iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44485

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Digitalised Information Security in Data Communication in Organizational Flow

Maneesh Choppara[1], Dr. Aruna Varanasi[2], Jai Minocha[3], K. Hima Sameera[4]
[1, 3, 4]*Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Hyderabad (T.S), India*
[2]*Professor & HOD of CSE, Sreenidhi Institute of Science and Technology, Hyderabad (T.S), India*

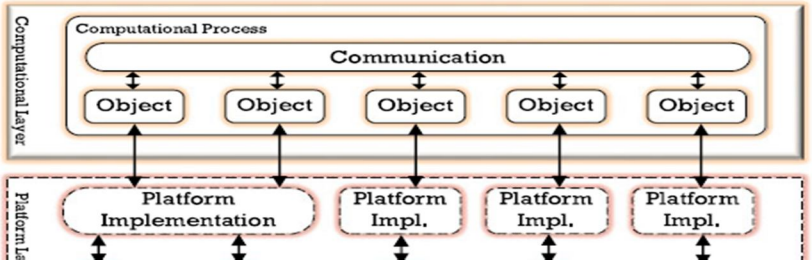
Abstract: ***Understanding what cyber security is and how to successfully apply it in today's culture, which is driven by technology and network connections, is vital. Systems, essential information, data, and other important virtual goods are at risk if there is no security to protect them. Every business, whether it is an IT firm or not, requires equal protection. Similarly, attackers do not lag behind in terms of developing new cyber security technology. They've upgraded their hacking techniques and are concentrating on the weak places of several businesses. Cyber security is vital because military, political, financial, medical, and corporate entities gather, practise, and store large amounts of data on PCs and other devices. Financial data, intellectual property, personal information, and other sorts of data that could be harmed by unauthorised access or acquaintance can make up a major amount of the data.***

I. INTRODUCTION

In today's business world, forming an alliance with suitable business partners is a popular strategy for a company to stay competitive by offering a wider range of products and services to its customers. Businesses are increasingly outsourcing portions of their company processes to third-party service providers, thanks to the advent of service-oriented computing, notably cloud computing. As a result, inter-organizational conceptual process management systems such as ERP, SCM, and Cross Flow are critical for dynamically and timely execution of business processes across corporate partners or outsourcers. An inter-organizational conceptual process management system, in a nutshell, is used to describe and regulate the execution of both manual and automated business processes. It can be managed either centrally or decentrally. Scalability and the varied and autonomous character of inter-organizational links are two reasons why the latter is often selected. A single conceptual process management engine is responsible for delivering tasks to the relevant execution agents in a centralised conceptual process system. Task dependencies are also satisfied by the core conceptual process engine, which only sends tasks to the relevant agents when all critical conditions are met. A central conceptual process engine, on the other hand, in a decentralised conceptual process system, only delivers the first execution agent the full conceptual process and receives the final output from the last agent in the conceptual process. In this case, the control of the conceptual process is localised, meaning that each agent in the process is responsible for not only executing a specific task, but also evaluating upcoming task dependencies and passing the remaining conceptual process to the next agent. From now on, we'll solely look at decentralised, inter-organizational conceptual process systems.

The purpose of the project is to develop a high-performance advanced computing layer for use in the broking system. An unique strategy was used on both the source and destination sides. The project's feasibility is evaluated in this phase, and a business proposal is presented, along with a very basic project design and some cost estimates. During the system analysis, a feasibility evaluation of the proposed system will be conducted. This is to ensure that the planned system will not cause any issues for the organisation. For feasibility study, a basic grasp of the system's primary requirements is required.

1) ECONOMICAL FEASIBILITY
2) TECHNICAL FEASIBILITY
3) SOCIAL FEASIBILITY are three major aspects in the feasibility analysis.



II. FEASIBILITY FROM AN ECONOMICAL POINT OF VIEW

This study is being conducted to analyse the system's financial impact on the company. The amount of money the company can spend on research and development for the system is limited. It is vital to provide justification for the expenditure. As a result, the designed system was completed on time and on budget, thanks to the fact that the majority of the technologies used were freely available. The customised products were the only ones that needed to be acquired.

