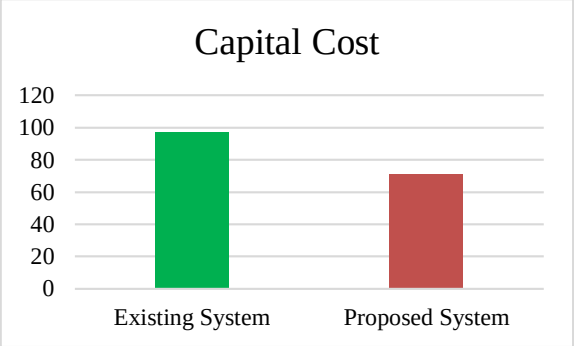

Fig. 11: Capital size comparison between proposed and Existing System (CSP)

Authentication Security: It tells about the level of security provided in the authentication. Models having high security in such have a wide application area. In this the information can be accessed by only those users whom we will provide the accessibility other users can't do. The proposed model provides higher authentication security than the existing model which is shown in fig. 12

Table 6 Comparison of Authentication Security

Systems	**Authentication Security**
Existing System (CSP)	62
Proposed System (ESPP)	98

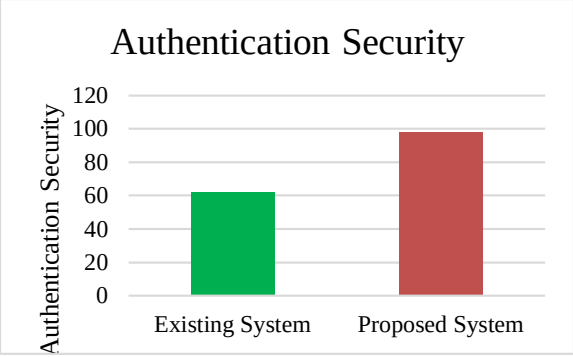

Fig. 12: Authentication security comparison between proposed and existing model

Authorization Security: It tells about the level of security provided in the authorization. Models having high security in such have a wide application area. The security is much more essential for the cloud ERP so design such model which provides more security to our information. Our proposed model of cloud ERP provide more security than the existing model and the comparison between them is shown through graph in fig. 13

Table 7 Comparison of Authorization Security

Systems	Authorization Security
Existing System (CSP)	40
Proposed System (ESPP)	99

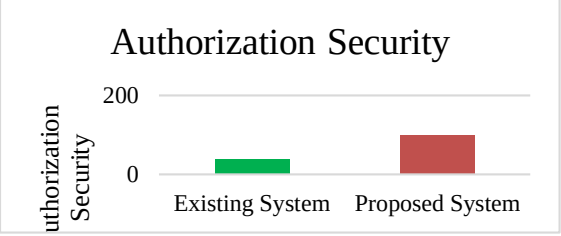

Fig. 13: Authorization Security comparison between proposed and existing model

Communication Security: It is the level of security provided in the communication. Models having high security in such have a wide application area. This evaluation metric focus on to provide the security to communication network to prevent the information from theft. Our proposed model provides higher communication security than the exiting model and it is shown in fig. 14.

Table 8 Comparison of Communication Security

Systems	Communication Security
Existing System (CSP)	20
Proposed System (ESPP)	80

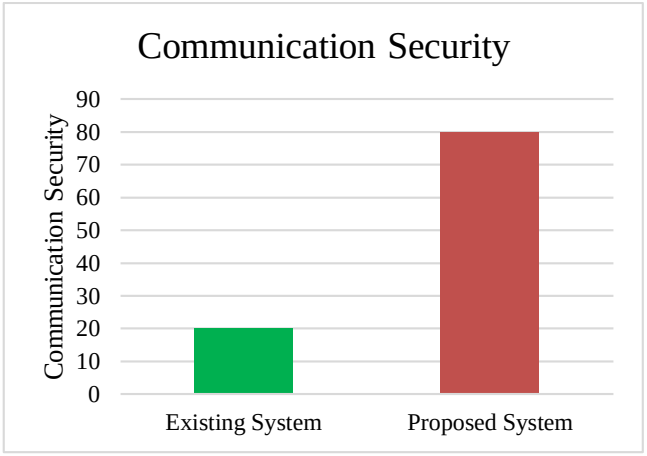

Fig. 14: Communication Security comparison between proposed and existing model

Integration Issues: It tells about the issues model going to face while integration on its own as well as to external application if required. Model having large issues don't have good efficiency. We perform the comparative analysis of proposed and exiting model for this evaluation metrics and it is found that the existing model has very high integration issue than the

proposed model. The comparative analysis of this metric is shown in fig. 15.

