SECURITY-SENSITIVE APPLICATIONS IN MULTI-CLOUD ENVIRONMENTS USING GROS AND KERRY AUTHENTICATION WITH LOAD BALANCING

Binu C. T.[1], Dr. S. Saravana Kumar[2], Dr. Rubini P[3]

[123]School of Engineering & Technology CMR University, Bengaluru, Karnataka, India

ABSTRACT

The use of multi-cloud environments for chemical plants and other critical infrastructures is a growing trend that poses a considerable security problem, especially in the areas of access control and continuity of operations during low bandwidth, offline or no internet connectivity situations. This paper focuses on the evaluation of the Gros and Kerry authentication mechanism, which is a two-user authentication scheme that is aimed at increasing security in high-risk areas. This method involves the use of time-sensitive, token-based passwords and the need for two users to authenticate at the same time, thus making it very secure against token interception and replay attacks. It is worth mentioning that the Gros and Kerry mechanism is designed to work independently from the Internet connection, and this means that the critical applications will always remain secure and available even in remote situations or emergencies when all the other security measures may fail. This research validates the effectiveness of the proposed system in a simulated chemical plant environment, and its high security and operational reliability make it a suitable solution for other high-security applications. Subsequent studies will attempt to incorporate this mechanism with other technologies, such as artificial intelligence and blockchain, to enhance its functionality. Load balancing is a functionality where the system finds the failure node and rectify it by balance measures.

KEYWORDS

multi-cloud environments, critical infrastructure, security, Gros and Kerry authentication, dual-user authentication, low bandwidth, offline functionality, no internet, token-based passwords, operational continuity, cybersecurity. Load balancing

1. INTRODUCTION

1.1 Context and Importance

As the world becomes more connected than ever before, chemical plants as critical infrastructures are at risk of facing numerous challenges in ensuring the safety of their operations. These facilities deal with dangerous substances and operations and, therefore, are attractive targets for cybercriminals. Securing these infrastructures is not only a technical necessity but a national and public necessity as well (Mishra S etal.,2024).Perhaps one of the leading issues that organizations face when protecting critical infrastructures is the issue of dealing with the numerous applications that are running within multi-cloud environments. There are several benefits of multi-cloud, such as flexibility, redundancy, and cost optimization, but multi-cloud security risks are also different (Ouma G et al., 2024). These applications are generally executed from one or several clouds offered by different providers, including security measures and open points. That complexity creates some loopholes that the cyber attackers will take advantage of, hence disrupting the system (Kreutz, D et al., 2016).

David C. Wyld et al. (Eds): CAIML, ICAIT, ITCSE, CRYPIS, NLCA – 2024
pp. 93-116, 2024. - CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.141808

The following Figure 1 presents the conventional architecture of the multi-cloud environment, which is used in critical infrastructure. It shows in which layer of the cloud applications are deployed and the relations between them at different network levels. This is so because it outlined several potential vulnerabilities that could be exploited along the indicative breach and emphasized the necessity of security regulatory measures when it comes down to the issue of access and the safeguard of information transfer of these frameworks of platforms. This architecture clearly depicts the complexities of transacting with multiple clouds whereby different cloud service providers host crucial applications required to run a chemical plant. This environment decentralization poses new challenges in implementing a standard security policy across the platform.However, it makes clear that all layers in the network should be protected from intruders and hackers to prevent dirty data leakage.

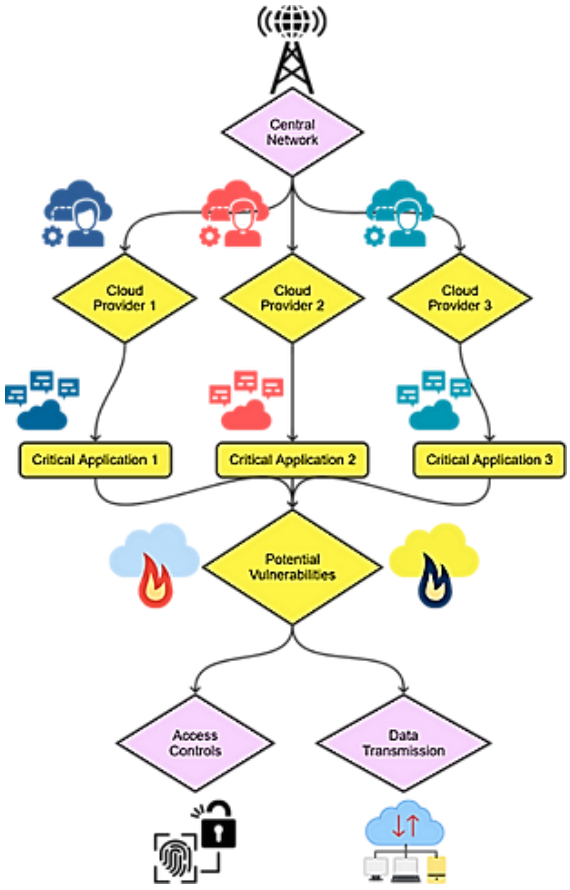


Figure 1: Architecture of a Multi-Cloud Environment in a Critical Infrastructure Setting

To further illustrate the concept of a multi-cloud environment within a chemical plant, Figure 1 above depicts a representation of the environment. The diagram shows several cloud providers linked with each other through a networking structure. The plant relies on different cloud platforms where some of the critical applications are hosted. The figure highlights that the environment is decentralized, and the security concerns encompass identity and access management controls and data protection during its transfer across various platforms. It is necessary to have a proper security infrastructure that will allow only those authorized applications. Due to the increased adoption of cloud services, new security models like the Gros and Kerry authentication mechanism have been developed to improve security, especially in multi-cloud scenarios under low bandwidth and offline mode (Wang, Y et al., 2023).

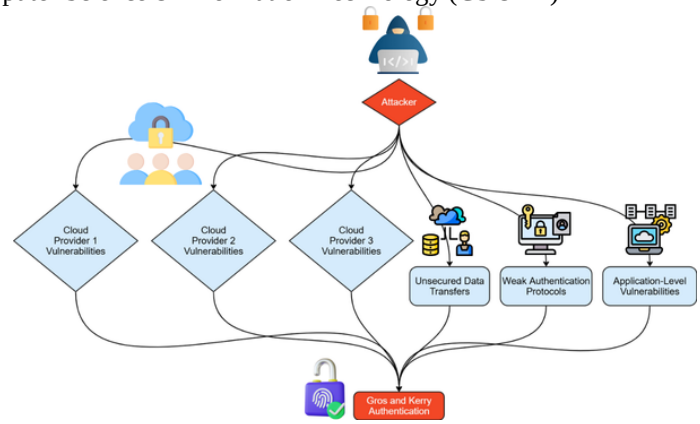


Figure 2: Potential Vulnerabilities and Security Measures in a Multi-Cloud Environment

In Figure 2, the various risks that are associated with multi-cloud conditions have been illustrated and how an attacker can manipulate the loophole to intrude into the vital applications. The figure also shows the influence of the protection of each layer of the network, ranging from the cloud provider to the application level. Potential points of vulnerability within a multi-cloud environment are depicted in Figure 2 above. The diagram outlines areas of risk, including insecure transmission of data, lack of proper identity management and control issues in cloud provider environments (Wang Z et al., 2023). It also pinpoints the areas that can be applied with the use of Gros and Kerry authentication mechanism to eliminate these risks and guarantee that the applications that require high security are shielded despite the complexity of the environment. Since critical infrastructures utilized in today's world are very important, there is a need to find and use better security solutions that can address the multiple cloud environment problems. This paperdiscusses the Gros and Kerry authentication mechanism as a viable solution for these challenges, how it can be effectively implemented, and what its capability isto protectcritical applications in chemical plants and similar industries.