III. FEASIBILITY FROM A TECHNICAL POINT OF VIEW

This study is being conducted to establish the technological viability, or technical needs, of the system. Any system developed should not exert a significant strain on the existing technical resources. As a result, the available technical resources will be in high demand. As a result, the client will be put under a lot of pressure. The developed system must have a minimal requirement since very minor or no adjustments are required to implement this system.

IV. FEASIBILITY IN SOCIAL SETTINGS

The purpose of the study is to determine the user's level of acceptance of the system. This refers to the practise of instructing a user on how to use technology successfully. Instead of being fearful of the system, the user should accept it as a necessity. The approaches utilised to educate and familiarise users with the system are entirely accountable for the consumers' level of acceptance. Because he is the system's final user, his self-esteem must be reinforced so that he may offer constructive criticism, which is encouraged.

A. Proposed System

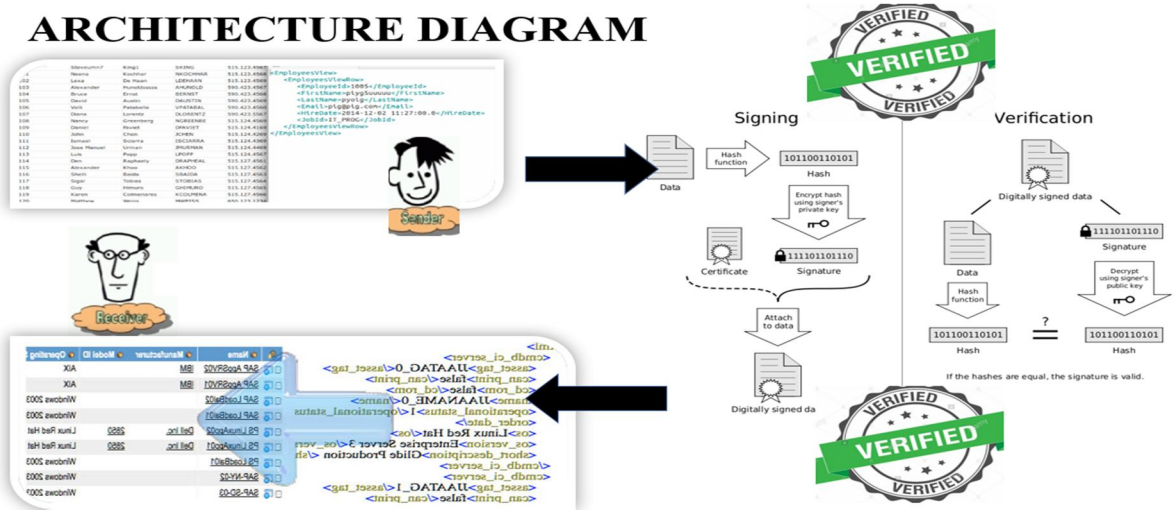
1) Creating a clear hierarchy in validating the data in each business process flow is the core extract of the project. Various steps involved in our proposed system,

2) A business rules for a clear automation process flow needs to be defined to identify/segregate the source and destination points. In addition, the process involves AND Joins(Process done in parallel to get the exact outcome), OR Join(Either one of the process needs to be done), XOR joins (Finalizing the deciding point)

3) This project involves the encrypting the data and amend them as XML formats which provides high end fast processing and running system. It involves the “World First” anti tampering XML protection mechanism implementation is done.

4) In the high-tech sector, more XML node updates and automatic calculation were applied with ontology flavours.

5) The multi-key option of signing the message will be introduced into the business flow based on the level of hierarchy. This project is a perfect fit for task-based authorisation control, in which task-based cryptographic keys are generated and issued as needed.



B. Advantages

1) It ensures transparency of certain business characteristics and control of specific aspects of business operations.

2) Typically, risk assessment and IT control frameworks are used to support the controls. These controls are then implemented in order to ensure that business processes are compliant with the relevant regulations and laws.

