DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

Enhancing data security in SAP-enabled healthcare systems with cryptography and digital signatures using blockchain technology

Sonali Shwetapadma Rath[1]*, Prabhudev Jagadeesh M P[2]
[1*,2] Department of Computer Science & Engineering
JSS Academy of Technical Education
Bengaluru, Visvesveraya Technological University, Belagavi-590018
JSSATE-B Campus, Dr Vishnuvardhan Road,
Uttarahalli-Kengeri Main Road, Srinivaspura-Post, Bengaluru-560060
*Corresponding author email: 29sonali@gmail.com
(Received 20 September 2023; Final version received 18 January 2024; Accepted 19 January 2024)

Abstract

As the healthcare industry adopts more digital technologies, guaranteeing the security and privacy of sensitive patient data becomes increasingly important. Traditional centralized authentication solutions leave cyber threats and unauthorized access vulnerable. In response, the research demonstrates a novel strategy to improving data security and authentication in a SAP-enabled healthcare system by leveraging encryption and blockchain technologies. The research paper discusses the development and integration of a blockchain-based decentralized identity management system within the SAP platform. Each healthcare entity, including patients, doctors, and administrators, is given a distinct digital identity that is protected by using base 64 activity through DocuSign protects in SAP platform. The benefits of the proposed solution are assessed using a complete security analysis that measures data confidentiality, integrity, and availability. A comparison of DocuSign and SignEasy reveals DocuSign's superior performance in timestamp accuracy and document delivery speed. Its precision and reliability ensure document verification accuracy, while its streamlined workflow and advanced infrastructure expedite document processing, making it an ideal choice for businesses.

Keywords: SAP *platform*, Digital signature, Block chain technology, Security, Healthcare system, cyberattacks.

1. Introduction

The healthcare business has seen a significant digital revolution in recent years, embracing cloud-based solutions and electronic health records for effectively handling patient data. As more healthcare organizations embrace SAP (Systems, Applications, and Products) platforms for complete data integration and real-time analytics (Kessler et al., 2019) protecting the security and privacy of sensitive patient information has become a top priority. While technology improvements provide several benefits, they also present new concerns in protecting healthcare data from potential cyber threats and unauthorized access, given the data's ever-increasing value (Spanakis et al.,2020).

Traditional centralized authentication techniques have been criticized for being vulnerable to security breaches, which can jeopardize data integrity and accountability. Blockchain technology serves as the foundation for addressing these difficulties, acting as a distributed ledger with immutable features capable of securely storing authenticated actions and medical records. This technology improves data integrity by leveraging cryptographic hashing and decentralized validation, dramatically lowering the danger of unauthorized edits or data breaches. Additionally, the use of smart contracts streamlines established procedures, increasing efficiency and transparency within the healthcare ecosystem (Al et al.,2020).

The SAP Cloud Foundry platform, which is known for its scalability and efficient cloud-based services (Figueiredo 2022), is a suitable setting for integrating advanced security measures. It functions as an immutable and transparent ledger, recording each validated action and healthcare transaction utilising block chain's distributed ledger capabilities (Treiblmaier et al.,2020, Faccia et al., 2021). Due to the decentralized nature of the blockchain network, it eliminates single points of

DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

failure, protecting the healthcare system against hacker attacks and unauthorized data breaches. The use of cryptographic algorithms and smart contracts strengthens data integrity even further, prohibiting unauthorized access and malicious adjustments. Fig.1 illustrates the growing value of healthcare.

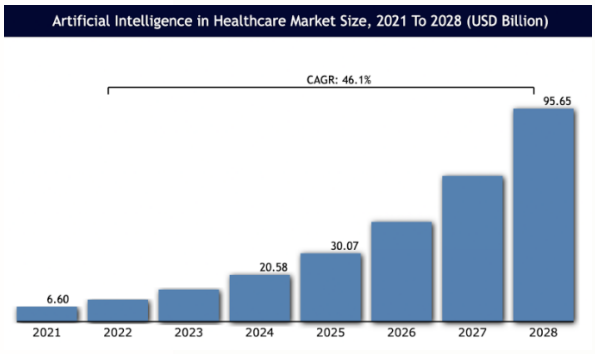

Fig.1. Growing value of healthcare data (https://resources.freeagentcrm.com/healthcare-industry-trends-and-statistics/)

The research highlights the importance of key management, legal compliance, and scalability in enhancing the security of healthcare systems. Key management is crucial in safeguarding patient privacy and maintaining health records. Legal compliance is essential in the healthcare sector, as it adheres to stringent data protection laws like HIPAA. Balancing security and compliance is a complex task, and healthcare institutions must be aware of their legal obligations while enhancing security measures. Scalability is crucial for healthcare systems dealing with vast amounts of data and serving a large number of patients. Scalability challenges can arise in hardware, software, network infrastructure, and security policy management across a larger system. To address these challenges, it is essential to invest in robust security solutions tailored to the healthcare sector's unique needs, such as advanced encryption techniques, secure access controls, and intrusion detection systems. Additionally, staying updated with evolving legal requirements and implementing compliance measures is vital. We also suggest integrating improved cryptographic authentication with the SAP Cloud Foundry backend, a cloud-based platform renowned for its scalability, flexibility, and ability to integrate seamlessly. This organization intends to create a dependable and expandable infrastructure for healthcare data access and storage while abiding by rules and regulations specific to the sector. In this research, we propose a novel method to strengthen healthcare data security by introducing encryption, employing Base64 activity through DocuSign for authentication, connecting it with blockchain technology, and doing so within the SAP Cloud Foundry backend. The primary contribution of this research can be summarised as follows:

One of the key contributions of this study is the development and integration of a blockchain-based decentralized identity management system for a healthcare system within the SAP platform. This decentralized method of identity management can improve security and privacy by minimizing reliance on a central authority for authentication.