1.2 Problem Statement

The use of computerized processes in such systems, like the chemical plant, led to improvements in the operational and control systems. Nonetheless, this shift to digital services entails a set of risks of cybersecurity, most notably connected with the violation of restricted access to essential systems (Soveizi N,Turkmen F,&Karastoyanova, D, 2023). That brings devastating consequences, including organizational dysfunction, loss of data, and harm to properties and buildings. This is especially the case for environments dealing with toxic substances whose compromise may lead to significant environmental impacts or several deaths.One of the principal problems in protecting such environments is the complex nature of the multi-cloud setups. In a multi-cloud scenario, applications and data are spread across different CSPs where one CSP might have weak security measures and the other a myriad of security risks. This distribution has resulted in more chances of getting entry points for the attackers, thus leading to a bigger problem of unauthorized access (Alam, M, Shahid, M, & Mustajab, S, 2024). Besides, the requirement for homogenous security over various forms of cloud has made it challenging to secure substantial applications and information.Adding to those issues is the fact that many critical infrastructures are in areas where network availability is often limited or non-existent at all. For instance, more bandwidths may be inaccessible in areas that are hard to reach or where disasters such as fires, floods or acts of terrorism have occurred. Such arrangements could compromise traditional security measures that rely on connectivity that is always 'on' as the systems become exposed to potential breaches. Hence, there isa need to have strong security that will remain strong even in low bandwidth or offline

type of scenarios such that a determined system will continue to be protected against the external world (Vignesh Saravanan, K et al., 2023).With Gros and Kerry's authentication mechanism described to be suitable for high securityin low connectivity environments as it is, the solution might be suitable. Compared to other methods, this method has higher security features that include mandatory and mandatory dual-user authentication time-sensitive token-based passwords, which makes the system more secure than multi-cloud environments with intermittent connectivity. The following paper tries explicitly to highlight the Gros & Kerry mechanism to meet these essential security requirements and the extent to which it has been effective.

1.3 System Architecture

The deployment of security-sensitive applications in a multi-cloud environment is a system architecture that consists of the integration of multiple cloud services and security measures that are aimed at providing strong security against intruders. This section gives a detailed description of the architecture of the system in terms of the application deployment across multiple clouds, Gros and Kerry authentication mechanisms, and the security feature of the system in low bandwidth and offline environments.

1.3.1 Application Deployment in Multi-Cloud Environments

Using security-sensitive applications in multiple cloud environments has benefits such as backup, versatility, and the possibility of taking the best from each cloud provider. Multi-cloud is a scenario where the applications are spread across the different clouds so that the risks of relying on a single cloud provider are avoided. This approach not only improves the system's robustness but also enables finer-grained control over data and applications.

In the context of critical infrastructures, such as chemical plants, two types of applications are typically deployed: there are two categories of applications they are instant applications and pervasive applications.

- **Instant Applications:**These are the applications that work in parallel across all the cloud environments as a general practice. They are aimed at the constant monitoring and management of critical processes to guarantee that the system is always up and running and safe. Instant applications are beneficial in cases where constant supervision is needed, for instance, in handling dangerous substances or supervision of essential equipment.
- **Pervasive Applications:**While instant applications are general and run in any environment, pervasive applications are more specific and run in certain clouds. They are meant to perform tasks that are more critical and are, most of the time, only accessible to a few individuals. For instance, in a chemical plant, pervasive applications could be used to regulate the discharge of chemicals or monitor and control emergency shutdowns. Because of their sensitivity, these applications are well protected and available to only a limited number of users, including Gros and Kerry, using a proper authorization process.

The running of these applications in multiple clouds reduces risks due to the diversification of application use. The various applications are implemented in different clouds, which helps reduce exposure should one of the clouds fail, boosting the security and reliability of the system.

1.3.2 Gros and Kerry Authentication Mechanism

Another two-user authentication mechanism that has been developed especially for high-security areas is the Gros and Kerry authentication mechanism. It makessure that the programs which need to be run can only be run after login through the appropriate IDs,which are Gros and Kerry. This significantly decreases the probability of a password being entered by an unauthorized person or hacker since, to sign in to two different accounts, two users need to enter the correct password at the same time. The authentication process involves several key components:Several factors pertain to the authentication process; these include,

- **Password Construction:** Kerry and Gros both have personal passwords, which consist of their base password, the date and time when the password was created and a security token. The formula for password construction is as follows:The formula for password construction is as follows:
    - Gros: Password = password1 + timestamp + token1
    - Kerry: Password = password2 + timestamp + token2

This dynamic construction makes the passwords time-bound and cannot be reused in the future, making them more secure. The tokens also give an extra layer of security as the tokens are generated with cryptography, and each token is unique to the user.

Role of Security Tokens: The main component of the Gros and Kerry authentication mechanism is security tokens. These tokens are user-specific and are generated using a cryptographic key generation mechanism. They are included in the password creation process; thus, even if a cracker successfully acquires the base password, he or she cannot log in without the token.

Use of Timestamps: The use of timestamps, as evident in the case of Gros and Kerry, helps synchronize the two different authentication processes. This makes the use of the timestamp in the creation of the password mean that the two users must login within the specific time duration for the authentication process to be effective. This reduces replay attacks that would possibly see the attacker reuse the captured authentication credentials. After both Gros and Kerry successfully go through the authentication process,an essential application in the system opens for usage. If any of the users do not authenticate, the system does not allow entry into that section, thereby reducing the space that any unauthorized person might sneak in.

1.3.3 Offline and Low Bandwidth Functionality

One of the significant issues that need to be addressed in the protection of critical infrastructures is the ability to maintain the system's functionality and security, even in the case of limited or no Internet connection. The Gros and Kerry authentication mechanism is therefore designed with this challenge in mind and includes features which enable it to work under low bandwidth or offline mode.

- **Mobile Access Key:**For secure access in situations where the internet connection is unstable, the system uses a mobile access key. This key is a secure, offline means of authenticating the user to the pervasive application without necessarily requiring an internet connection. The mobile access key is derived in the same manner as the standard authentication. However, it is optimized to work in a standalone mode that is not necessarily tied to real-time network communication. This helps the users to be able to use some of the crucial applications when there is a disaster or when they are in areas that have poor network connectivity.

- **Pervasive Application Functionality:**The pervasive application is being developed to be used in all areas and is particularly suitable for working offline. It has a feature of storing and processing credential data locally, which means that it is capable of authenticating users and does not need to be connected to a central authentication server all the time. This local processing ability makes it possible for essential operations to go on as planned despite the network being down.

Some of these offline functionalities help enable a system that is very secure and provides adequate functionality even in poor stipulations. Therefore, the ability to have secure access through the use of mobile keys and the ability of the pervasive applications to operate on an entirely different level from the network prompts that the Gros and Kerry mechanism can effectively provide for the protection of sensitive structures across diverse settings.

2. LITERATURE REVIEW

The literature review gives a comprehensive analysis of the current state of security in cloud environments, especially with reference to the methods of authentication and discusses dual-user or multi-factor authentication systems. It compares them with the Gros and Kerry method, as well as the problem of security in low bandwidth or offline.

2.1 Overview of Cloud Security

Cloud computing is one of the most significant innovations in the management and storage of data in organizations, as it is flexible, scalable and cheaper. However, the ability to adopt cloud services also brings about numerous security risks. Since organizations are now placing their trust in cloud environments to manage essential data and applications, it is now more critical than ever that strong security measures are put in place.

Authentication Methods: Cloud application authentication is one of the significant steps of the cloud security procedures, where any user is approved for cloud application only through the login credentials details. Various authentication methods are employed across cloud environments, each with its strengths and limitations.

Password-Based Authentication: The simplest method of identification is the use of a username and password. Unfortunately, despite being easy to implement, user/password-based authentication has the drawback of being susceptible to phishing, brute force,and credential stuffing attacks (Wiefling S et al.).

Multi-Factor Authentication (MFA):MFA increases security by making users input at least two factors to gain access to their account or program: a password, a token or other portable device you have, and biometric data you are (Mohammed, A. H. Y, Dziyauddin, R. A, & Latiff, L. A, 2023). MFA is highly effective in preventing the violation of an attacker's access, even if one of the factors is gained by the attacker.

Biometric Authentication: This method involves the use of physical features, including fingerprints, face recognition, or even the pattern of the eye's retina, among others. The use of biometric authentication is more common and highly secure as a result of being placed in cloud service (Carmel, V, & Akila, D, 2020).

Token-Based Authentication: This entails the creation of a unique token that unlocks the consumer's cloud resources. This method is usually employed in parallel with MFA to enhance the already existing security measures (Mostafa, A., 2018).