3) Anti-tampering XML implementation provides a high-end support on "Touch me Die Concept"

V. IMPLEMENTATION

The project's implementation stage is when the theoretical design is translated into a workable system.

Avoiding the publication of sensitive information by suppressing all sensitive data in a table as well as a predetermined number of other table entries, a process known as complimentary suppression.

The goal is to replace each table entry xi with an appropriate interval

[xi z I xi + z+ I

The extreme values of each interval must then be computed in order to provide the appropriate security for the sensitive entries while minimising the overall data loss.

The configuration information for the server is hidden from users and outsiders using this method. The owner's data is encrypted using Triple DES encryptionThe owner digitally certifies the data, which is in XML format, before sending it to a third party (data updater).

In this module, an XML verification token will be used by the third party (data updater) to verify the encrypted data.

If the XML is correct, the updater will make changes to the owner's data.

The data owner received data from the Updater. First, the Data Owner eliminates any new values given by the updater. Data.

That data must be decrypted by the owner. If the information is correct, corresponds to the original Xml data. The Owner makes changes to the values sent by the user.

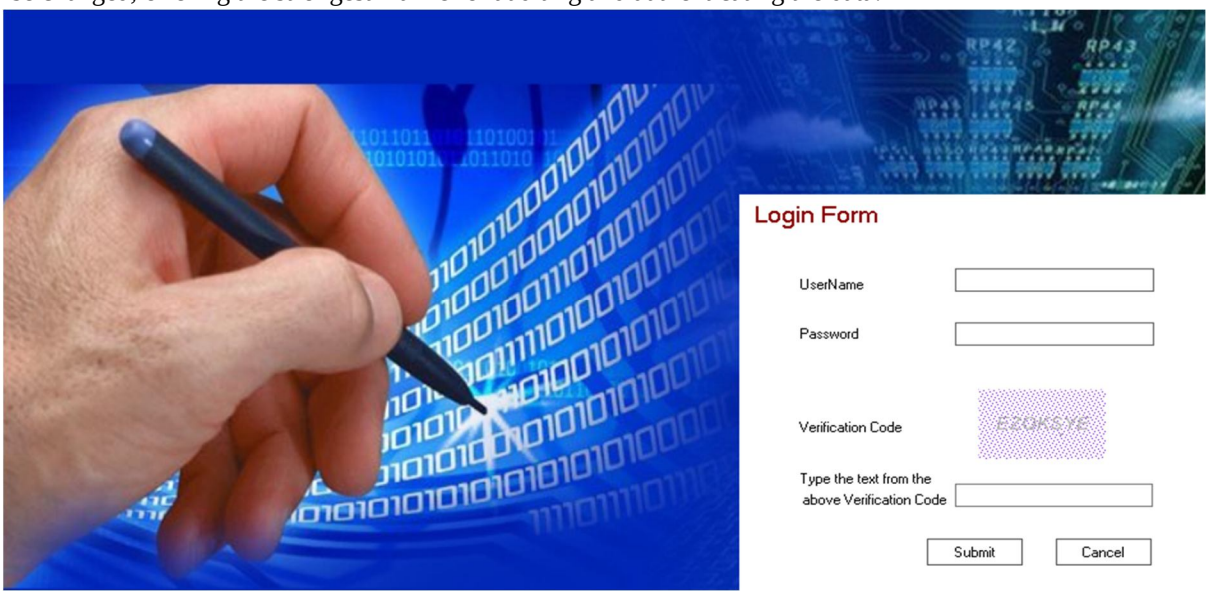
Updater-The Owner makes changes to the values sent by the user.

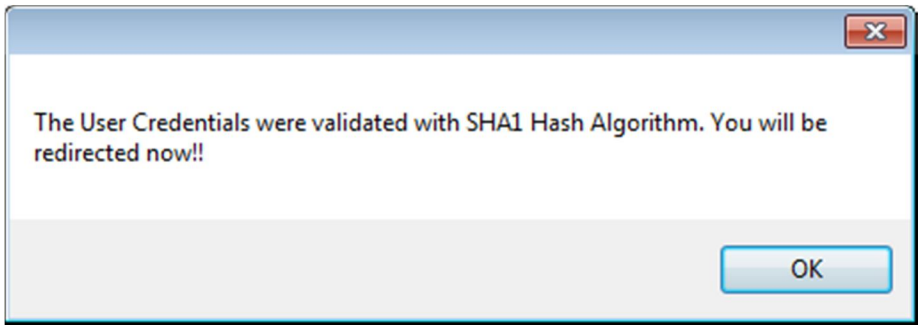
The original data will be preserved. As a result of a background check as well as many layers of authentication.