The study recommends using encryption and blockchain technology to improve data security in healthcare systems by ensuring secrecy and transparency in data access and transactions.

The proposed blockchain-based solution's security, concentrating on data confidentiality, integrity, and availability, demonstrates its usefulness in assuring patient data protection.

According to the findings, blockchain-based solutions are more immune to cyberattacks and data breaches than traditional centralized authentication systems, which is critical in the healthcare industry.

2. Literature survey

A thorough analysis of the EHR security and privacy literature discovered 26 legislations, 23 symmetric key methods, 13 pseudo anonymity approaches, 11 digital signature systems, and Role-Based Access Control (RBAC) models proposed by (Fernández-Alemán et. Al., 2013). According to the study, more work is needed to implement these regulations and build secure EHR systems. However, in order to distribute health-related data via these approaches, more security is needed.

This study describes a patient-centric authorization protocol for Health Information Exchange (HIE) systems that addresses the shortcomings of previous techniques. The system assures authentication and outperforms existing techniques by employing a trapdoor hash-based proxy signature scheme by (Chandrasekhar et.al 2017). Adding network components can improve data distribution and broadcasting. However, extra security and privacy risks are built into the system design,

which leaves some users unable to use these applications. Therefore, it is imperative to immediately suggest a mechanism for protecting the security of EHR data.

In order to use the cloud for electronic medical records, (Al Omar et al., 2019) have suggested certain national level frameworks. One of the challenges in fusing information from the Internet is protecting patient privacy.

In order to reconcile data processing capabilities with privacy concerns, a distributed dynamic authorization system based on blockchain is presented (Xu et.al 2022) for trustworthy data access. Patients' privacy information is not maintained on blockchain for greater data processing efficiency; instead, data access interfaces are provided via URLs in the authorization information.

This study describes a patient-centric authorization protocol for Health Information Exchange (HIE) systems that addresses the shortcomings of previous techniques. The system assures authentication and outperforms existing techniques by employing a trapdoor hash-based proxy signature scheme by (Roy et.al 2021).

The healthcare sector's resilience has been tested ever since the Covid-19 outbreak. Additionally, the sector was a prominent target of cyberattacks that worldwide disrupted important hospitals and health organizations. This explains why implementing suitable cyber security controls and making use of required technologies, such as the modern cloud, is essential.

(Kumar et. al.,2022) In the healthcare business, blockchain technology is critical for tackling data vulnerability and security. This study describes a secure blockchain mechanism for data management, with the goal of lowering overhead costs and speeding up ledger updates. The experimental results demonstrate a tenfold reduction in network traffic. However, storing a huge volume of data may result in inefficiencies and costlier issues in the proposed architecture.

Hospitals have personally identifiable information (PII) and personal health information (PHI), and when the PII or PHI data is stolen due to cyber-attacks, it puts patients' lives at risk and compromises the trust between doctors/providers and patient research by (He et. al.,2021) Cybersecurity challenges, risks, and plan to mitigate those risks are discussed. Risk assessment should be the first step in protecting sensitive PII and PHI data in the life sciences and healthcare industries. There are five phases of the NIST Cyber Security Framework, (NIST CSF). It begins with identifying or knowing what we need to defend (assets or data), followed by protecting, detecting, and then responding to any cyber-threats or incidents, and then concludes with recovering from them. We need to create policies, standards, and procedures for healthcare businesses with the aid of NIST CSF, and then deploy cutting-edge SAP S4Cloud products—which also leverage AI and their business technology platform (BTP) to enable Cyber domains—to protect their PHI/PII data. (SAP News 2021, SAP Help). The public, private, and hybrid cloud models offered by SAP S4/HANA allow you to select the model that will best serve your company needs and preserve your sensitive data. You can help develop your cyber security program based on the NIST CSF standard by implementing SAP S4/HANA.

3. Proposed methodology

Healthcare professionals today generate enormous amounts of medical-related data every day thanks to technology. The main repository for medical data in a hospital is called health records. Electronically generated clinical data is stored in health records. Data from health records is used for secondary purposes, such as medical trials, ongoing illness monitoring, and quality-improvement audits, in addition to the primary use of treating patients. When Health Records data are utilized for unrelated reasons without authorization—or, in certain cases, even with consent—privacy issues arise. The safety of individuals may be seriously jeopardized if sensitive personal information from health records is made available to or published to the public. Because of this and other problems with the present health records system, as demonstrated in Fig.2, data leaks and breaches constitute a major threat to any healthcare facility. Blockchain has the potential to make the entire facility secure depending on the specific permissions and conditions that the patient establishes. The data on a block chain is secured via cryptography. Each member of the network has a special private key that is associated with the transactions they execute and acts as a special digital signature. Any modifications to a record will be promptly detected by the peer network if the signature is changed, invalidating it.

DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

Fig.2. Issues in health record data storage

Additionally, recent research has discovered a searchable block chain that guarantee privacy preservation while enabling reliable search across encrypted distributed storage systems (Jiang et. Al.,2019). Another way for data security is to use smart contracts and verified computation (Avizheh et.al., 2019, Maddali et.al.,2020). The blockchain-based health records system may also include privacy-preserving homomorphic encryption methods [19,20]. However, as the volume of users and transactions grows, the block chain networks may experience scalability issues. As the network expands, the process of coming to an agreement and adding blocks to the chain may get slower, which could cause delays when handling a significant amount of health records. Additionally, keeping a lot of health records on the block chain may cause the chain's size to grow over time. This may increase the amount of storage needed and make it more difficult to maintain and replicate block chain data between nodes. Hence there is a need to develop a block chain-based decentralised identity management system within the SAP platform.

3.1. Proposed architecture

SAP Cloud Foundry provides a framework for the seamless integration of blockchain technology with existing healthcare systems and applications, allowing you to transition to a blockchain-based solution without disrupting the existing infrastructure. Also, the block chain incorporated with Base64 Activity via DocuSign to give an additional layer of data security in the healthcare industry. The term "Base64 Activity via DocuSign SAP" refers to a specific function or process within an organization that involves the use of Base64 encoding in conjunction with the DocuSign electronic signature platform and SAP (Systems, Applications, and Products in Data Processing), a widely used enterprise resource planning (ERP) software suite. This activity often involves the encoding and transfer of data in the Base64 format between SAP and DocuSign for a variety of applications such as document management, electronic signature workflows, and data interchange. Base64 encoding is a way of transforming binary data into a text-based format that is suited for secure transmission across different systems and platforms. It is frequently used when data, like as digital documents or photographs, must be securely transferred or processed between different applications or systems, as is frequently the case in an integrated environment such as SAP and DocuSign. Sensitive health information and user credentials are securely encoded and safeguarded by using Base64 Activity via DocuSign for cryptographic operations shown in Fig. 3. By using cryptographic techniques, this strategy maintains the confidentiality of the data and prevents unauthorized access by ensuring that only authorized users with valid digital signatures can access and interact with health records.

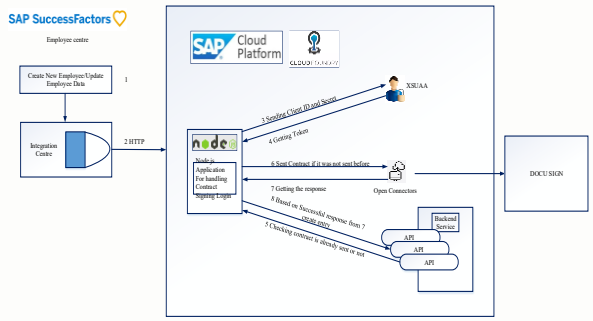

Fig.3. Proposed SAP cloud platform architecture with DocuSign

Using block chain authentication along with cryptographic digital signatures, it is possible to securely and transparently authenticate the validity of user actions and transactions. Every action is verified using the block chain, which serves as an auditable and transparent authentication mechanism, increasing accountability and promoting trust in the healthcare system. The architecture of the block chain technology illustrated in Fig 4.

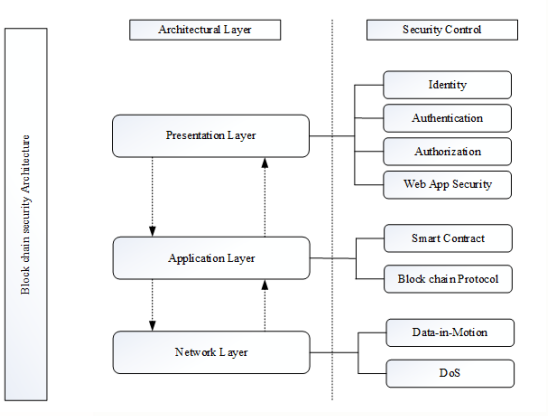

Fig.4. Block chain security architecture

The combination of blockchain technology with SAP Cloud Foundry improves the platform's ability to manage enormous volumes of health records while also ensuring the system's ability to adapt and scale as the healthcare ecosystem evolves. In conclusion, by combining Base64 Activity via DocuSign and Blockchain Technology in SAP Cloud Foundry Backend, the healthcare sector now has a strong, open, and safe method for safeguarding patient records and maintaining data integrity. This method tackles a variety of security and privacy issues, improves stakeholder confidence, and encourages effective and safe data sharing for better patient care.

Process flow

1. User enrolment and identity creation

- Within the SAP Cloud Foundry backend, users (such as patients, physicians, and administrators) register and build their digital identities.
- Each user receives a distinct public-private key pair from the backend. The user's device securely stores the user's private key, while the SAP backend stores the user's public key.

2. Base64 activity via Docusign

- The SAP Cloud Foundry backend creates a transaction hash encoding the action's contents when a user initiates an activity that needs authentication (such as viewing medical information or approving a prescription).
- The transaction hash is Base64 encoded by the backend, which transforms it into an ASCII representation.
- To serve as a cryptographic service provider, DocuSign receives the transaction hash in ASCII format.
- DocuSign uses its private key to perform extra cryptographic operations, like hashing and digital signing, to provide a special digital signature for the transaction hash.
- The digital signature is returned by DocuSign to the SAP Cloud Foundry backend.

3. Integration of Blockchain for Authentication

- The authorized activity is saved in a transaction block by the SAP Cloud Foundry backend along with its digital signature.
- The transaction block is sent by the backend to the blockchain network for consensus and confirmation.
- Using DocuSign's public key that is kept on the blockchain, the blockchain network verifies the legitimacy of the digital signature.
- By adding the transaction block to the blockchain after attaining consensus, all authenticated actions are recorded in an immutable and visible audit trail.

4. Using the Base64 activity through DocuSign, the user must create a fresh digital signature for each successive action.

5. The blockchain and user's public key that are both stored in the backend and SAP Cloud Foundry validate the digital signature.

6. After a successful verification, the user is permitted to carry out the authorized operation.

An immutable audit trail is produced on the blockchain by the recording of all verified actions. The blockchain can be accessed by healthcare managers and authorities to confirm the legitimacy of all actions and data flows. As a result, the blockchain technology combined with SAP Cloud Foundry's scalability and interoperability allow for smooth integration with current healthcare apps and systems.

3.2. Creation of oData service using CDS model

The simplest method to achieve this is by using SAP Cloud Foundry Backend Service, which retains data on all users who have already received contracts so that contracts won't be delivered again if changes are attempted to be triggered from the SFEC Integration Center. For storing user data and confirming whether or not a user has consented to a contract, it will build the oDATA service on-the-fly using the CDS architecture. Data models and annotations that specify the structure and behavior of the service you are creating must be

DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

defined in order to create an OData service using SAP's Core Data Services (CDS). oData is a standard protocol that makes it possible to build and use RESTful APIs for manipulating data.

Basic summary of the SAP CDS oData service creation process:

1. Begin by utilizing CDS to define the data model. Declaratively describing data structures, connections, and behavior is possible with CDS. Defining entities, properties, and relationships is possible.
2. Add OData-specific annotations to the CDS entities. The entities' oData service exposure will be determined by these annotations.
3. Create an oData service definition that outlines the entities and associations that will be made available.
4. Activate your CDS artifacts after defining your CDS model and service definition. This produces the runtime objects, information, and artifacts for the oData service.
5. Use the oData endpoint to access the service once it has been produced.

In order to provide specific functionality through oData endpoints, DocuSign's APIs must be integrated using Cloud Platform Integration (CPI) in order to create an oData service. DocuSign is a platform for managing and signing documents electronically.

3.3. Creation of oData service using CPI

Using Cloud Platform Integration (CPI), a component of SAP Cloud Integration, you can build, configure, and deploy integration flows that expose data as oData endpoints. DocuSign is a platform for electronic signatures and document management that helps businesses to digitize and automate their contract-creation procedures. For drafting, distributing, signing, and managing electronic contracts and documents, the DocuSign service provides a number of capabilities.

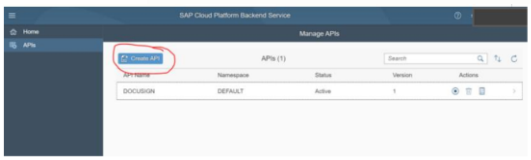

Fig.5. SAP cloud platform backend subscription with DocuSign API

Subscribing to and integrating the SAP Cloud Platform Backend service with the DocuSign API entails creating a connection between your SAP Cloud Platform environment and the DocuSign API to allow for easy data exchange as illustrated in Fig 5.

The process flow can be described below:

1. Create a new integration flow in SAP Cloud Platform Integration.
2. Configure the source endpoint to receive data from your application/system.
3. Configure the target endpoint to connect with the DocuSign API.
4. Obtain DocuSign API credentials (e.g., client ID, secret).
5. Configure the authentication mechanism in CPI to securely store and use these credentials.
6. Map the incoming data from your source system to the format expected by the DocuSign API request.
7. Use CPI's HTTP adapter to send a POST request to the appropriate DocuSign API endpoint.
8. Pass the mapped data as the request payload.
9. Receive the response from the DocuSign API.
10. Parse and process the response as needed.

Success factors Integration Centre and SAP Cloud Platform Integration provide suggestions on when to use each tool for interconnection creation. To create, test, and maintain incoming and outgoing integration, Success Factors features an integrated tool called Integration Centre. There are many other output file types available, including conversions from CSV to XML or JSON. The output can be safely stored on SFTP servers, and a number of scheduling options are available. Additionally, premade integration from the IntegrationCenter's catalog may be used and deployed on the customer instance.

DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

Algorithm: DocuSign Service

Initialize users as an empty collection.
Repeat until the user chooses to exit:
Prompt the user for an action (create, retrieve, update, delete, or exit).
If the action is "create":
Prompt the user to enter the userID and sent status.
Call the CreateUser function with the provided input.
If the action is "retrieve":
Prompt the user to enter the userID to retrieve.
Call the GetUser function with the provided userID and display the user details.
If the action is "update":
Prompt the user to enter the userID and new sent status.
Call the UpdateSentStatus function with the provided input.
If the action is "delete":
Prompt the user to enter the userID to delete.
Call the DeleteUser function with the provided userID.
If the action is "exit":
Exit the program.
End Algorithm

Developing an integration with the DocuSign API (Fig.6) entails a number of stages, including registering your application, acquiring authentication credentials, sending API requests, and dealing with answers.