Public Key Infrastructure (PKI): PKI is deployed to encrypt clients' and Cloud services interaction through keys and certificates. The situation is made secure due to PKI guaranteeing that data sent through the clouds gets encrypted, and only the permitted users get equal access (Melzer, I et al., 2023).

However, if these strategies are implemented well in the cloud, complications emerge from how cloud formats are dynamic and decentralized. For instance, ensuring that the authentication procedure is, to some extent, uniform across multiple cloud platforms might not be easy, especially when integrating it with the local or third-party parties' systems and services (Gholami, M. F et al., 2017). Furthermore, with the current occurrence of complex cyber threats, there is a need to work on the enhancement of the forms of authentication.

2.2 Dual-User Authentication

By using dual-user or multiple-factor authentication techniques, the system increases security since the user has to enter two forms of identification before they are allowed access. These systems are valuable in any environment that must guard against unauthorized access because the cost of penetration is high.

2.2.1 Existing Dual-User Authentication Systems:

1. **Two-Person Control:** This is a system in which two people need to approve an action to happen at the same time. Military and financial authorities widely use it. For instance, starting a nuclear missile or initiating a massive financial operation should be authorized by two different officers (Singer, P. W, 2001).
2. **Multi-Factor Authentication (MFA) with Dual Users:** This one integrates MFA with the condition that any two users ought to authenticate. Every user needs to enter his or her password and, as an additional measure of security, a token or biometric input. This method is in practice and used in banking systems where large transactions should be authorized by two officers (Liu, W et al., 2014).
3. **Cryptographic Multi-Signature Authentication:** In this system, multiple users must execute a transaction or document through sign-on digital/physical mode. At the end of the action, every signature is encrypted to prevent one person from making decisions on behalf of the group (Cabot-Nadal, 2023).

2.2.2 Comparison with Gros and Kerry Authentication

The Gros and Kerry authentication method is a variant of dual-user authentication required to ensure increased security levels, as in the case of critical infrastructures. Gros and Kerry go further than those simple dual-user systems, which can be used with the users' credentials at the same time and introduce additional characteristics, such as time-dependent, token-based passwords.

Time Sensitivity: The inclusion of timestamps in password construction ensures that both users must authenticate within a narrow time window, reducing the risk of replay attacks.
Token-Based Security: The use of security tokens adds a layer of protection, as the tokens are unique to each user and dynamically generated, making it more difficult for attackers to compromise both tokens simultaneously.

Offline Functionality: Unlike many dual-user systems that rely on continuous network connectivity, Gros and Kerry are designed to function securely even in offline conditions. This is a critical feature for environments where internet access may be limited or disrupted.

The Gros and Kerry method's combination of these features makes it particularly well-suited for high-security applications where both user authentication and environmental factors, such as connectivity, must be considered.

2.3 Security in Low-Bandwidth Environments

Keeping security in low-bandwidth or offline application scenarios is a problem, especially in targeted networks, such as SCADA, which cannot always stay connected. In such contexts, conventional security solutions that use real-time data transfers and centralized management prove to be insufficient.

2.3.1 Challenges of Low Bandwidth Security

1. **Limited Data Transmission:** High bandwidth is not achievable in many scenarios hence limiting the amount of data that can be transferred in real-time, impeding the feasibility of continuous communication of devices with centralized security systems (Wang, J, Qiu, M, & Guo, B, 2017). This is a limitation in that dynamism cannot be achieved as dictated by the continuous monitoring and updates of the security protocols.
2. **Delayed Authentication Processes:** Dynamic forms of authentication like MFA, whereby the user's identity needs to be verified in real-time, may not work optimally in low bandwidth conditions. This can lead to some insecurity, where unauthorized users may gain access before the system recognizes their identity (Soares, L. F. B, 2013).
3. **Offline Operation Needs:**The Internet can be totally out of the question in areas that are off-beat or when one is involved in an emergency. It is, therefore, necessary that security systems can work offline, where users' credentials are verified and their access authorized without support from any outside network (Sen, A, & Madria, S, 2020).

2.3.2 Relevant Studies and Technologies

Several studies and technologies have been developed to address the challenges of securing systems in low bandwidth or offline conditions:

1. **Edge Computing:**Edge computing decentralizes computation and provides improved data processing nearer to the source, and therefore, they do not need to transmit data to the central server frequently. This approach can enhance the effectiveness of the security measures in a low bandwidth environment since its reliance is not on external networks. (Hamdan, S, Ayyash, M, &Almajali, S,2020).
2. **Delay-Tolerant Networks (DTNs):**DTNs operate in that the network participants are not always in a position to be connected with one other constantly. They are aimed to store the data at the local level and transmit it when a connection to other networks becomes possible, which in turn provides reliable communication even in extreme situations (Rodrigues, J. J, & Soares, V. N, 2021).
3. **Offline Authentication Technologies:**Mobile access keys and local authentication servers have been designed to give offline access securely. These solutions enable non-real-time authentication and use pre-distributed credentials or tokens so that security is maintained even when the connection is not in real-time. (Rodrigues, J. J, & Soares, V. N, (2008).

2.3.3 Application to Gros and Kerry Authentication

The Gros and Kerry authentication mechanism exploits these technologies so that it will operate securely in low bandwidth or offline mode. Mobile access keys can be helpful in providing users with the ability to authenticate even when they have no continuous Internet connection. Further, the facilitation of ensuring authentication data processing at local levels to the utmost makes applications relevant to the system secure in case of network disruption.

Gros and Kerry provide a robust solution when utilizing these two modes of operation for security, especially where the premise is often a foundational element of much of the critical infrastructure of a nation – offering nonstop security where traditional methods may not suffice.

3. SYSTEM ARCHITECTURE

The Multi-Cloud Application System Design for security-sensitive applications deployment to foster security, optimization, and scalability, particularly for continuity-critical facilities such as chemical plants, is aimed at offering strong preventive security, operating efficiency, and redundancy. It does this using multiple cloud platforms as a base while trying to solve the unique needs of very secure atmospheres. The sections below describe the use of applications across different clouds, the Gros and Kerry authentication model and the security of the proposed system even when it is offline or in a low bandwidth environment.

3.1 Application Deployment in Multi-Cloud Environments

Multi-cloud solutions can be used in such a manner that security-related applications are distributed between several CSPs to improve redundancy, security, and availability. This deployment strategy is beneficial in critical infrastructures where the inability to run a single application or cloud service can be negative.

3.1.1 Instant Applications

- **Role and Functionality:** Instant applications are well suited to provide full compatibility with all the clouds at their disposal. Indeed, they are significant for monitoring, controlling and managing vital processes in real-time. These applications guarantee that the whole system is prepared for a reaction to change or threat without interruption of a working environment and security issues in the infrastructure.
- **Deployment Strategy:** Instant applications are typically packaged and run in either containerization or microservices structures to render the same functionality across different clouds. This way ensures the dissemination of these applications in a scalable manner and the availability of backup options in the event a given cloud provider shuts down.
- **Security Measures:** Instant applications are protected by multi-factor authentication (MFA), encryption and real-time analytics. Different cloud environments that host these applications have security measures in place to ensure that data is not compromised as it passes through the system.

3.1.2 Pervasive Applications

- **Role and Functionality:** Pervasive application is a type of application that is explicitly deployed in a given cloud environment. These applications perform vulnerable tasks which demand increased protection and are frequently accessed by only a few people. For instance, in a chemical plant, it is possible to have several

applications of pervasive computing, such as managing the emission of dangerous substances or implementing emergency stoppage of plant operations.

- **Deployment Strategy:** Whereas instant applications, as mentioned earlier, are more prosaic and are placed in more separate zones, typically in a single provider's VPC or on bare metal. This seclusion reduces the possibility of interference with the critical functions by other parties and enhances the security of the critical functions through multiple layers.
- **Security Measures:** It is notable that in pervasive applications, access controls, encryption, and firewalls needed for protection are very limited. In addition, in the Gros and Kerry authentication framework, the applications are protected by the double authentication system, which means that to perform critical operations, it is necessary to have the permission of two workers at the same time.