Table 9 Comparison of Integration issue

Systems	Integration Issue
Existing System (CSP)	20
Proposed System (ESPP)	80

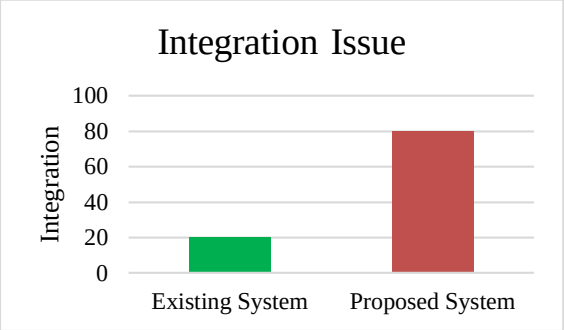

Fig. 15: Integration issue comparison between proposed and existing model

Operational Support: This evaluation metrics describe about the operational parameter of any model or tells about the process count in the same. For this metrics our proposed model is compared with the existing model and found that our model is much better than the existing and it is shown in fig. 16.

Table 10 Comparison of Operational support

Systems	Operational Support
Existing System (CSP)	40
Proposed System (ESPP)	98

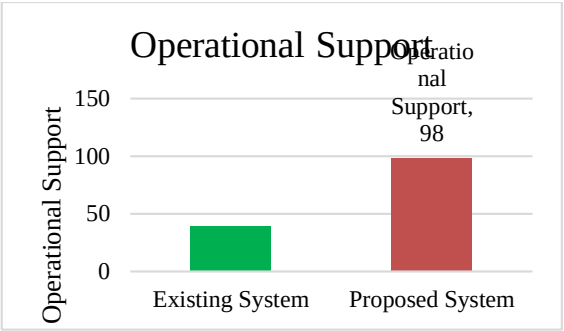

Fig. 16: Operational Support comparison between proposed and existing model

Maturity of Cloud: It tells about the specifications of cloud with respect of the development as opting the environment. High the maturity is, more the efficiency will be. The comparative analysis of this proposed model is done with the existing model and analyzed that our model is much more effective than the existing model and the analysis is shown in fig. 17

Table 11 Comparison of Maturity of cloud

Systems	Maturity of cloud
Existing System (CSP)	20
Proposed System (ESPP)	95

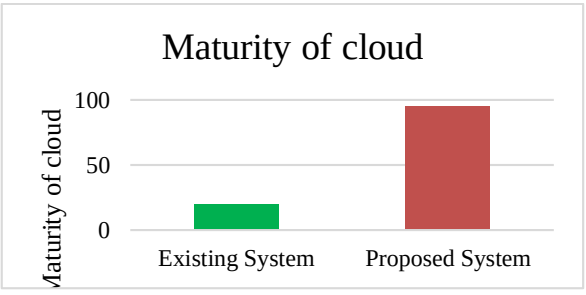

Fig. 17: Maturity of Cloud comparison between proposed and existing model

Service Availability: It tells about the system working with others about the availability of the system. Our proposed model provides much more availability of resource and services than the existing

model and the analysis of it shown through fig. 18.

Table 12 Comparison of Service Availability

Systems	Service Availability
Existing System (CSP)	40
Proposed System (ESPP)	92

Fig. 18: Service availability comparison between proposed and existing model

Adaptability of System: Tells about the capability of a system to adapt the changes. Our proposed model having high adaptabilities system than the Existing System (CSP) which is shown in fig. 19.

Table 13 Comparison of Adaptability of System

Systems	Adaptability of System
Existing System (CSP)	40
Proposed System (ESPP)	92

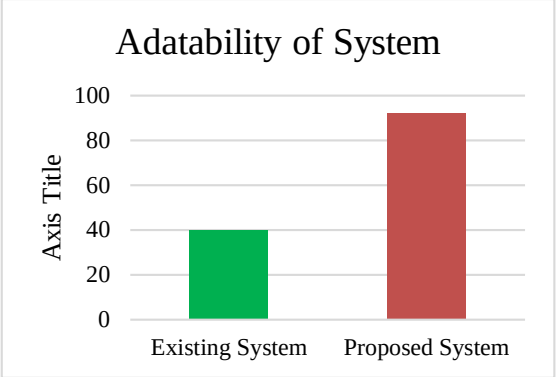

Fig.19: Adaptability of System comparison between proposed and existing model

Failure Tolerance: It tells about the capabilities of the system to handle the fault as per desires. Our models having a high fault tolerance carries a good efficiency in practical applications than the Existing System (CSP) and their comparison is shown through graph in fig. 20