As a result, the Data Owner is modified, a comparative security analysis Relationship between the IDS from a different point of view, taken under consideration Reports a list of the security advantages and disadvantages, possible improvements in performance in the suggested system is depicted graphically.

After retrieving the message's verification token and several system characteristics from the Signing Authority (fixed and published by the PKG). This message will be sent to the intended recipient, who will compare the verification token to the basic identifier and system parameters that the target individual is familiar with.

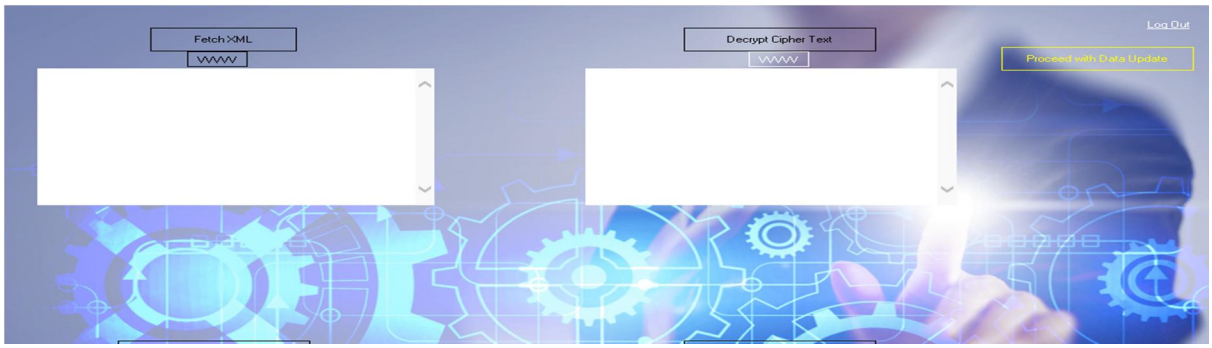
The Identity Based Verification Token (IBS) system comprises four phases: setting up the master keys, extracting the private key from the master keys, signing the message with the obtained verification token, and confirming the verification token in the destination. A set of work flows are in charge of everything. With many approvals in the multilevel work flow, the verification token will be changed, offering the strongest manner of auditing and authenticating the data.




The User Credentials were validated with SHA1 Hash Algorithm. You will be redirected now!!
OK