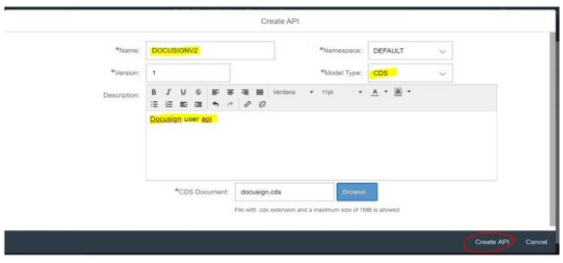

Fig.6. DocuSign API Creation

The credentials, which come with a Client ID and Secret Key, are sent after the API is created. The use of these credentials is for authentication.

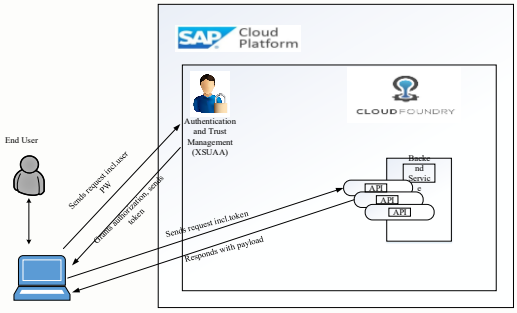

Fig.7. DocuSign API connection to Backend Service

The creation, deployment, and management of integration are all made possible by the SAP Cloud Platform Integration (CPI) solution for cloud middleware. Third-party programs and SAP OnPremise, SAP Cloud, or both may be connected in this manner. When linking SAP solutions to other SAP solutions and with other parties, it offers a broad range of connectivity options, including message translation, authentication, and even readymade integration options as shown in Fig 7. Successfactors is advised about solutions that range from modest to high level SAP Cloud Platform Integration. The Integration Center provides different scheduling options for the interfaces, such as once daily, once weekly, once monthly, and once yearly. Interfaces run more frequently, such as once every five minutes or once every day. CPI may be utilized in all of these situations. CPI also provides schedules with the "Run Once" option.

The overall process can be described below algorithm:

Import package like sap.gateway.ip.core.customdev.util.Message, ITApiFactory, securestore.SecureStoreService, securestore.UserCredential, usermodel.XSSFSheet, usermodel.XSSFWorkbook.
Define process data and SSFWorkbook (body)
//Extract Rows Data from Spreadsheet//
Set rowsData as an empty list.
Set headerCount to 0.
For each Row (row) in the sheet (mySheet):
Create a new empty list called rowData.
For each Cell (cell) in the row (row):
Append the value of the cell to the rowData list.
Append the rowData list to the rowsData list.
If headerCount is 0:
Set headerCount to the number of cells in the current row (row.getLastCellNum()).
End

DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

//Process rows Data and Generate Output//
If rowsData is not empty:
Sort the rowsData list in ascending order (based on default comparison).
For each row (rowData) in rowsData:
If headerCount is 0 (no headers):
Increment headerCount by 1 to mark that the headers have been processed.
Else (headers have been processed):
Append the elements of rowData joined by commas to the output string.
Append a new line character ("\n") to the output string.
End
//Set Client ID and Client Secret, Define Services, and Handle User Credentials//
Set DocuSign_MS by calling ITApiFactory.getApi() to retrieve the DocuSign Microservice instance.
If DocuSign_MS is null:
// DocuSign_MS is not initialized, meaning user credentials are required.
Prompt the user to input their client ID and client secret.
Set clientSecret by replacing "&" with "%26" to handle special characters.
Set the message property "clientId" with the value of clientId.
Set the message property "clientSecret" with the value of clientSecret.
Return the message object.
Else
// DocuSign_MS is already initialized, no need to handle user credentials.
Proceed with defining the services and any other necessary operations using DocuSign_MS.
End
//Process Data and Modify Message Body//
Find the occurrence of "@odata.context" in the body string.
Replace "@odata.context" with "odata.context" in the body string.
Find the occurrence of "@microsoft.graph.downloadUrl" in the body string.
Replace "@microsoft.graph.downloadUrl" with "microsoft.graph.downloadUrl" in the body string.
Set the body of the message object to the modified body string.
Return the message object.
End
//Split Download URL and Map Properties with Complete URL//
Split the completeUrl using the "?" character as the delimiter.
Store the second part (index 1) of the split result into the query variable.
Extract the base URL part from completeUrl by taking the substring from index 0 to the index of the "?" character.
Store the base URL into the url variable.
Set the "url" property of the message object with the value of the url variable.
Set the "query" property of the message object with the value of the query variable.
Return the message object.
End
//Format JSON and Get User Details//
Remove the opening and closing brackets from the JSON string by taking a substring from index 1 to body.size()-1.
Store the modified JSON string back into the body variable.
Replace the substring "Comment_Rank" with "Comment Rank" in the body.
Replace the substring "Signature_Rank" with "SignatureRank" in the body.
Replace the substring "Business_Unit" with "Business Unit" in the body.
Set the modified body as the new body of the message object using message.setBody(body.toString()).
Return the message object.
End

As a result, DocuSign is a comprehensive electronic signing an agreement platform with a variety of features, such as advanced document routing, templates, support for mobile apps, identity verification, analysis, and more. It is well-known for its many integrations and workflow automation features. DocuSign has an advantage when it comes to establishing trust with highly regulated industries because it has been in the market longer. It offers a well-designed, intuitive interface with several customization

DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

possibilities. It is made to accommodate businesses in a variety of sectors and sizes.

4. Analysis of experimental results & discussion

4.1. DocuSign to daily data synchronization

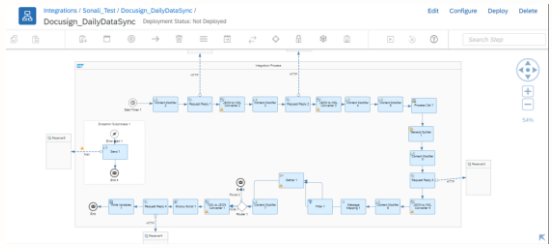

Fig.8. DocuSign daily data synchronization

Data extraction is the first step in the DocuSign Daily Data Sync process as shown in Fig 8, and it starts with obtaining pertinent data from internal sources or systems. Documents, recipients, signature statuses, templates, and other relevant elements could all be included in this data. Data Upload & Synchronisation involves accessing the proper API endpoints to upload the modified data to the DocuSign platform. This could require making envelopes, managing recipients, updating document statuses, and other things, depending on the data being synchronized. The name "Docusign_DailyDataSync" indicates daily synchronization; hence, the process should be set up to execute every day at a certain time. Your DocuSign data is kept current thanks to this.

4.2. DocuSign to envelope creation

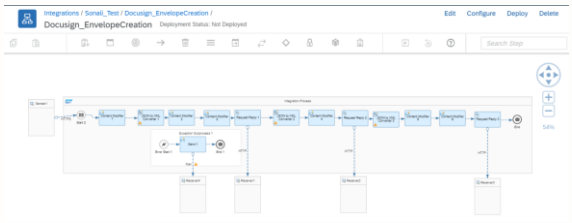

Fig.9. DocuSign to envelope creation

Fig 9 illustrates how the DocuSign Create Envelope constructs an envelope definition that outlines the desired creation of the envelope. The title of the email, email messages, receivers (signers, carbon copies, etc.), document location, tabs (signature, date, text fields), and any customized fields are all included in this. To connect the prepared documents to the envelope is to "add documents to envelope." Each document has a document ID assigned to it.

4.3. DocuSign to get envelope

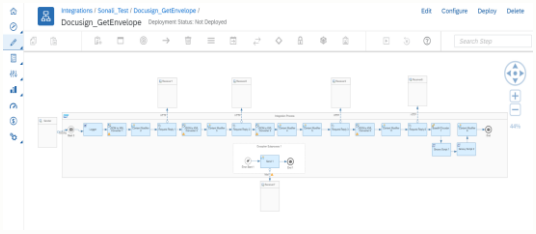

Fig.10. DocuSign to create envelope

4.4. DocuSign to event trigger

A specific envelope's status, recipients, documents, timestamps, and other pertinent data can be programmatically fetched using the "Docusign GetEnvelope" procedure, as is seen in Fig. 10. Tracking, reporting, auditing, and integration uses can all be made of this data. You can access the status and usage history of the envelope as well as the recipients' actions by utilizing the GetEnvelope API.

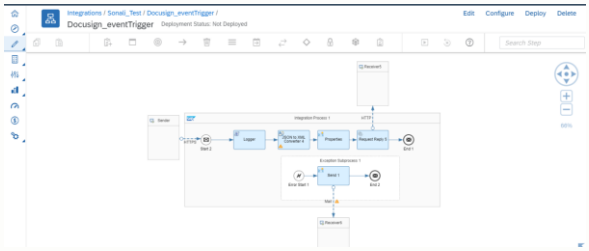

Fig.11. DocuSign to event trigger

The systems depicted in Fig 11 can be seamlessly and automatically integrated with the DocuSign platform through event triggers. They make sure the programme can react immediately to crucial occurrences inside the DocuSign workflow, optimising effectiveness and the user experience.

DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

4.5. Performance Parameters

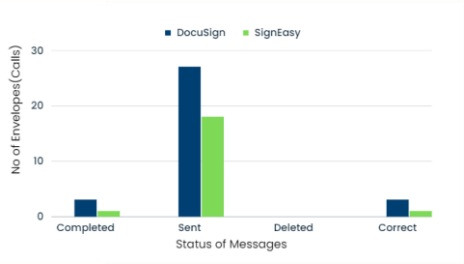

Fig.12. Envelope vs message

Fig 12 compares the number of envelopes with the status of messages, including completed, sent, deleted, and accurate messages. Strict security and compliance standards DocuSign may be chosen because of its reputation for strong security procedures, allowing it to manage a greater number of envelopes containing sensitive information. So it reveals that DocuSign has more envelopes than the SignEasy technique.

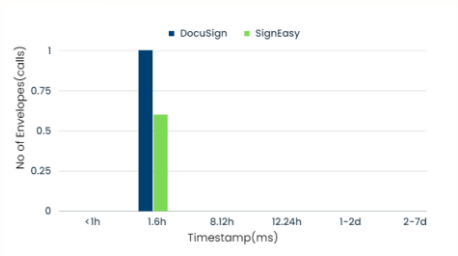

Fig.13. Envelope vs timestamp

Fig 13 compares the quantity of envelopes with the timestamp in terms of hours and days and DocuSign is well-known for its scalability, and it can manage a high amount of envelope transactions, making it ideal for enterprises that require a large number of signatures. As a result, DocuSign has more envelopes in the brief time stamp.

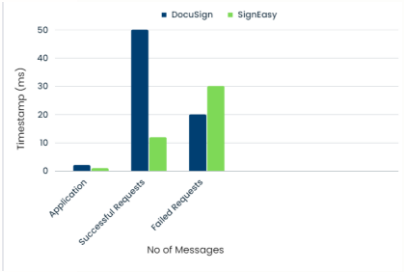

Fig.14. Timestamp vs messages

Fig 14 compares the number of messages processed in terms of application, successful requests, and unsuccessful requests with the timestamp in milliseconds. DocuSign receives more successful requests, including timestamping, implying that it has a strong and dependable infrastructure. This is especially important that rely on electronic signatures and document management to maintain constant efficiency and uptime. The figure indicates that DocuSign receives more successful requests than SignEasy. In comparison to SignEasy, DocuSign has less rejected requests.

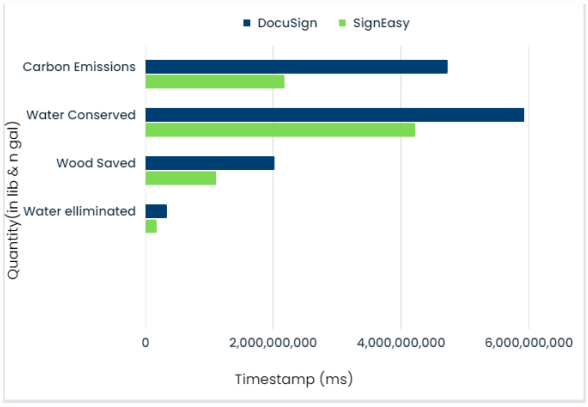

Fig. 15. DocuSign environmental impact

Fig 15 shows an analysis of the effects of DocuSign and SignEasy on the quantity assessed for carbon emissions, water conservation, wood preservation, and water elimination.

DocuSign outperforms SignEasy in terms of security, interaction with enterprise systems such as SAP, scalability, and global support. These benefits make it an appealing option for enterprises looking for a comprehensive electronic signature and document management solution, especially when dealing with high-security and high-volume document processing requirements.

4.6. Discussion

A user-friendly design and optimized e-signature functionalities are the main goals of this development. While providing the fundamental features of an electronic signature. DocuSign has an advantage in establishing trust with highly regulated businesses because of its longer history in the sector. Comparing other streamlined e-signature, the DocuSign has more regulations and trust. It offers comprehensive customer support and resources due to its larger user base.

DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

5. Conclusion

This research paper investigates the topic of data security in SAP-enabled healthcare systems and presents a plan for addressing challenges such as data breaches, unauthorised access, and manipulation by utilising sophisticated technologies such as blockchain, digital signatures, and cryptography. With strong encryption techniques, cryptography protects confidential patient information and fortifies sensitive data. Digital signatures give an additional layer of assurance to document accuracy, lowering the chance of unauthorised changes. The proposed approach uses blockchain technology to create an immutable and decentralised ledger. According to the empirical review, security risks and data breaches have been significantly reduced. Performance benchmarks show that cryptographic procedures and digital signature verification are carried out efficiently within the SAP system. However, difficulties remain, needing careful planning and collaboration among healthcare institutions, technological professionals, and regulatory bodies. To keep healthcare data safe and secure in the ever-changing context of digital security, adaptability is critical. Our study improves healthcare data security by addressing immediate security problems while also fostering efficient, safe, and patient-centric data management, ensuring important patient and provider data remains secure and accessible.

However, the study identifies limitations and problems in applying a framework in healthcare settings, requiring coordination among institutions, technology professionals, and regulatory bodies, as well as adaptation to the ever-changing cybersecurity landscape. The revolutionary potential of this work has the potential to have a long-term impact on healthcare systems, ultimately benefiting both patients and healthcare professionals. In the future, this study investigates the feasibility of integrating public and private blockchain networks in healthcare systems to improve data access control, privacy, transparency, and scalability.

Reference

Kessler, S., Hoff, J. & Freytag, J. C. (2019). SAP HANA goes private: from privacy research to privacy aware enterprise analytics. Proceedings of the VLDB Endowment, 12(12), 1998-2009.

Spanakis, E. G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M. & Magalini, S. (2020, July). Cyber-attacks and threats for healthcare–a multi-layer thread analysis. In 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC) IEEE, 5705-5708.

Al Asad, N., Elahi, M. T., Al Hasan, A. & Yousuf, M. A. (2020, November). Permission-based blockchain with proof of authority for secured healthcare data sharing. In 2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT), IEEE, 35-40.

Figueiredo, M. (2022). Developing Applications on SAP HANA Cloud. In SAP HANA Cloud in a Nutshell: Design, Develop, and Deploy Data Models using SAP HANA Cloud Berkeley, CA: Apress, 103-127.

Treiblmaier, H. & Sillaber, C. (2020). A case study of blockchain-induced digital transformation in the public sector. Blockchain and Distributed ledger technology use cases: Applications and lessons learned, 227-244.

Faccia, A. & Petratos, P. (2021). Blockchain, enterprise resource planning (ERP) and accounting information systems (AIS): Research on e-procurement and system integration. Applied Sciences, 11(15), 6792.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O. & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of biomedical informatics, 46(3), 541-562.

Chandrasekhar, S., Ibrahim, A. & Singhal, M. (2017). A novel access control protocol using proxy signatures for cloud-based health information exchange. Computers & security, 67, 73-88.

Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S. & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on block chain environment. Future generation computer systems, 95, 511-521.

Xu, B., Xu, L. D., Wang, Y. & Cai, H. (2022). A distributed dynamic authorisation method for Internet+ medical & healthcare data access based on consortium block chain. Enterprise Information Systems, 16(12), 1922757.

Roy, M. & Singh, M. (2021, April). Analytical Study of Block Chain Enabled Security Enhancement Methods for Healthcare Data. In IOP Conference Series: Materials Science and Engineering, IOP Publishing, 1131(1), 012002.

He, Y., Aliyu, A., Evans, M. & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. Journal of medical Internet research, 23(4), e21747.

Kumar, A., Singh, A. K., Ahmad, I., Kumar Singh, P., Anushree, Verma, P. K. & Tag-Eldin, E. (2022). A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. Sensors, 22(15), 5921.

SAP News, Enterprise Threat Detection Cloud [Online]. Available: https://news.sap.com/2021/07/sap-enterprise-threat-detection-cloudbased-managed-service/

SAP Help, Enterprise Threat Detection Cloud Edition [Online]. Available: https://help.sap.com/docs/SAP_ENTERPRISE_THREAT_DETECTION_CLOUD_EDITION.

Jiang, S., Cao, J., McCann, J. A., Yang, Y., Liu, Y., Wang, X. & Deng, Y. (2019, July). Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain. In 2019 IEEE international conference on Blockchain (Blockchain), IEEE, 405-410.

Avizheh, S., Nabi, M., Safavi-Naini, R. & Venkateswarlu K, M. (2019, November). Verifiable computation using smart contracts. In Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop, 17-28.

Maddali, L. P., Thakur, M. S. D., Vigneswaran, R., Rajan, M. A., Kanchanapalli, S. & Das, B. (2020, January). VeriBlock: A novel blockchain framework based on verifiable computing and trusted execution environment. In 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS) IEEE, 1-6.

Jia, B., Zhang, X., Liu, J., Zhang, Y., Huang, K. & Liang, Y. (2021). Block chain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. IEEE Transactions on Industrial Informatics, 18(6), 4049-4058.

Wood, A., Najarian, K., & Kahrobaei, D. (2020). Homomorphic encryption for machine learning in medicine and bioinformatics. ACM Computing Surveys (CSUR), 53(4), 1-35.

DOI: 10.6977/IJoSI.202403_8(1).0004
S. S. Rath, P. Jagadeesh MP., J. Systematic Innovation, 8(1), 36-48 (2024)

AUTHOR BIOGRAPHIES

Mrs Sonali Shwetapadma Rath (PhD) is a Research Scholar in the Department of Computer Science and Engineering at JSS Academy of Technical Education, Bengaluru, India. She has completed her M.Tech in Computer Science from Visveswaraya Technological University, Belagavi, and B.E in Information Technology from BPUT, Odisha. Her area of research interest includes Cyber & Information Security/Threats, Block chain, and SAP BTP Integration Suite. She has published 7 papers in International/National conferences and Journals. She has published 1 book chapter in Springer edited Book. She has acted as a resource person for various FDP/seminars/workshops on DevOps approach, Docker, Block chain, SAP Integration Suite,Dell Boomi . She has experience of mentoring critical projects sponsored by universities. She has been awarded as STAR faculty & MOUNTAIN MOVER. She has certified in Sales & CRM Overview from Salesforce Pathstream, certified in Robotic Process automation from Blueprism University, certified in Block chain Technologies, Smart Contract. She also received certificate as placement trainer under TCSion.

Dr. Prabhudev Jagadeesh is a Professor in the Department of Computer Science and Engineering at JSS Academy of Technical Education, Bengaluru, India. He completed his PhD in Computer Science from the University of Mysore, M.Tech in Software Engineering from Visveswaraya Technological University, Belagavi, and B.E in Computer Science & Engineering from the University of Mysore. His area of research interest includes Information Security, Machine learning, and Deep Learning. He has published 20 papers in International conferences and Journals. He has experience executing sponsored research projects in computer vision applications. He has worked on a consultancy project to explore a framework for a comprehensive sensor data processing engine. He has experience as General Chair and editor of proceedings of the 3rd International Conference on Cognitive Computing and Information Processing published by Springer.