Table 14 Comparison of Fault Tolerance

Systems	Fault Tolerance
Existing System (CSP)	40
Proposed System (ESPP)	92

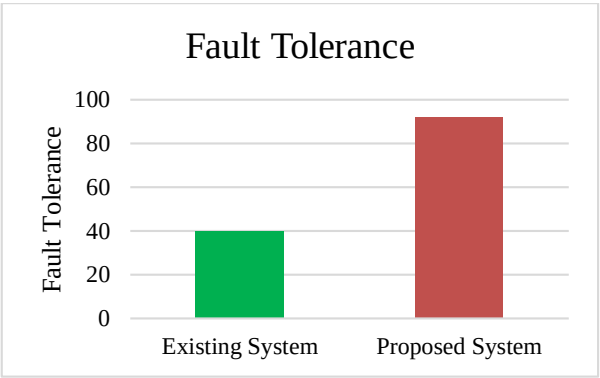

Fig. 20: Fault Tolerance comparison between proposed and existing model

5. CONCLUSION & FUTURE SCOPE

Applications of cloud ERP have been in high demand from businesses coping with business issues. It is a mellow deployment methodology that can give you a better chance to profit from an ERP speculative opportunity that promotes standardisation through observable economic factors and gives you the chance to better concentrate on planned operations. Realistic expectations must coexist with enthusiasm for cloud-based ERP. Due to the fact that both ERP and cloud computing have numerous benefits and few drawbacks, their implementation has helped many businesses tackle a variety of issues too However, when two good things are combined, they become even better over time, as was discussed above. For example, ERP enables businesses to manage information from all areas of their operations, including manufacturing, marketing, and sales, inventory management, shipping, and payment, as well as product planning, cost, and development, while Cloud Computing offers flexibility. ERP hosted on the cloud by cloud service providers is all that cloud ERP is. For small and medium-sized businesses, cloud ERP is a flexible and cost-effective option that offers significant benefits for growth and expansion. However, because of the flexibility of the cloud, security and privacy are now more important than ever, and many models and architecture have been created for this purpose. In this dissertation, we also design a secure efficient and privacy-preserving (SEPP) model that uses components for sharing encrypted data and data flow, validation, authorization, authentication, and user verification to increase the security level of our proposed model.

The suggested ESPP model verifies the physical address, but here, only the first time the requested resources or services are used will the user's identity be verified. This is the final phase to fulfil the request if any user successfully completes the first three steps. This SEPP architecture that has been presented also encrypts data before it is shared, adding to the security of our cloud-based ERP system. Overall, our suggested SEPP paradigm gives our ERP system significantly more security and privacy than the current one, according to our analysis. Our cloud ERP system is more secure and effectively protected from prying eyes thanks to the proposed SEPP concept. This model's complexity was discovered during development, despite the fact that it offers greater security and privacy. Therefore, the proposed model will be used in real-time applications in further work, and the architecture's design must be less complicated.

REFERENCE

[1] W. Voorsluys, J. Broberg, & R. Buyya, (2011), “Introduction to cloud computing”, Cloud computing: Principles and paradigms, 2-44.

[2] Dheresh Soni, Atish Mishra, Satyendra Singh Thakur, Nishant Chaurasia," Applying Frequent Pattern Mining in Cloud Computing Environment ", 2011, International Journal of Advanced Computer Research (IJACR), Volume-1, Issue-2, December-2011, pp.84-88.

[3] Kuldeep Mishra, Ravi Rai Chaudhary, Dheresh Soni, A PREMEDITATED CDM ALGORITHM IN CLOUD COMPUTING ENVIRONMENT FOR FPM, 2013, International Journal of Computer Engineering and Technology (IJCET), 2013, 4(4), PP213-223.

[4] L. Bangfan, Z. Huihui, & W. Meng, (2014), “How to Design the Cloud Computing Used in Egovernment’s Information Security?”, Applied Mechanics and Materials, Vol. 536-537, pp616-619.

[5] E. Fathi Kiadehi, & S. Mohammadi, (2012), "Cloud ERP: Implementation of Enterprise Resource Planning Using Cloud Computing Technology", Journal of Basic and Applied Scientific Research, Vol. 6.

[6] P.S. Petra Schubert, & A.F. Femi Adisa, (2011), "Cloud Computing for Standard ERP Systems: Reference Framework and Research Agenda", Arbeitsberichte aus dem Fachbereich Informatik, Vol. 4, No. 27, pp29.

[7] L. Bangfan, Z. Huihui, & W. Meng, (2014), "How to Design the Cloud Computing Used in Egovernment's Information Security?", Applied Mechanics and Materials, Vol. 536-537, pp616-619.

[8] Chen Guang-hui, Li Chun-qing, and Sai Yun-xiu, "Critical Success Factors for ERP Life Cycle Implementation", in International Federation for Information Processing, Volume 205, Research and Practical Issues of Enterprise Information Systems, eds. Tjoa, A.M., Xu, L., Chaudhry, S., (Boston:Springer), pp.553-562.

[9] Anukriti Singh, Shruti Nagpal "Implementation Of ERP In Cloud Computing", International Journal Of Scientific & Technology Research Volume 3, Issue 10, October 2014 ISSN 2277-8616.

[10] D. Soni, V. Sharma and D. Srivastava, "Optimization of security issues in adoption of cloud ecosystem," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1-5, : 10.1109/IoT-SIU.2019.8777670.

[11] Reetu Gupta , Priyesh Kanungo, Nirmal Dagdee , Golla Madhu , Kshira Sagar Sahoo , N. Z. Jhanjhi , Mehedi Masud , Nabil Sharaf Almalki and Mohammed A. AlZain, "Secured and Privacy-Preserving Multi-Authority Access Control System for Cloud-Based Healthcare Data Sharing", Sensors 2023, 23, 2617. https://doi.org/10.3390/s23052617.

[12] Gayathri S and Gowri S, "Securing medical image privacy in cloud using deep learning network", Journal of Cloud Computing (2023) 12:40.Y. Xu, N. Rahmati, & V. Lee, (2008, June), "A review of literature on Enterprise Resource Planning systems", In Service Systems and Service Management, 2008 International Conference on (pp1-6). IEEE.

[13] Soumya Ray, Kamta Nath Mishra, Sandip Dutta, "Sensitive Data Identification and Security Assurance in Cloud and IoT based Networks", I. J. Computer Network and Information Security, 2022, 5, 11-27.

[14] Al-Amri, Bayan & AlZain, Mohammed & Al-Amri, Jehad & Baz, Mohammed & Masud, Mehedi. (2020). A Comprehensive Study of Privacy Preserving Techniques in Cloud Computing Environment. Advances in Science, Technology and Engineering Systems Journal. 5. 419-424. 10.25046/aj050254.

[15] Hadidi, Saleh & Hadidi, Mamoun. (2020). ERP Security Based on Web Services. Global Journal of Computer Science and Technology. 20. 4.

[16] D. Soni and M. Kumar, "Secure data communication in client-cloud environment: A survey," 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), 2017, pp. 246-252, : 10.1109/CSNT.2017.8418546.J. Umble, R. Ronald, M. Haft, & U. Michael, (2003), "Enterprise resource planning: Implementation procedures and critical success factors", European Journal of Operational Research, Vol. 146, pp241– 257.

[17] Dheresh Soni, Atish Mishra, and Hitesh Gupta, "An Efficient Cloud

Data Mining (CDM) Algorithm for Frequent Pattern Mining in Cloud Computing Environment," 2016, Lecture Notes on Software Engineering vol. 4, no. 3, pp. 234-237, 2016.

[18] B Nareshkumar, Mr. G. Ananthanath, " Secure and Efficient Privacy Preserving Provable Data Possession in Cloud Storage," 2019, International Journal for Scientific Research and Development, ID: IJSRDV7I10600, Volume : 7, Issue : 1, 01/04/2019 Page(s): 857-861.

[19] Devaraju S, Ramakrishnan S, D. Soni "Association Rule-Mining-Based Intrusion Detection System with Entropy-Based Feature Selection: Intrusion Detection System (Chapter 1)", Handbook of Research on Intelligent Data Processing and Information Security Systems, IGI Global, DOI: 10.4018/978-1-7998-1290-6, pp. 1-24, Pages: 24, ISBN: 9781799812906.

[20] D. Soni, V. Tiwari, B. Kaur and M. Kumar, "Cloud computing security analysis based on RC6, AES and RSA algorithms in user-cloud environment," 2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT), Meerut, India, 2021, pp. 269-273, doi: 10.1109/ICACFCT53978.2021.9837360.

[21] Dheresh Soni, and M. Kumar "An Automated Cloud Security Framework Based on FCM in User-Cloud Environment." International Journal of Engineering and Advanced Technology 8 (6). Blue Eyes Intelligence Engineering and Sciences Publication: 3235–40. 2019, doi:10.35940/ijeat.F8831.088619.

[22] Kulwinder Kaur and Brahmaleen Sidhu, "A Review of Searchable Encryptions Over Cloud Data Sources", International Journal of Research in Electronics and Computer Engineering (IJRECE), VOL. 6 ISSUE 4, OCTOBER-DECEMBER 2018, ISSN: 2393-9028 (PRINT), 2348-2281 (ONLINE).

[23] Dheresh Soni, Deepak Srivastava, Ashutosh Bhatt, Ambika Aggarwal, Sunil Kumar, Mohd Asif Shah, "An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol", Mathematical Problems in Engineering, vol. 2022, Article ID 4696649, 14 pages, 2022. Hindawi. https://doi.org/10.1155/2022/4696649.