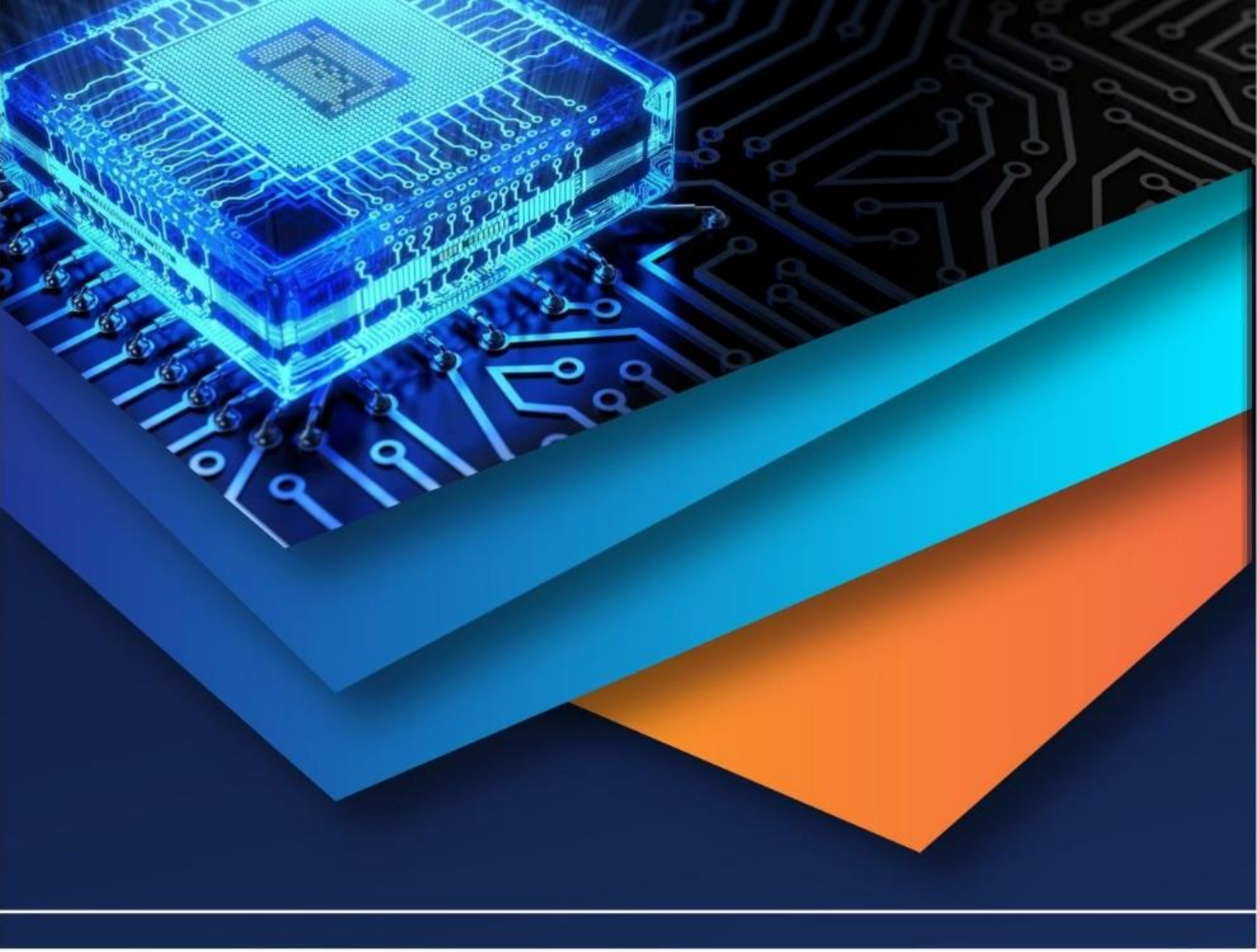

Refresh Data
Log Out
Amend Data
E-signature
Encrypt to Transfer Data ==>>


Validate XML ==>>
SCANNING..
57%
Amend Data into XML for Updates


Fetch XML
Decrypt Cipher Text
Log Out
Proceed with Data Update

REFERENCES

[1] W. Bartschat, J. Burrington-Brown, S. Carey, J. Chen, S.Deming, and S. Durkin, "Surveying the RHIO landscape: A description of current {RHIO} models, with a focus on patient identification," J. AHIMA, vol. 77, pp. 64A–64D, Jan. 2006.
[2] A. P. Sheth and J. A. Larson, "Federated database systems for managing distributed, heterogeneous, and autonomous databases," ACM Comput. Surveys (CSUR), vol. 22, no. 3, pp. 183–236, 1990.
[3] L. M.Haas, E. T. Lin, andM.A. Roth, "Data integration through database federation," IBM Syst. J., vol. 41, no. 4, pp. 578–596, 2002.
[4] X. Zhang, J. Liu, B. Li, and T.-S. P. Yum, "CoolStreaming/DONet: A data-driven overlay network for efficient live media streaming," in Proc. IEEE INFOCOM,Miami, FL, USA, 2005, vol. 3, pp. 2102–2111.
[5] A. C. Snoeren, K. Conley, and D. K. Gifford, "Mesh-based content routing using XML," in Proc. SOSP, 2001, pp. 160–173.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY