Proceedings of the 4th International Conference on Computing and Data Science (CONF-CDS 2022)
DOI: 10.54254/2755-2721/2/20220678

Defense communication system AWS

Prakruthi P[1] , K Yashawanth[1], Chethan D[1], Bhuvan Kumar[1] Chandana N[2],Divya C D[2,3] and Radhika A D[2]
[1]Student, Vidyavardhaka College of Engineering Mysore, India;
[2]Assistant Professor,Dept of CSE, Vidyavardhaka College of Engineering Mysore, India

[3]divyacd@vvce.ac.in

Abstract. AWS is an upcoming technology along with decentralized infrastructure. This knowledge is employed in variety of different domains including cloud computing, finance, energy, messaging and others. AWS really takes up vital part in military message passing which enables certainty and safety of messages by dodging changes created to data that is collected in blocks. AWS needs the access where each user is an authorized user. In this paper we will be proposing different cryptographic techniques along with AWS technology to ensure safe and secure passage of messages between different teams in the defence sector.

Keywords: Shamir's algorithm , AES Rijndael algorithm, Q R code image & AWS S3

1. INTRODUCTION

With rapidly developing and propaganda of the expertise with respect to blockchain which has shown enormous growth, AWS helps to protect digital_messaging system,messaging data from one to another, using cloud computing. These are the essential uses of AWS. Data encryption is the main purpose or the advantages of AWS. Also, once original data is being delivered from one node to the other, it should be in the encrypted setup and it must also have integration among source and end users wherever nodes may not trust the unwanted materials thus presenting a response for the problems regarding price, ineffective outlook, and data storing risk that succeeds in intensive firm. It is hard to confess that the encryption in military enterprise have considerably weak encryption standards and it is definitely not advisable. Anyhow, in each use case scenario, it's viable that they might integrate an area of automation due to AWS cryptographic encryption, decreasing price of oversight for email. Anyway, there are various kinds of inter department as well as in field trade-off.

2. LITERATURE SURVEY

Cloud records source is metadata which documents the steps of the generation and functions carried out on a cloud data object. Safe data provenance is essential for data liability, forensics ,privacy and security. In this paper, they have proposed an open and trusted cloud data provenance framework using blockchain. A Blockchain related Data Provenance Architecture in Cloud. The takeaways of this paper are some advantages that include Data Security, Data Privacy, Tamper-proof Blockchain. The disadvantages of the proposed system is the use of cloud storage applications that have very less security [1].

© 2025 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2/20220678

Blockchain is an emerging technology with decentralized infrastructure. This technology is applied in all domains involving banking and finance, ,messaging and many. Blockchain plays a critical role in military message passing that guarantees safety and security of messages by preventing manipulations made to data that is stored in blocks. Consortium blockchain entails the permission where every user is an authorized user. The main issue is Distributed Consensus in the current system of Proof of Work algorithms. So at this point we have consortium blockchain technology is suggested on "MESSAGE PASSING TECHNOLOGY" in a military messaging system named HPBC. This algorithm will work well on an asynchronous network that gives the results with great performance and analysis[2].

Blockchain creates a blind trust situation where an user can trust in the yields of a given system without believing in any user within it . We have used the above concept and taken this as the main reference for our project but we aren't going to use blockchain technology as it requires a lot of hardware equipment that is hard to source.

Security infringes flexible users' privacy call into matter the current standard, where third parties gather and manage large quantities of personal data. Bitcoin has shown in the crypto industry that trusted, auditable computing is feasible by making use of decentralized network of peers together by a public ledger. This process is also called the Proof of Work[3]. Here the authors have described a decentralized personal data management system that make certain users own and manage their data efficiently.They have also implemented a protocol that transforms a blockchain into an automated access control manager that won't trust in any third party. Unlike Bitcoin, transactions in their proposed system which may not be mandatorily financial. They are utilised to follow instructions, such as storing, querying and sharing data. Advantages of the proposed system include Data Ownership-Control/Permissions by users,data transparency and auditability.We also have fine-grained Access Control to avoid third-party services.Disadvantages of these can be the use of Mobile Based applications which can be less secure and not so reliable for the use of this technology.

Cyber-physical-social system (CPSS) lets users give out personal information gathered from both cyberspace as well as physical space. This results in making huge amounts of data in the regional storage[4]. Though, it is not feasible. Many programs suggested to permit a third party audit to authenticate data cohesion utilizing the public keys of the users. The majority of the programs hold a robust assumption that the audits are good and reliable, and thus are unsafe when auditors are malicious. Also, in most of these programs, an auditor should manage users certificates to pick the proper public keys for authentication. Here, they have proposed a secure certificateless public integrity verification scheme (SCLPV). The SCLPV is an exclusive work that concurrently supports certificateless public verification,authentication and opposition against melevolent auditors to authenticate the solidarity of deployed data in the cyber physical social system[5]. A formal security proof proves the rightness and safety of their proposed scheme. In addition, a detailed execution analysis determines that the SCLPV is well organized and practically applicable. Associated with the only current certificateless public verification scheme , the SCLPV offers more robust security in terms of resolving the security liability of the CLPV and opposition against malicious auditors. Advantages of this system that we have observed that can be a takeaway are extended data security and data privacy. Disadvantages of the system include that the blockchain is not used and it is not tamper proof and also there is no Encryption/Decryption of data[6].

3. EXISTING SYSTEM

The key concern comes with Distributed Consensus in the existing system of Proof of Work algorithm. The Proof Of Work is a prevailing blockchain , to enable correct implementation, it waits an encounter with the hash problem. So every block will have to queue the six subsequent blocks to confirm. This is time and energy consuming.

DRAWBACKS:

- Misuse of Government information.
- Tedious to manage a huge bulk of data.
- Time consuming.

DOI: 10.54254/2755-2721/2/20220678

4. PROPOSED SYSTEM

Data security is among the most crucial aspects in defence sector. There would be numerous features which has to be safely maintained and it is essential that it shouldn't be known to commoners who are residing in the same territory. The features such as types of teams employed in a particular team such as war engagement unit, hospitality unit, weapon producing/distribution unit, handling the criminal data and functioning and these data has to be moved from one command to another. So, the proposed system using Shamir's algorithm,AES Rijndael algorithm,QRCode Image & AWS S3 service plays a crucial role in ensuring safety to this kind of data without changing the data.

ADVANTAGES:

- Security is achieved
- Enables Privacy
- Easy access and retrieval
- Cost effective

5. METHODOLOGY

The methodology consists of two sides- the sender side and the receiver side. We can see from figure1 that there are two sides namely MT-1(Military transmission 1) and MT-2(Military transmission 2).

The main objective of this process is to encrypt the message that we want to send to the other side of the system. To achieve this we use two algorithms called AES(Advanced Encryption Standard Algorithm) and Shamir's algorithm.

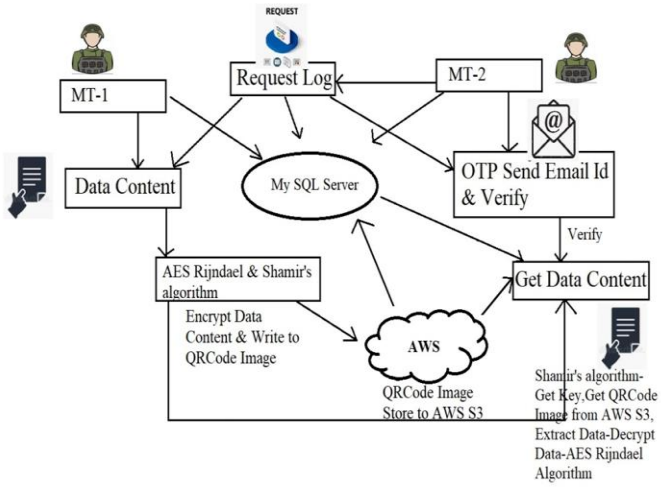

Figure 1. Workflow of proposed system

5.1. AES rijndael algorithm

In the rijndael algorithm, encryption takes place through a sequence of matrix transformations. The total rounds are dynamic that depends upon the key or block sizes.

128 bit uses 9 rounds,192 bit uses 11 rounds , 256 bits uses 13 rounds. The rijndael algorithm is based on byte by byte restoration, swapping or XOR action.

The algorithm creates ten 128 bit keys from the 128 bit key stored in 4x4 stables. The plain text is partitioned into 4x4 tables each of 128 bit sizes. Each 12 bit plaintext experiences a varying number of rounds. The code is created after the 1th round. Each round contains 4 steps namely- Byte sub,Shift row,Mix column,Add round key. When the rijndael is executed numerous times with varying round keys, its safety is increased.

DOI: 10.54254/2755-2721/2/20220678

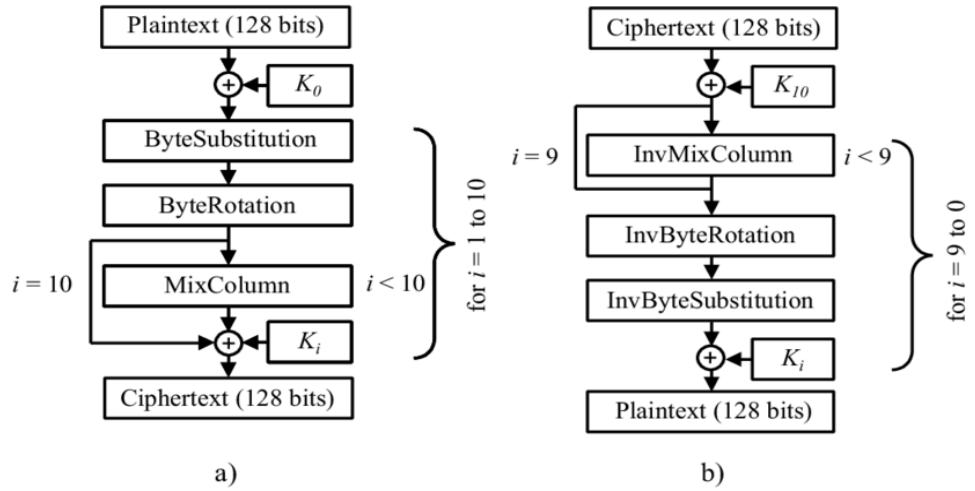

Figure 2. Working of AES

5.2. Shamir's algorithm

Shamir's Secret Sharing (SSS) is employed to secure a secret in a distributed way, most often to secure other encryption keys. The secret is split into multiple parts, called shares. These shares are used to reconstruct the original secret during decryption.

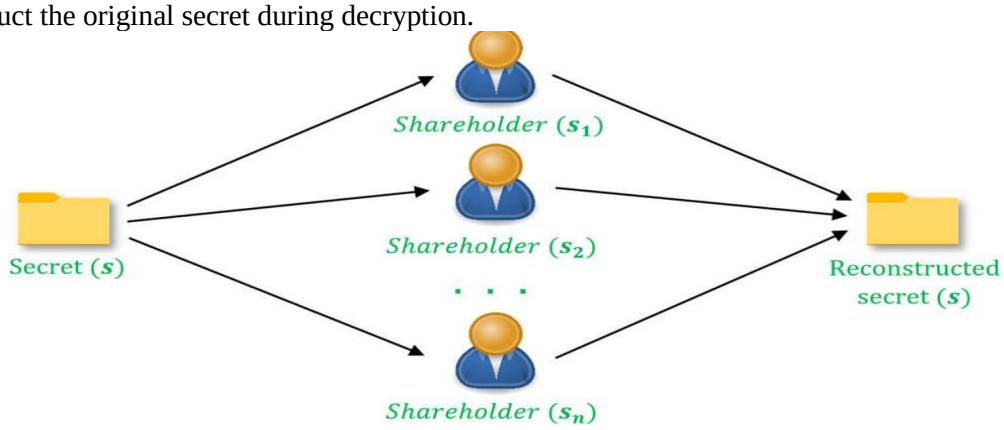

Figure 3. Shamir's algorithm

5.3. Sender Side

The aes algorithm is run and the key is generated in this process. The process of encryption is started here where the data content is encrypted.The encryption takes place due to a series of matrix transformations in the aes algorithm. The encrypted data is stored as QRcode Image. The QR code image is then stored in the AWS S3 cloud storage for secure storage. Amazon Simple Storage Service (AWS S3), is the most rudimentary and world wide Infrastructure as a Service (IaaS) solution given by Amazon Web Services. Using Amazon S3 expidites extensible, secured and minimum latency data storaging from the cloud. With its easy to use web service interface, it is unchallenging to store and recover data on Amazon S3 from anywhere on the web. We just have to choose a region create a S3 bucket,name it and start storing data.

The key is now split into multiple shards by the process of sharding by shamir's algorithm. This ensures extra security for the key to not be found by any external agent.

DOI: 10.54254/2755-2721/2/20220678

5.4. Receiver side

The MT2 sends a request log to the application. To verify their identity an OTP mail is sent to their registered email id using SMTP protocol. The key is then reconstructed by the shamir algorithm as the key is essential in the decrypting process of the data. So now the QR image stored in the AWS is extracted and encrypted data is read. This is encrypted data that has to go through the decrypting phase using the AES algorithm and its key again. Once this process is completed the message is received in a readable format by MT-2.

6. CONCLUSION

This research proposes a constructive way to ensure safety and security of transfer of messages between different teams in a defense organization using the cryptographic techniques explained above. The message passed between different teams in an organization is highly confidential and sensitive for external agents to access them. This may turn out to be a risk for national security. Hence using our proposed methods, there is a huge possibility to reduce these types of risks associated during message passing in the defense sector.

References

[1] Kavya K R and Smt. Kavitha M ,Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020) IEEE Conference Record ,IEEE Xplore ISBN: 978-1-7281-5371-1,Military Message Passing using Consortium Blockchain Technology.

[2] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla,2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability.

[3] Guy Zyskind, Oz Nathan ,Alex 'Sandy' Pentland,2015 IEEE CS Security and Privacy Workshops Decentralizing Privacy: Using Blockchain to Protect Personal Data.

[4] Yuan Zhang, Chunxiang Xu, Shui Yu, Hongwei Li, Member, IEEE, and Xiaojun Zhang

[5] IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS, VOL. 2, NO. 4, DECEMBER 2015,SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors.

[6] Sweeney. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570,k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY

[7] Karim El Defrawy, Joshua Lampkins ,Founding Digital Currency on Secure Computation,November 2014.