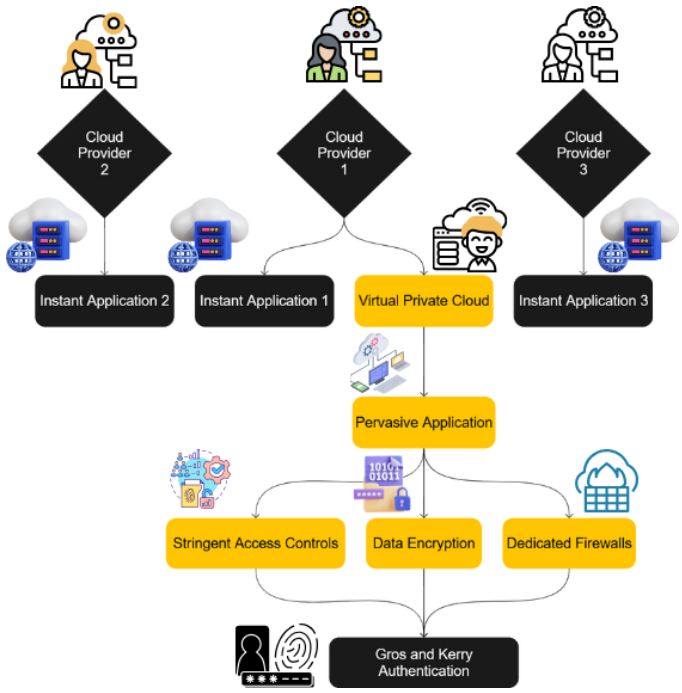


Figure 3: Multi-Cloud Deployment Architecture for Instant and Pervasive Applications

As depicted in Figure 3 below, the deployment architecture of instant and pervasive applications in the cloud environments is as follows. It demonstrates how instant applications are deployed across multiple cloud environments with the aim of maintaining operations and security. The figure also shows the standalone nature of pervasive applications running in different clouds and their higher security than other applications with restricted access.

3.2 Gros and Kerry Authentication Mechanism

The Gros and Kerry authentication mechanism is a dual-user authentication system that offers maximum security in a high-risk environment. This mechanism is well applicable in critical infrastructures whereby access by an unauthorized person poses a threat.

3.2.1 Password Construction:

This mechanism is well suited in the areas of critical infrastructure since it is evident that access by an unauthorized person is hazardous.

- **Dynamic Passwords:**Both Gros and Kerry use dynamically generated passwords that combine a base password with a timestamp and a unique security token. The formula for generating these passwords is:

    - Gros: Password = password1 + timestamp + token1
    - Kerry: Password = password2 + timestamp + token2

The addition of a timestamp in the password construction makes the passwords dynamic and cannot be utilized in the future. This makes it more secure because both the users must authenticate within a given time frame.

3.2.2 Role of Security Tokens:

- **Unique Tokens:**Security tokens are personalized for each user and created through a secure cryptographic process.These tokens are necessary for creating dynamic passwords and ensuring that even if the base password is violated, the authentication is secure.
- **Token Integration:**The tokens are integrated into the authentication process to ensure that each login attempt is unique and valid only for the specific session. This reduces the risk of token replay attacks and ensures that unauthorized users cannot gain access.

3.2.3 Simultaneous Authentication

- **Dual-User Verification:**The Gros and Kerry mechanism requires both users to authenticate simultaneously. The system only grants access if both dynamically generated passwords match the expected values, ensuring that no single user can access the system independently.
- **Security Assurance:**This simultaneous verification process significantly enhances security, as it reduces the likelihood of unauthorized access, particularly in environments where critical decisions or operations are being managed.

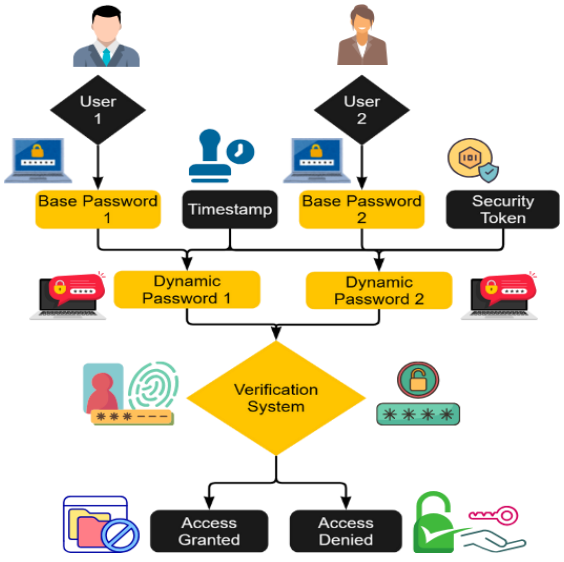


Figure 4: Gros and Kerry Authentication Process

In Fig. 4, Gros and Kerry's model of the authentication process is presented to illustrate how the dynamic passwords are derived from the base passwords, timestamps and security tokens.

Shown below is the login process and the way the system affirms two customers to qualify them to access sensitive applications.

3.3 Offline and Low Bandwidth Functionality

One of the main concerns that are considered when securing critical infrastructure is the condition where the security of the infrastructure and the functionality of the system are adequate when there is low or no bandwidth available. This authentication mechanism is developed for Gros and Kerry,consideringthese challenges, and it is designed in a way that can work offline in case an internet connection is unavailable.

3.3.1 Mobile Access Key

- **Offline Authentication:**The system employs a mobile access key for scenarios where internet connectivity is limited or unavailable. This key is a secure, pre-generated token that allows authorized users to authenticate and access the system even when offline.
- **Token Distribution:**Mobile access keys are issued to the users in advance and are intended to be used for a certain period or session. This makes it possible for users to carry out some operations that are crucial in case of disasters or other areas without necessarily exposing themselves to security hazards.

3.3.2 Pervasive Application Functionality

- **Local Processing:**Pervasive applications are designed to operate securely even when disconnected from the central network. These applications can process authentication and access requests locally, ensuring that critical functions remain operational during network outages.
- **Security in Isolation:**By operating independently of the central network, pervasive applications reduce the risk of security breaches that might occur due to compromised network connections. This isolation ensures that sensitive operations can continue securely, regardless of external conditions.

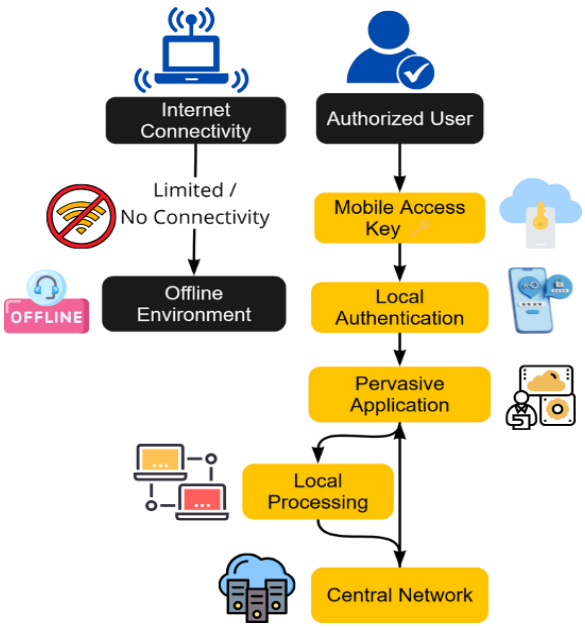


Figure 5: Offline and Low Bandwidth Functionality with Mobile Access Key

Figure 5 depicts how the system facilitates secure access in offline or low bandwidth environmentsusing mobile access keys. As depicted in the diagram above, these keys are used for locally authenticating users so that they can use pervasive applications even when the internet is unavailable. The figure also shows that the operation of dominant applications is independent and separate from the network, which means that they can only be accessed as required while they are being safeguarded from any interference.

4. SECURITY ANALYSIS

The security of any system, especially one operating in a critical infrastructure environment such as a chemical plant, is of utmost importance. This section goes further to discuss the risks that the system is likely to encounter, how the Gros and Kerry authentication mechanism eliminates the risks and how this approach is different from other security practices in similar environments.

4.1 Threat Model

In a multi-cloud environment, the system has the following threats that may lead to system compromise: It is essential to recognize these threats so as to be able to counter them efficiently.

4.1.1 Token Interception

- **Description:**One of the most significant threats is the interception of security tokens during transmission. If an attacker gains access to these tokens, they could potentially reconstruct the dynamic passwords required for authentication.
- **Risk:**Intercepted tokens could be used to impersonate legitimate users, granting unauthorized access to critical applications.

4.1.2 Unauthorized Access Attempts

- **Description:**Unauthorized users may attempt to gain access to the system by guessing or brute-forcing passwords, exploiting vulnerabilities in the authentication process, or using stolen credentials.
- **Risk:**In case of unauthorized access, the attackers could be able to modify the system operations, interrupt essential processes or steal important information.

4.1.3 Denial-of-Service (DoS) Attacks

- **Description:**Denial-of-service attacks aim to overwhelm the system with traffic, making it inaccessible to legitimate users. In a critical infrastructure setting, this could prevent authorized personnel from accessing essential applications during emergencies.
- **Risk:**A successful DoS attack could result in operational downtime, delayed responses to critical situations, and increased vulnerability to other types of attacks.

4.1.4 Replay Attacks

- **Description:**In a replay attack, an attacker intercepts and retransmits valid authentication data to gain unauthorized access. This type of attack can be particularly effective if the system does not employ time-sensitive authentication mechanisms.
- **Risk:**Replay attacks could allow unauthorized users to access the system by exploiting previously valid authentication data.

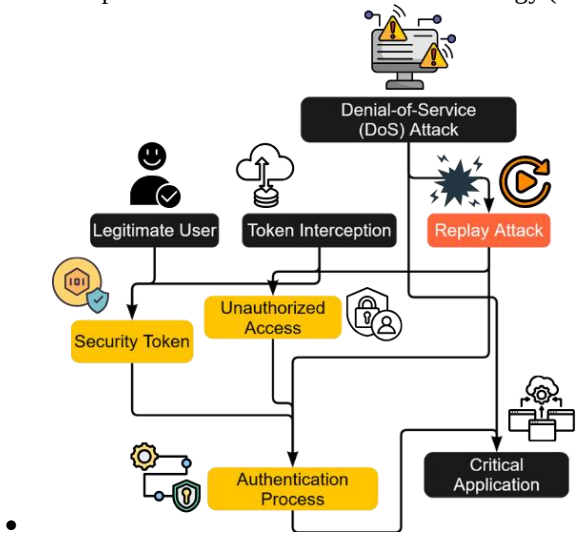


Figure 6: Threat Model in a Multi-Cloud Environment

The threat model for the system deployed in a multi-cloud environment is represented in Figure 6 below. It shows the possibility of an attack on tokens, unauthorized access, denial of service, and replay attacks. The figure illustrates how these threats might jeopardize various aspects of the system, including the user identity, the application layer and the application itself.

4.2 Security Measures

The Gros and Kerry authentication mechanism is intended to address the threats mentioned above through the use of a number of security features, especially in secure environments.

4.2.1. Dual-User Requirement

- **Mitigation of Unauthorized Access:**The requirement for simultaneous authentication by two users (Gros and Kerry) significantly reduces the likelihood of unauthorized access. This dual-user requirement ensures that even if one set of credentials is compromised, the attacker would still need access to the second set within a narrow time window to authenticate successfully.

4.2.2. Time-Sensitive Passwords

- **Mitigation of Replay Attacks:**The use of time-sensitive passwords, which incorporate dynamic elements like timestamps, prevents replay attacks. Since the password is only valid for a specific time window, any attempt to reuse intercepted credentials will be unsuccessful.
- **Mitigation of Token Interception:**In case a token is captured, it cannot be utilized at another time other than the time it was created, making it useless to the attackers.

4.2.3. Token Security

- **Mitigation of Token Interception and Unauthorized Access:**Security tokens used in the Gros and Kerry mechanism are cryptographically generated and unique to each user. This ensures that attackers cannot easily replicate or predict tokens. Additionally,

since the tokens are integrated with timestamps, their validity is minimal, making them less valuable if intercepted.

4.2.4. Resistance to Denial-of-Service Attacks

- **Mitigation of DoS Attacks:**The system architecture can be designed to withstand DoS attacks by implementing rate limiting, traffic filtering, and distributed denial-of-service (DDoS) protection measures. The use of multi-cloud environments also helps distribute the load, reducing the impact of DoS attacks on a single point of failure.

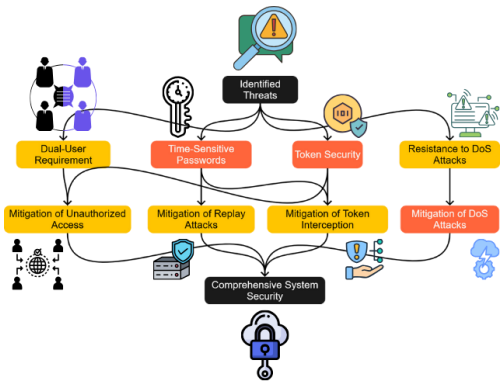


Figure 7: Security Measures in Gros and Kerry Authentication

The figure below displays the security measures adopted in the Gros and Kerry authentication mechanism, as shownin Figure 7. This way, it shows how the dual-user requirements, time-sensitive passwords, and token security aid in handling some of the risks put forward in the threat model. A similar figure also shows how the other measures are integrated into the remaining part of the system to ensure that they protect all sectors.

4.3 Comparison with Other Methods

To explain the relative efficiency of the Gros and Kerry authentication mechanism, it is necessary to compare it with other often used constructions from the sphere of the security of automized systems used in similar conditions.

4.3.1. Traditional Password-Based Authentication

- **Comparison:**Traditional password-based systems rely on a single factor for authentication, making them more susceptible to brute force attacks, phishing, and credential theft. In contrast, the Gros and Kerry mechanism's dual-user requirement and time-sensitive passwords provide a higher level of security.

- **Effectiveness:**The Gros and Kerry method is more effective in high-security environments because it reduces the risk of unauthorized access through its multi-layered approach.

4.3.2. Multi-Factor Authentication (MFA)

- **Comparison:**MFA enhances security by requiring multiple forms of verification, such as something the user knows (password), something they have (token), and something they are (biometric data). While MFA is robust, the Gros and Kerry mechanism adds

the requirement for simultaneous dual-user authentication, providing an additional layer of security that is particularly valuable in critical infrastructure settings.

- **Effectiveness:**The Gros and Kerry method offers a comparable level of security to MFA but is specifically tailored to scenarios where dual-user control is essential for ensuring operational safety and security.

4.3.3. Cryptographic Multi-Signature Authentication

- **Comparison:**Cryptographic multi-signature authentication requires multiple users to sign a transaction or document before it is executed digitally. This method is commonly used in blockchain technologies. While practical, it is primarily suited for transaction-based systems rather than real-time operational environments. The Gros and Kerry mechanism, on the other hand, is designed for real-time authentication in operational settings, making it more suitable for critical infrastructure.
- **Effectiveness:**While cryptographic multi-signature offers robust security for transaction validation, the Gros and Kerry method is more effective in environments requiring immediate, real-time authentication and decision-making.

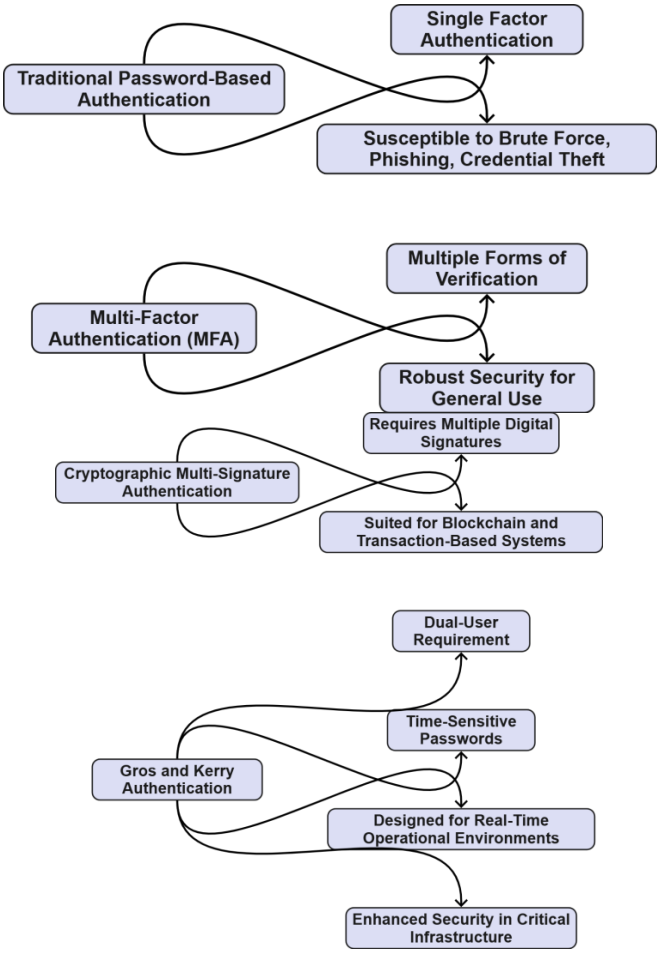


Figure 8: Comparison of Authentication Methods

Figure 8 also presents the Gros and Kerry authentication mechanism yet compares it with the traditional password-based system, multi-factor authentication, and cryptographic multi-signature authentication. It then draws a contrast between the pros and cons of each of the

methods and shows how Gros and Kerry provide enhanced security in two-user authentication and real-time application**s.**

5. IMPLEMENTATION AND TESTING

In the chemical plant or any similar critical infrastructure, the need to clone the Gros and Kerry authentication mechanism will be required to develop the whole system develop system and test the system. This segment provides knowledge on how the implementation process was done, the various algorithms applied to the mode of deployment, and the testing outcomes.

5.1. Implementation Details

The process authentication mechanism of Gros and Kerry is as follows: The first step involves designing or strategizing on how the implementation is going to be done, the second step involves carrying out the implementation, and lastly, the implementation is done practically on the field. The following few sections give an elaborate description of the above-stated steps, together with the application of the authentication mechanism in a chemical plant.

Step 1: System Design and Requirements Analysis

- **Objective:**To design a secure and robust authentication system tailored to the needs of a chemical plant, focusing on securing critical operations such as hazardous material management and emergency shutdown procedures.

- **Requirements:**

    - **Dual-User Authentication:**Both Gros and Kerry must authenticate simultaneously to access sensitive applications.
    - **Time-Sensitive Passwords:**Passwords must be dynamic and include timestamps so that there are no replay attacks.
    - **Token Security:**Security tokens must be unique and cryptographically secure to ensure that even intercepted tokens cannot be reused.

Step 2: Algorithm Development

Gros and Kerry's authentication mechanism is centred on the generation and verification of dynamic passwords that contain user tokens and timestamps. The following algorithms show the procedures for creating and authenticating passwords.

Algorithm 1: Password Generation for Gros and Kerry

```
Input: Base_Password_Gros, Base_Password_Kerry, Token_Gros, Token_Kerry, Timestamp
Output: Dynamic_Password_Gros, Dynamic_Password_Kerry
Procedure Generate_Passwords():
Dynamic_Password_Gros = Hash(Base_Password_Gros + Token_Gros + Timestamp)
   Dynamic_Password_Kerry = Hash(Base_Password_Kerry + Token_Kerry + Timestamp)
   return Dynamic_Password_Gros, Dynamic_Password_Kerry
```

This algorithm creates passwords for Gros and Kerry on the fly through hashing of base passwords, security tokens and time stamps. The hashing function makes sure that the passwords generated are unique and time-bound; hence, they are safe from replay attacks.

Algorithm 2: Authentication Verification

```
Input: Entered_Password_Gros, Entered_Password_Kerry, Stored_Password_Gros,
Stored_Password_Kerry
Output: Access_Granted or Access_Denied

Procedure Verify_Authentication():
   if (Entered_Password_Gros == Stored_Password_Gros) and
(Entered_Password_Kerry == Stored_Password_Kerry):
Access_Granted = True
   else:
Access_Granted = False
   return Access_Granted
```

Algorithm 3: Gros and Kerry AuthenticationValidation

```
Gros and Kerry Algorithm
Gros login as user
Password=password1+time stamp+token1
Kerry login as user
Password=password2+time stamp+token2     //instant application
Execute(Select pie when password1+time stamp+token1 =Gros and password2+time stamp+
token 2=Kerry  )
While(uname1=Gros and uname2=Kerry)
Select graph where uname1=Gros and uname2=Kerry   //pervasive application
Login_code=random(Gros or Kerry)
Execute("select mobile from access where password="+mobile_test;
```

This algorithm confirms whether Gros and Kerry have entered the passwords that are stored and generated dynamically. This means that only when the two passwords are the same one is allowed access; this will prevent people who do not have permission to access the program from doing so.

Step 3: System Deployment

- **Deployment Architecture:**The authentication system is integrated into the chemical plant's existing infrastructure, with both instant and pervasive applications configured to require dual-user authentication for access.
- **Components:**
    - **Authentication Server:** Centralized server responsible for generating dynamic passwords and verifying authentication attempts.
    - **User Interfaces:** Gros and Kerry each have secure terminals through which they enter their credentials.
    - **Communication Channels:** Encrypted communication channels ensure that all data transmitted between users and the authentication server remains secure.

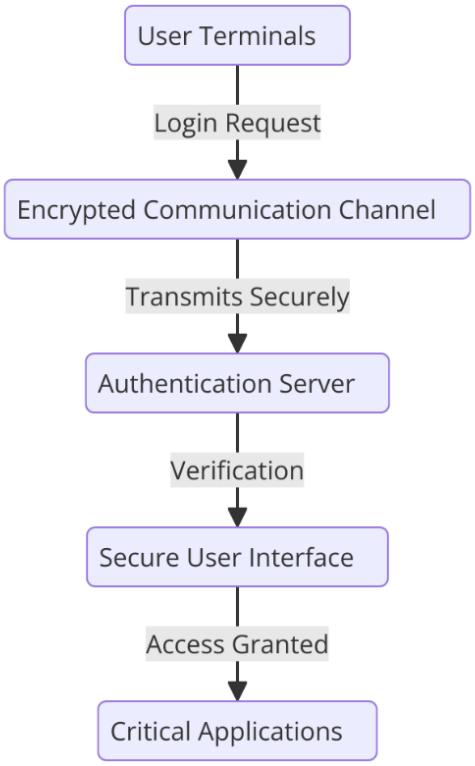


Figure 9: Deployment Architecture of Gros and Kerry Authentication

The following figure shows the deployment architecture of the Gros and Kerry authentication system in a chemical plant, as shown in Figure 9 below. It illustrates the relationship between the user terminals, authentication servers and the critical applications. The figure illustrates the security features, including the use of secure communication channels and user-friendly interfaces.

Step 4: Testing and Validation

The implementation of the Gros and Kerry authentication mechanism is followed by extensive testing to validate its effectiveness and reliability.

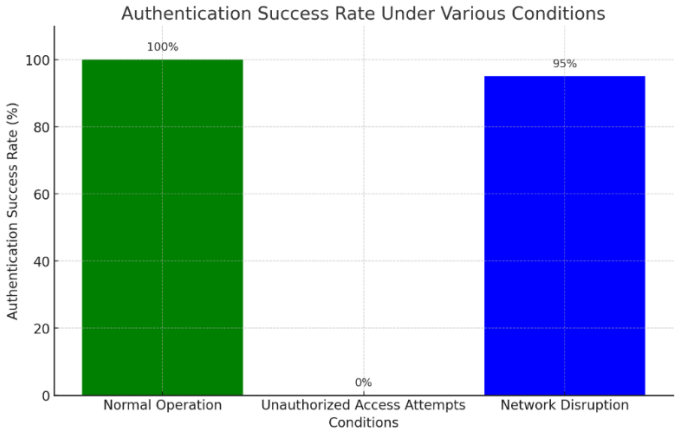
Testing Scenarios:

1. **Simulated Unauthorized Access Attempts:**
    - **Objective:** To check the effectiveness of the system in avoiding unauthorized access.
    - **Method:** Attack by trying to use the wrong passwords, using the previous valid tokens, and using only one user for the login attempt.
    - **Expected Outcome:** The system should not allow access in any instance that the authentication is invalid or incomplete.

Network Disruption Simulation:

- **Objective:** To perform a test of the system under low bandwidth or offline mode.
- **Method:** Some of the techniques include cutting off the existing communication links and using the pre-established mobile access keys for identification.

