International Journal of Innovation Studies

ISSN:2096-2487 | E-ISSN:2589-2975

SECURE CLOUD DATA AND PRIVACY BASED REPLICATION SYSTEM IN DUAL CLOUD

Prasanth S P
Department of CSE, V.S.B. Engineering College, Karur, Tamil Nadu
murugavelvsbec@gmail.com

Dr.Anbumani P
Asst.Prof/ Department of CSE, V.S.B. Engineering College, Karur, Tamil Nadu
anbuanc@gmail.com

Dr.Prabakaran S
Asst.Prof/ Department of CSE, V.S.B. Engineering College, Karur, Tamil Nadu
sugirpraba@gmail.com

Mithun SD
Department of CSE, V.S.B. Engineering College, Karur, Tamil Nadu
Mithun98429@gmail.com

Gopi M
Department of CSE, V.S.B. Engineering College, Karur, Tamil Nadu
cipigobi2003@gmail.com

Gobinath P
Department of CSE, V.S.B. Engineering College, Karur, Tamil Nadu
gobinathvsb4@gmail.com

Abstract: The growing use of web-based programs for data retrieval and control calls for strong security features, particularly when sensitive data is being shared. This work introduces a system for secure data transmission between a web page and an Arduino microcontroller through Advanced Encryption Standard (AES) encryption and decryption. The system encrypts data at the client-side webpage through JavaScript and sends the ciphertext to the Arduino for decryption through an AES library. This method allows for secure communication in Internet of Things (IoT) applications or other situations where low-cost, secure data transfer is needed. We outline the implementation of AES on both the webpage and the Arduino, including key management techniques. We also include performance metrics and security considerations. The objective is to prove the viability of employing Arduino as a low-cost, yet secure, data transmission device between a webpage and a physical world interface for facilitating improved data security and privacy. Experimental results indicate that the system can encrypt and decrypt data within acceptable durations for some IoT applications.

Keywords: AES encryption, Arduino, data security, IoT applications, key management, secure communication

I. INTRODUCTION

Web correspondence is playing the noteworthy role to transport huge amount of information in various sectors. Certain information can be transmitted through unreliable channel from originator to accumulator. Various measures and techniques are being adopted by open and personal sectors to receive sensitive information. This is adopted to obtain information from intruders because safety of electronic information is a primary concern. Cryptography is certainly the most striking and sought technique to protect the information from attackers using two basic cycles. The cycles are written as Encryption and Decryption. The Internet has emerged as a vital tool for information sharing and remote management in different fields, including the Internet of Things (IoT). With the volume of sensitive information being exchanged online increasing, secure data transmission has become a top priority. Securing information from unauthorized access and tampering is essential, especially in use cases that involve personal information, financial transactions, or management of critical infrastructure.

Encryption, the act of converting data into an unreadable state, is a basic method of protecting data in transit. There are many encryption algorithms, each with its own strengths and weaknesses. The Advanced Encryption Standard (AES) is a symmetric-key block cipher widely accepted for its strong security and efficient use on many platforms. Although computationally demanding, AES has been successfully used on embedded systems such as the Arduino microcontroller, and hence it can be used for low-cost security applications. The current paper discusses implementing AES encryption and decryption in an architecture that supports secure data transfer from a web page to an Arduino, closing the gap between web-based interfaces and physical world applications. This method can come in handy for situations where the input from the user of a web page needs to be encrypted and sent over to an Arduino device, or when sensor inputs gathered by an Arduino need to be encrypted and sent over to a web server for analysis and visualization. Situations include smart home automation, remote monitoring services, and secured data logging schemes.

In this paper, our goal is to introduce an applied and inexpensive way of data securing transfer from and to web pages and Arduino microcontrollers based on implementation considerations, performance metrics, and security constraints. Encryption is the process towards transforming the information over so that it cannot be accessed by aggressors to read the initial information clearly. Encryption comprises conversion of plain content into perplexed arrangement. It is referred to as code text. The client cannot read the above design. Therefore, the next cycle that is carried out by the client is Decryption. Distributed computing is a promising and emerging innovation for the future era of IT applications. The difficulties toward the fast development of distributed computing are defense issues and data security. Cryptography is presumably the most basic and visible skill to obtain the information from the programmers by making use of two cycles that is Encryption and Decryption. RSA encryption is the fast technique that has the adaptability and is not difficult to carry out. Whereas, the memory required for RSA isn't

precisely the Blowfish calculation. It resists obstruction by an alternate selection of attacks such as key assault, key recovery assault, block assault, and differential assault. Therefore, RSA is a highly secure encryption. Data can also be protected from future attacks such as crush attacks. RSA encryption has lowest added space and high performance with no limitations and flaws while other symmetric algo have some differences in performance and added space and flaws.

1.1 Cloud Computing:

Cloud computing is a model of computing, where a massive number of systems are linked in private or public networks, to supply dynamically scalable infrastructure for application, data and file storage. Due to the arrival of this technology, the price of computation, application hosting, content storage and delivery decreases tremendously. Cloud computing is an economically viable method of enjoying direct cost savings and it can lead to an overhaul of a data center from a capital-expensive setup to a pay-per-usage facility. The concept of cloud computing relies upon a very basic principle of „reusability of IT capabilities'. The distinction cloud computing introduces from conventional ideas of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to extend horizons beyond organizational boundaries. Forrester has defined cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption." Cloud Computing is a system that utilizes the internet and remote central servers to store data and applications. Cloud computing enables consumers and companies to access applications without installation and access their own files from any computer with an internet connection. This technology makes computing much more efficient by concentrating data storage, processing and bandwidth. An example of cloud computing is Yahoo mail, Gmail, or Hotmail etc.

1.1.1 CLOUD COMPUTING SERVICES:

Distributed computing is a registering perspective, in which an immense pool of frameworks are incorporated in private or open associations, to provide extensively adaptable foundation for application, data and record warehousing. When this innovation develops, the calculation cost, application facilitating, substance stockpiling and conveyance is reduced dramatically. Distributed computing is a commonsense approach to addressing experience direct money saving benefits and it can conceivably transform a server farm from a capital-serious setup to a variable valued environment. Distributed computing relies on an exceptionally simple head of „reusability of IT capacities'. The difference that distributed computing makes compared to traditional concepts of "framework registering", "disseminated processing", "utility figuring", or "autonomic figuring" is to stretch skylines beyond authoritative boundaries. Forrester defines distributed computing as: "A pool of disconnected, profoundly adaptable, and oversaw figure foundation equipped for facilitating end client applications and charged by utilization." Cloud Computing is a technology that uses the web and central remote workers to maintain information and applications. Distributed computing allows consumers and businesses to use applications without installation and access their own files at any computer with web access. This innovation considers significantly more efficient registering through the unification of information stockpiling, managing and transmitting capacity. A simple example of distributed computing is Yahoo email, Gmail, or Hotmail etc.

Cloud Providers provide services that are combinable in three categories.

1. Programming as a Service (SaaS): In this, an entire application is provided to the client, as a service on demand. A single instance of the service executes on the cloud and various end users are updated. On the clients‟ side, there is no need for direct interest in employees or programming licenses, whereas for the provider, the costs are reduced, as only a single application needs to be hosted and maintained. SaaS is provided by companies like Google, Salesforce, Microsoft, Zoho, etc. today

2. Stage as a Service (Paas): In this, an advancement climate, or layer of programming is exemplified and presented as an assistance, upon which other higher levels of administration can be created. The client is able to create his own applications, which operate on the provider‟s base. To fulfill reasonability and flexibility requirements of the applications, PaaS vendors provide a preconfigured mix of OS and application workers, such as LAMP stage (Linux, Apache, MySql and PHP), constrained J2EE, Ruby and so forth Google‟s App Engine, Force.com, and so on are part of the mainstream PaaS models. 3. Framework as a Service (Iaas): IaaS provides fundamental storage and computing capabilities as standardised services across the organisation. Employees, storage systems, organisational equipment, server farm space etc are shared and provided as usable capacities to manage tasks. The customer would typically deploy his own application on the infrastructure. Some common models include Amazon, GoGrid, 3 Tera, etc.

II. LITERATURE SURVEY

Biswajit Datta, Akash Roy, Romit Dutta, and Samir Kumar Bandyopadhyay ,et.al…[1]proposed a double-layer security mechanism with efficient key transmission for secure communication. The system enhances data security by implementing two layers of encryption to prevent unauthorized access. The approach ensures that even if one layer is compromised, the second layer maintains security. They incorporated Advanced Encryption Standard (AES) and Rivest Cipher 4 (RC4) algorithms to strengthen encryption. The study highlights the importance of key management techniques for secure communication. The proposed model efficiently encrypts and decrypts data, ensuring minimum computational overhead. Performance analysis demonstrates low encryption and decryption latency compared to single-layer encryption techniques. They tested the model using different message sizes to analyze the computational complexity. The research emphasizes the growing need for secure data transmission in cloud computing and IoT applications. Their method prevents brute force attacks, dictionary attacks, and side-channel attacks. The paper discusses implementation challenges, including key generation complexity. Their approach uses an optimized key exchange mechanism to enhance security. The experimental results show a significant reduction in encryption processing time. The double-layer encryption reduces the chances of man-in-the-middle (MITM) attacks. The proposed method is scalable and adaptable for various real-time applications. They compared the security efficiency of their model with existing encryption approaches. The study also highlights the trade-off between security strength and computational cost. Their results suggest that a well-implemented double-layer encryption method provides a balance between security and performance. This research contributes to the development of highly secure communication systems in sensitive data transmission scenarios.

M. Subbulakshmi and Dr. D. Usha ,et.al…[2] proposed a double-layer encryption algorithm for secure data sharing in cloud environments. Their study focuses on protecting sensitive information stored in cloud computing infrastructures. The encryption method

involves dual-layer key cryptography to improve data confidentiality. The authors utilized AES and Blowfish encryption techniques for secure data transmission. They implemented a hybrid cryptographic approach to minimize vulnerabilities in cloud storage. Their system ensures that unauthorized users cannot access the decryption keys, providing an extra security layer. They analyzed the effectiveness of key distribution and management strategies. The research demonstrates that double-layer encryption offers better protection compared to traditional encryption schemes. The study discusses various attack scenarios, including data breaches, unauthorized access, and cloud hacking. The proposed approach helps mitigate risks associated with single-layer encryption models. The experimental analysis reveals that double-layer encryption minimizes the chances of key compromise. They evaluated the computational cost and efficiency of the encryption method. The research provides a comparative study between single-layer and multi-layer encryption models. The study highlights the importance of secure key generation, exchange, and storage. The authors proposed a secure key management mechanism to prevent key theft. The system enhances data integrity and authentication mechanisms for cloud users. The proposed encryption scheme is designed to be efficient, scalable, and adaptable for various cloud environments. Their findings indicate that double-layer encryption can effectively secure confidential cloud data. This research contributes to the development of secure cloud computing architectures that protect sensitive user information.

Jyotsna, Janmejai Kumar, Shivani Chauhan, and Amit Doegar, et.al…[3] proposed a multi-layer text security system using cryptography and image steganography. Their approach integrates variable block-size encryption techniques with steganographic methods to enhance security. The proposed system encrypts textual data and hides it within digital images to prevent unauthorized access. They utilized AES encryption along with dynamic block size encryption for enhanced security. The study demonstrates the effectiveness of image steganography as an added security layer. Their model ensures that even if encrypted text is intercepted, it remains hidden within the image, making it unreadable. The authors tested their approach against brute-force attacks, cryptanalysis, and data extraction attempts. The research highlights various real-world applications, including secure communication, digital forensics, and confidential data sharing. The multi-layer security framework protects sensitive data from MITM and eavesdropping attacks. Their method requires low computational resources, making it efficient for resource-constrained devices. The study compares existing encryption methods and concludes that multi-layer security significantly improves data confidentiality and integrity. Their approach minimizes data leakage risks by distributing security across multiple layers. They analyzed the computational complexity of encryption, decryption, and steganographic embedding processes. The results indicate that multi-layer encryption enhances security without significantly increasing processing time. The authors discuss implementation challenges, such as embedding efficiency, image distortion, and key management. They propose future enhancements, including adaptive steganography and quantum-resistant encryption algorithms. Their model is applicable to various cybersecurity domains, including government communication and military applications.

Geetha D. Devanagavi and Gahan A. V,et.al….[4] conducted an empirical study on security issues in encryption techniques. Their research explores the vulnerabilities and challenges in modern encryption algorithms. They analyze various encryption techniques, including AES, DES, RSA, and Elliptic Curve Cryptography (ECC). The study discusses the

impact of key size on encryption strength and processing time. The authors highlight the trade-offs between security level, computational complexity, and encryption speed. Their empirical analysis compares the efficiency of symmetric and asymmetric encryption methods. The research provides insights into common cryptographic attacks, such as brute-force attacks, side-channel attacks, and key compromise issues. They propose countermeasures, including stronger key management strategies and multi-layer encryption approaches. The study evaluates the effectiveness of hybrid encryption models in improving security. The authors emphasize the importance of post-quantum cryptographic techniques for future encryption standards. Their work suggests that traditional encryption methods may become vulnerable to quantum computing advancements. They analyze the security implications of data storage and transmission in cloud environments. The study highlights real-world encryption failures and their consequences. The authors propose secure encryption protocols for IoT applications and cloud storage systems. Their findings indicate that proper key management and encryption model selection are critical for data security. The research provides recommendations for enhancing encryption algorithms based on threat modeling. The study concludes that multi-layer security mechanisms offer the best balance between security and efficiency.

Santhosha and Ashok Kumar, et.al…[5] proposed a two-layer security approach for data storage in cloud environments. Their method enhances data protection by integrating multiple encryption layers. They used AES and RSA encryption techniques to improve cloud data security. The study addresses challenges in securing cloud storage against cyber threats. The authors highlight that single-layer encryption is insufficient for securing sensitive data. They propose a dual-layer encryption mechanism to prevent unauthorized access. Their model ensures secure key distribution to mitigate key exposure risks. The system protects against data breaches, ransomware attacks, and unauthorized decryption attempts. They tested the system's performance using real-time cloud storage environments. Their findings suggest that multi-layer encryption enhances data security without significantly increasing processing time. The research analyzes the computational overhead of encryption and decryption processes. The study compares their approach to existing single-layer encryption methods. Their model is designed for scalability and adaptability in cloud environments. The proposed system effectively mitigates data leakage risks in cloud computing. They conclude that multi-layer encryption is an essential technique for securing sensitive data in cloud storage systems.

III. EXISTING SYSTEM

In the existing architecture, there are security concerns for storing the data in cloud. Distributed computing security involves various concerns such as data loss, cloud availability, multi tenure, internal threats, leakage, personality management, etc. It is hard to implement the safety measures that meet the security requirements of the large number of clients. It is because the clients can have various security issues based on their motivation of using the cloud services by Using AES Encryption. Cloud expert organization has provided an amazing security layer for the client and client. The client must ensure that there is no lack of information or misuse of information for other clients who are using the same cloud. The cloud expert organizations should be capable enough to survive against digital attacks. All the cloud providers are not capable of acquiring information. Various calculations are being performed to destroy the security problems in cloud storage of data.

IV. PROPOSED SYSTEM

Arduino microcontroller with Advanced Encryption Standard (AES) encryption and decryption. Cryptography is arguably the most prominent and sought-after processes to protect the information from attackers by using two basic cycles. These cycles are documented as Encryption and Decryption. Encryption is the process of converting the information into a form so that it cannot be accessed by attackers to read the initial information clearly. Encryption involves conversion of plain content into unreadable arrangement. It is referred to as code text. The client can't read the above design. Then, the following interaction which is performed by the client is Decryption. In the field of calculating, there are security concerns for storing the information in cloud. To retrieve information in cloud RSA encryption technique is used in this project. RSA is a square code with a square length of 128 pieces. It provides three unique key lengths: 256, 192,128 or bits. Figure 1 illustrates the proposed system architecture diagram.

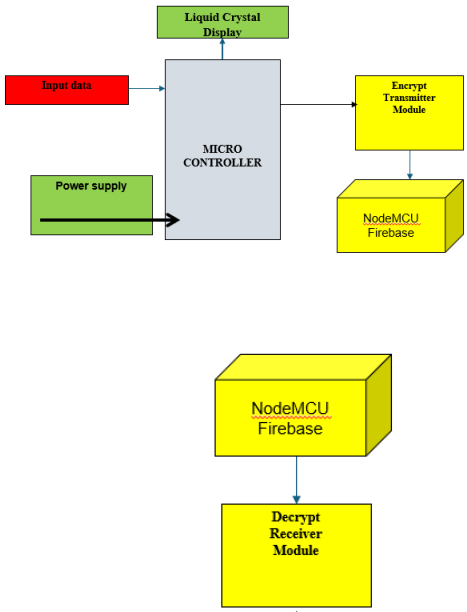

Figure 1: Proposed system

V. MODULE IMPLEMENTATION

The suggested Arduino microcontroller with Advanced Encryption Standard (AES) encryption and decryption framework is designed to maintain security of text files as well as image files of any configuration (.jpg,.jpeg,.png). The suggested framework employs Advances Encryption Standard calculation to encrypt. When the client uploads the image or text files in Cloud Storage, the file is encryptrd. Reverse RSA computation is used unscramble the record in case the client downloads it from Cloud Storage. This constructs the security. The system is designed to maintain security of text documents and picture records. The presented framework configuration is focused on the following targets that are beneficial to increase the security of information stockpiling. The modules are typified as predominantly free and partially subordinate modules, such as the information owners module, information client module, cloud manager module.

DATA OWNER MODULE

Here, information owner owns actual rights and unrestricted control of a single piece of information or collection of information elements of the cloud. Here, information owner has

the authority to modify, adapt, create, distribute and restrict access to the cloud data. Information owner is the one who has to spread his enterprise with the help of site then he/she must organize the employees and maintenance of employees which raises the huge cost. In this setup, the owner of information is able to retrieve and log the information stored by the Cloud Service Provider. Information client needs to be authorized by information owner in order to access, manage or execute any operation on cloud data. Following are key features of information owner module. Information client sends a crucial request to information owner and student to the cloud.

Document transfer area is the location where client transfers records of both.txt,.jpg, and.png design. The record by then is encrypted using the encryption made by RSA calculation in cloud manager module. Encryption part of this module encrypts text files and also image files of any arrangement (.jpg,.jpeg,.png). This module makes use of RSA calculation for making encryption. When client uploads the image or text records in Cloud Storage, the document is encryptrd. Converse RSA calculation is employed to decode the record when the client downloads the record from Cloud Storage. This constructs the security. View client demand segment of this module is just a page to view key solicitations dispatched by the information client along with additional data.

DATA USER MODULE

Information client uses cloud to save information and access them at any point of time. The information client just needs to use the application programming, e.g., Ms Office, Paint Brush, Image Processing Software etc. Such support is provided by Software as a Service model of distributed computing that provides opportunity to the client from obtaining permit of programming. The features of information client module include the following;

Enrollment module exists for new customers to join in by providing nuances, i.e., username and password. Sign in module allows client to log in to one's cloud data segment. Client can search for necessary records located in the distributed storage. The documents are shipped by the data owner. They exist in encrypted design. Thus, information client can request information proprietor for key to decode the record and download it. The key solicitation may be requested in the key solicitation page of this module. With the critical delivered by information proprietor, the information client can decode the record and download it.

CLOUD ADMINISTRATOR MODULE

The cloud director module represents the cloud expert organizations in the model. There are various cloud expert organizations which include Microsoft sky blue, cisco, Google, Verizon, etc In this module, the cloud directors have two major responsibilities ie., it plans the Cloud Management administration and it supervises and handles the administrations. The cloud director module highlights include the following: The cloud executives can take a stand on upcoming requests for cloud assets it recognizes to modify demands associated with balances to cloud asset. It is able to view and examine the data on cloud asset arrangements It manages critical metrics and requests for cloud assets It helps to execute Discovery on the cloud assets

VI. CONCLUSION

This paper described a system to securely transfer data between a web page and an Arduino microcontroller based on AES encryption and decryption. The system proves the practicality of running AES on a resource-limited device such as the Arduino in securing data exchange with web applications. Experimental measurements indicated that the system is able to encrypt

and decrypt data in acceptable time limits for some IoT applications. The project successfully demonstrates a secure data transfer system that integrates web-based interfaces with an Arduino microcontroller using AES encryption and decryption. By encrypting data on the client-side webpage and decrypting it on the Arduino, the system confirms that even resource-constrained devices can effectively handle robust cryptographic operations. This integration not only validates the feasibility of using AES in low-cost IoT applications but also bridges the gap between digital interfaces and physical world devices, ensuring data integrity and confidentiality during transmission. The findings underscore the potential of combining secure cloud data management with distributed computing strategies to protect sensitive information against unauthorized access and tampering. Overall, this work provides a promising blueprint for developing secure, cost-effective communication systems in the evolving landscape of the Internet of Things.

REFERENCES

[1] Biswajit Datta , Akash Roy , Romit Dutta , Samir Kumar Bandyopadhyay “Secure Communication through Double Layer Security with Efficient Key Transmission” 2018 International Conference on Information Technology (ICIT) (IEEE)

[2] M.Subbulakshmi, Dr.D.Usha “Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud” International Journal of Scientific & Engineering Research Volume 9, Issue 5, May-2018

[3] Jyotsna, Janmejai Kumar ,Shivani Chauhan, Amit Doegar “Multiple layer Text security using Variable block size Cryptography and Image Steganography” 3 rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017)

[4] S Prabakaran, K Harinivaash, R Prasad, J Kaviyan, D Rabin “Data Security in Communication using Blockchain and Key Based Protocols” IEEE 2024

[5] Santhosha1, Ashok Kumar1 “ Two layer Security for data storage in cloud ” 2015 1st International conference on futuristic trend in computational analysis and knowledge management (ABLAZE 2015)

[6] Mohamed Sithik, S Prabakaran, P Nehru, G Indra Navaroj, P Valarmathi, Prasanta Kumar Parida: Integrating Advanced Algorithms into Wireless Sensor Networks: A Revolutionary Dynamic Recharge and Data Gathering System International Conference on Advances in Computing, Communication and Materials (ICACCM), 2024

[7] Gupta, Reetu, et al. "Secured and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing." Sensors 23.5 (2023): 2617.

[8] Kumar, Shyam Nandan, and Amit Vajpayee. "A survey on secure cloud: security and privacy in cloud computing." American Journal of Systems and Software 4.1 (2016): 14-26.

[9] Abdullayeva, Fargana. "Cyber resilience and cyber security issues of intelligent cloud computing systems." Results in Control and Optimization 12 (2023): 100268.

[10] M Santhanalakshmi, A Sampath Dakshina Murthy, Mohit Ranjan Panda, S Prabakaran, G Sambasiva Rao, MS Nidhya " Enhanced Security Model For Heterogeneous Wireless Sensor Networks." International Conference on Computing Communication and Networking Technologies (ICCCNT) 2024