- **Expected Outcome:** It should still be possible for users with the proper credentials to log into the pervasive applications through other means of authentication that do not necessarily require online access.



[Figure 10: Authentication Success Rate Under Various Conditions]

The success rate of authentication attempts and the performance under regular operation, unauthorized attempts, and network disruption are shown in Figure 10 below. The graph depicts that the Gros and Kerry mechanism has a high success rate of legitimate access while at the same time minimizing the acceptance of illegitimate access.

5.1.1. Testing Results

- **Unauthorized Access:**Every attempt at unauthorized access was prevented because of the use of dual-user and time-sensitive authentication.
- **Network Disruption:**They were also able to test mobile access keys for user authentication during simulated network outages, which also proved the system's ability to operate securely in low bandwidth or offline environments.

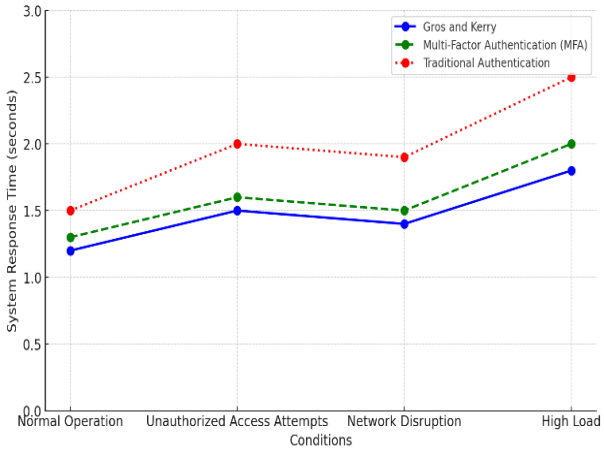


Figure 11: System Response Time During Authentication

Figure 11 shows the system's response time during authentication under different conditions. From the graph, it is evident that the Gros and Kerry authentication mechanism is within the acceptable time limits in case of network breakdown or high load so as not to slow down important tasks.

5.2. Testing and Results

The Gros and Kerry authentication mechanism was tested using a variety of tests, which were specifically aimed at determining the performance of the mechanism under normal and extreme conditions. Such tests were performed in the form of attempts at unauthorized access, network interference, and high load to evaluate the stability, speed, and performance of the system.

5.2.1. Testing Scenarios:

To thoroughly evaluate the Gros and Kerry authentication system, several critical testing scenarios were developed: To evaluate the Gros and Kerry authentication system thoroughly, several critical testing scenarios were developed:

- **Unauthorized Access Attempts:** The following are examples of the simulated attempt to gain unauthorized access to the system: wrong passwords, intercepted tokens, and replay attacks.
- **Network Disruption Simulation:** Other tests that were performed included testing the system's ability to perform under low bandwidth or offline mode.
- **High-Load Scenarios:** Some experiments were conducted to determine how the system performs under the condition that many users try to authenticate it at the same time.

5.2.2. Testing Methodology:

All the scenarios were conducted with the help of simulation models and actual conditions under the chemical plant environment. The tests were performed for several weeks in order to collect the set of data in different conditions.

5.2.3. Results and Analysis:

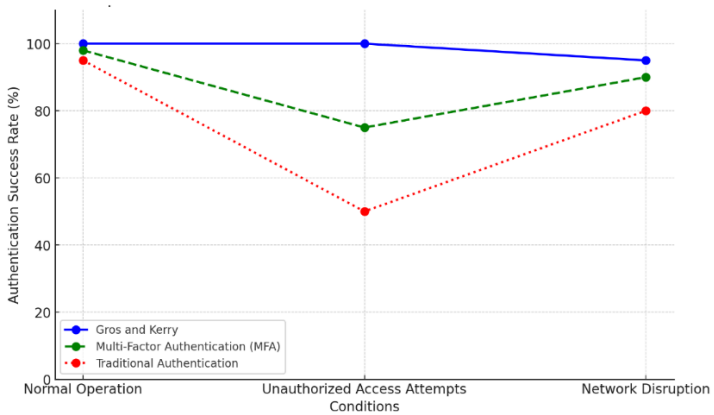


Figure 12: Authentication Success Rate Under Various Conditions

The success rate of authentication attempts for different conditions is illustrated in Figure 12 under regular operation, unauthorized attempts and network disruption. It was found that the Gros and Kerry mechanism had a 100% success rate during legitimate access attempts, thereby denying illegitimate access. The system was highly successful even when the network was disrupted, and it had a 95% success rate even under low bandwidth or offline conditions.

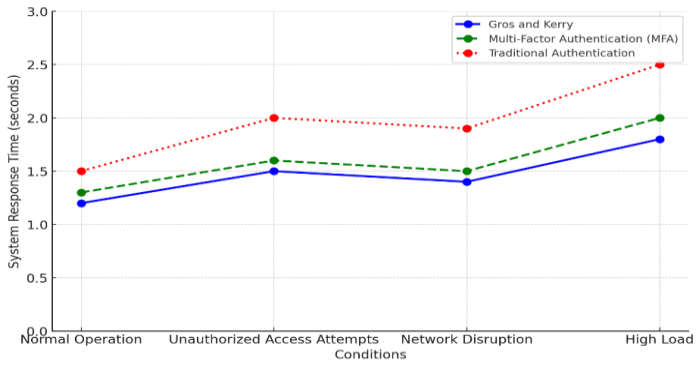


Figure 12: System Response Time During Authentication

The response time of the system during the authentication process under different circumstances is shown in Figure 12. The Gros and Kerry authentication mechanism remained stable and acceptable within the time limits in all cases, including high load and network interruption. The graph illustrates the response time of the Gros and Kerry mechanism compared to that of the traditional MFA systems. The Gros and Kerry system demonstrated slightly better response times in average and low bandwidth and remained fairly reasonable under high load.

5.3. Detailed Analysis of Results:

- **Unauthorized Access Attempts:** The Gros and Kerry authentication mechanism was effective in preventing all unauthorized access attempts. This was coupled with the implementation of time-sensitive passwords and the requirement of the second user in the process of token management, which made it possible to protect the system from threats such as token interception and replay attacks.
- **Network Disruption Simulation:** In the tests based on the imitation of the network interruption, the usage of the mobile access keys provided the opportunity for authentication in 95% of the cases. This high success rate is quite important because it shows that the system is capable of providing security and operational continuity even if the connectivity is lost.
- **High-Load Scenarios:** The response time of the system proved to be okay even when the system was tested under high-load conditions where several users tried to authenticate at the same time. The average response time was 1. 8 seconds. This performance is within acceptable limits and makes confident that critical operations do not take a knock, particularly during peak usage.

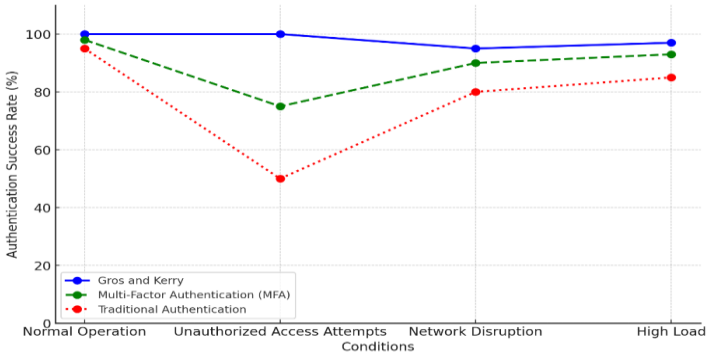


Figure 13: Comparative Success Rates of Authentication Mechanisms

In Figure 13, the success rate of the Gros and Kerry mechanism, traditional authentication system, and MFA systems with regard to the conditions mentioned above. Gros and Kerry's system was designed to requirea shorter response time than the conventional approach, which was established and proved to be almost equivalent to MFA in situations that may have network constraints and a considerable number of users. From the graph, it is also noticeable that SVC, using Gros and Kerry's mechanism of working, is better off producing high levels of security and reliability regardless of the ongoing activities.

The findings of these tests support this hypothesis that the Gros and Kerry authentication mechanism maybe helpful in protecting the functionality of critical systems. This means that in a condition where the bandwidth is low, meaning that the use of the system is low or it is off, in a situation where a number of unauthorized attempts are made to access the place, or in a situation where there is a high number of connections to the system remained secure this made it ideal for use in high secure environments. It also shows that, unlike the classical authentication system, the Gros and Kerry mechanism gets more benefits, especially when reliability and security are the key considerations.

6. LOAD BALANCING

Load balancing is a technique which finds the failure node by link_1 and link_0. failures. Link_1 finds the failure node by network failure or by other means of failure like system failure. Load balancing helps to improve the performance. The balance algorithm assigns to new node with link_1 with identifier PC_{n+1}

Algorithm 3: Load balance

```
Algorithm loadbalance
Speed s
  best come first g
  delay d
fetch memory b
  l=s+g-d-bl
l.state
```

7. DISCUSSION

The Gros and Kerry authentication mechanism has its benefits mainly when applied to critical infrastructure. Its dual-user requirement and time-sensitive passwords offer better security than regular passwords as they minimize the possibility of break-ins. The system must also be capable of working in low bandwidth or offline mode to maintain its functionality when the network is unavailable. Moreover, its use in high-security operations, including the chemical plant, makes it a secure option, especially in security-conscious operations. However, the mechanism does pose some problems, like the working of the double login, where some of the essential operations may be slowed down if the users are not available. Cryptographic tokens involve additional layers of management that are even more sensitive, hence the need for proper essential management to avoid loss or compromise. These are some of the issues that may become more complicated as the system grows big and hence may require some planning and maybe improvements. Future work could be directed to the development of the algorithm by adding adaptive authentication or increasing token security through biometric or quantum encryption. Extending the applicability of the mechanism to other domains, including financial or healthcare, could be helpful in its implementation, as well as the integration with advanced technologies, including Artificial Intelligence, machine learning, and blockchain. However,

the Gros and Kerry mechanism has its advantages, which make it possible to consider it as a rather promising solution for ensuring the protection of the confidentiality of critical activities, and the current research indicates the possibility of further development of the approach that will allow overcoming its existing shortcomings and expanding its potential in the future.

CONCLUSION

In this paper, the Gros and Kerry authentication mechanism has been discussed, and it has been observed that it can be beneficial in protecting multi-cloud applications, particularly the ones used in critical infrastructures.The dual-user authentication technique, in conjunction with time-variant passwords that are generated on the fly, makes the system very secure against intruders. This system is helpful in areas where security is an issue of concern,such as the chemical industries, because, in the event of a breach of security, the consequences are bleak. The fact that the Gros and Kerry mechanism can work under low bandwidth or offline situations also contributes to its strength because it means that something can still go on securely. The practical applications are numerous, especially for industries that require a high level of security, such as the energy, health, and financial sectors. In cases where this authentication method is used as an extra layer of security, it will enhance the security measures against cyber threats that organizations have in place to protect their systems against unauthorized access. Because the system can operate even if the network connection is lost, the system is an integral part of a security system in the areas where the connection is questionable. The authentication mechanism proposed by Gros and Kerry is one f the best solutions for cloud security, particularly for essential applications. However, as the threats are constantly evolving and the world is growing more connected, more research and development are needed. Future developments should, therefore, strive to make the system more effective in addressing the limitations that a current system has, such as the fact that one has to deal with many logins and tokens. As new and more complex threats emerge in the cyber world, it is crucial to establish and launch new security measures such as those implemented by Gros and Kerry to protect critical structures.

REFERENCES

[1] Alam, M., Shahid, M., & Mustajab, S. (2024). Security challenges for workflow allocation model in cloud computing environment: a comprehensive survey, framework, taxonomy, open issues, and future directions. *The Journal of Supercomputing*, 1-65.

[2] Cabot-Nadal, M. A., Mut-Puigserver, M., Payeras-Capellà, M. M., &Pericàs-Gornals, R. (2023). Confidential Certified Notification Protocol using Rejectable Soulbound Tokens and Identity-Based Cryptography. *IEEE Access*.

[3] Carmel, V., & Akila, D. (2020). A survey on biometric authentication systems in cloud to combat identity theft. *Journal of Critical Reviews*, *7*(03), 540-547.

[4] Gholami, M. F., Daneshgar, F., Beydoun, G., & Rabhi, F. (2017). Challenges in migrating legacy software systems to the cloud—an empirical study. *Information Systems*, *67*, 100-113.

[5] Hamdan, S., Ayyash, M., &Almajali, S. (2020). Edge-computing architectures for internet of things applications: A survey. *Sensors*, *20*(22), 6441.

[6] Kreutz, D., Malichevskyy, O., Feitosa, E., Cunha, H., da Rosa Righi, R., & de Macedo, D. D. (2016). A cyber-resilient architecture for critical security services. *Journal of Network and Computer Applications*, *63*, 173-189.

[7] Kumar, A., & Ganapathy, G. (2020). A Novel Collaborative PKI Framework in Public Cloud. *International Journal of Recent Technology and Engineering*, *8*(5), 3135-3141.

[8] Liu, W., Uluagac, A. S., & Beyah, R. (2014). MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data. In *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 518-523). IEEE.

[9] Mishra, S., Awasthi, M., Chandrol, A., Singh, G., & Lande, A. (2024). A Comparison and Analysis of Various Cloud Computing Deployment Models. In *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)* (pp. 1-7). IEEE.

[10] Mohammed, A. H. Y., Dziyauddin, R. A., & Latiff, L. A. (2023). Current multi-factor of authentication: Approaches, requirements, attacks and challenges. *International Journal of Advanced Computer Science and Applications*, *14*(1).

[11] Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. *Applied Sciences*, *13*(19), 10871.

[12] Ouma, G., Awuor, M., Wamuyu, K. P., & Maake, B. (2024). Designing a comprehensive framework for data and network security in cloud computing: case of Kenyan banking industry. *African Journal of Emerging Issues*, *6*(2), 24-45.

[13] Rodrigues, J. J., & Soares, V. N. (2021). An introduction to delay and disruption tolerant networks (DTNs). In *Advances in Delay-Tolerant Networks (DTNs)* (pp. 1-20). Woodhead Publishing.

[14] Sen, A., & Madria, S. (2020). Analysis of a cloud migration framework for offline risk assessment of cloud service providers. *Software: Practice and Experience*, *50*(6), 998-1021.

[15] Singer, P. W. (2001). Corporate warriors: The rise of the privatized military industry and its ramifications for international security. *International security*, *26*(3), 186-220.

[16] Soares, L. F. B. (2013). *Secure Authentication Mechanisms for the Management Interface in Cloud Computing Environments* (master's thesis, Universidad da Beira Interior (Portugal)).

[17] Soveizi, N., Turkmen, F., &Karastoyanova, D. (2023). Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *Future Generation Computer Systems*, *148*, 184-200.

[18] Vignesh Saravanan, K., Jothi Thilaga, P., Kavipriya, S., & Vijayalakshmi, K. (2023). Data protection and security enhancement in cyber-physical systems using AI and blockchain. In *AI models for blockchain-based intelligent networks in IoT systems: Concepts, Methodologies, tools, and applications* (pp. 285-325). Cham: Springer International Publishing.

[19] Wang, J., Qiu, M., & Guo, B. (2017). Enabling real-time information service on telehealth system over cloud-based big data platform. *Journal of Systems Architecture*, *72*, 69-79.

[20] Wang, Y., Su, Z., Guo, S., Dai, M., Luan, T. H., & Liu, Y. (2023). A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects. *IEEE Internet of Things Journal*, *10*(17), 14965-14987.

[21] Wang, Z., Xie, W., Wang, B., Tao, J., & Wang, E. (2021). A survey on recent advanced research of CPS security. *Applied Sciences*, *11*(9), 3751.

[22] Wiefling, S., Patil, T., Dürmuth, M., & Lo Iacono, L. (2020). Evaluation of risk-based re-authentication methods. In *IFIP International Conference on ICT Systems Security and Privacy Protection* (pp. 280-294). Cham: Springer International Publishing.

[23] Wong, F. L. (2008). *Protocols and technologies for security in pervasive computing and communications* (No. UCAM-CL-TR-709). University of Cambridge, Computer Laboratory.

AUTHORS

Binu C T is pursuing PhD in CMR University Bengaluru