A Novel Authentication Protocol for Securing Cloud Database

[1]Jasmine Samraj, [2]K.Abirami

PG & Research Department of Computer Science
Quaid-E-Millath Government College for Women(A),
Chennai, India.

Abstract: Cloud computing has improved the flexibility and speed of software development process, but it also Contributed to a rise in security attacks. Cloud computing has increased theflexibility and speed of software development, but it has also contributed to an increase in security attacks. Employees in Cloud organisations who manage data may be the target of insider attacks, which could harm their reputation. They have the benefit from the ability to access user data by engaging withthe authentication system. Cloud database has developed an innovative technology that delivers compelling data integrity characteristics development to provide security in terms of confidentiality, integrity and authenticity. The primary goal ofthis research paper is to present a new secure authentication mechanism for Cloud Database technology. An insider Changing the user login credentials details during the user authentication process is made more difficult by the Cloud Database. The mechanism of proposed algorithm have been provided to show their applicability and accuracy. On theAuthentication formal system tool, the proposed method is tested for resistance to impersonation, no-replay attacks, denial-of-service and offline guessing of cybercrime.

Keywords: Cloud Database, Insider threat, Outer threat, Cloud computing, Access control, Hash value, Timestamp value, and Nonce value

I. INTRODUCTION

The rapid expansion of networks and cloud computing has raised serious concerns about data security. Methods for protecting data from tampering, fabrication and interception have evolved into a critical concern. The cloud database contains a significant amount of data. Users can save, change, and retrieve data from any locationin the world. As a result, maintaining privacy in cloud databases is critical.[2]. The most dangerous threat to various companies like Yahoo, Facebook, and Google is the insider threat. The cost of datarecords lost due to insider attacks is more than the cost of records lost due to outsiders, as proved by Richardson et al. [3]. This is dueto the fact that insiders are aware of the system framework's target.

profitable records, although outsiders do not obtain the informationframework's target profitable records, although outsiders do not obtain the information architecture, the information that is accessible [4].
An insider was involved in 26% of all computer crimes, according to 2016 Cybercrime survey of US states[5]. Furthermore, roughly one third of those respondents believed that insider attacks were more dangerous than outside attacks. The movement of data to the cloud may increase the number of an insiders, raising the danger ofinsider threats.

New security measures also necessary to safeguard unauthorised data from insiders who know how and where the data is stored within the organisation. Various algorithms were utilised to securecloud data from insider attacks. Although these algorithms do not protect the data from unauthorised users who abuse their privilegesto threaten the system's security, they do protect data from malicioususers. Due to the increasing demands that insiders may place on data, developing an algorithm to secure data from insiders has become critical.
(1) An insider can quickly guess the user's password. (2) Google Authenticator's two-factor authentication method (GA) sends codesto users through Short Message Service, which is risky because a security violation might result in the loss of all user Authenticationcodes, [24],(3) GA as well as other third party authentication applications (TPAA) manage all of their authentication codes witha unique identity, which increases their vulnerability[25].

A. Motivation

The research paper employs a Cloud Database technology as it is open and general to solve the loopholes above mentioned. Cloud Database operates in a decentralized manner, with the chain being completely public and storing no

sensitive information. An insideris unable to alter the user's authentication information. All of CloudDatabase's previous nodes must be altered in order to make changesto any existing node. Cloud Database-based authentication is beingused for cloud database services that end users can access

B. Research Contribution

A novel authentication technique based on the cloud Database is proposed for restricting and managing insiders onthe cloud

The following contains the contributions of the proposed work:

- The proposed method authenticates both insiders and outsiderssystem attacks.
- Cloud Database technology offers the cloud database user peer-to-peer authentication.
- Authentication formal system tool for analysing system performance shows that the proposed mechanism is strong and secure.

The following show the research paper is organised: -. The researchpaper is organised as follows: -. Section 2 focuses the authentication technique for insiders and cloud users. Section3 contains the recommended methodology by utilising the Authentication formal verification tool. Section 4 the paper is concluded.

II. PROPOSED CLOUD DATABASE AUTHENTICATIONMECHANISM

This section describes the Cloud Database authentication protocol as well as proposed authentication standards for both insiders and database cloud users.

A.Literature Survey

Zheng et al. [15] emphasised the significance of the Cloud Database method. According to the author, Cloud Database can improve system speed by removing the limits on numerous applications that exist in current technology. The author discoveredthat Cloud Database may also be used for user authentication. TheCloud Database employs a Cloud Database ID that is bound by a public key and grants the specified user access to the private key. The user signatures helped validate the public key, which is storedin the Cloud Database ID.

Minoli et al. [16] applied the Cloud Database in an IoT-based healthcare system with varying degrees of security. The author claims that,the linked list of blocks in Cloud Database was resistant to changes to existing data. It removed the necessity for authenticationfrom a trustworthy third party. Furthermore, when the peer- supported state of the distributed ledger and network is not centralised in distributed systems, it operate as a peer-to -peer system. The Cloud Database technique is decentralised, which provides various advantages over traditional authentication approaches, including the ability to follow the user's previous records and activities, as discussed in the value ofthe Cloud Database mechanism.

Each Cloud Database node is further composed of elements that operate on a variety of parameters. The genesis block which is theCloud Database's initial node/starting node, as well as the index node value and all preceding hashes are set to zero. The Timestampshows when the node was created, whereas the current hash value stores a predetermined value. The Index value represented the current block nodes position in the chain. The data or digital data fingerprints are uniquely identified by the Hash value's length andAlphanumeric value. A proper hash should have three digits that are all zero. In addition, the same data value was assigned to the same hash value every time.

B.Cloud Database Mechanism with Overall Framework

The Transformation of hash value to Data value is Computationallyimpossible. Equation(1).describes how to use a hashing function tocompute the current hash value

Hashing Function (Index Value+Previous Hash Value+TimeStampValue+Data +Nonce Value)= Current Hash Valiue.

To generate a valid hash, the Nonce value is used. As a result, it is critical to identify a Nonce value that produces a valid hash result, when it is combined with the remaining data from that block. The credentials of the user are then stored in the Cloud in order to authenticate users on the database. The Cloud Database Mechanismprevents any disclosure of user data. The user's login information ismaintained and authenticated in a cloud database at several stages inthe cloud database's peer -to-peer architecture. Cloud Database finds a wide range of applications in numerous areas [19-34].

The overall framework for the current user request is authenticatedto the cloud database as shown in Figure 1.

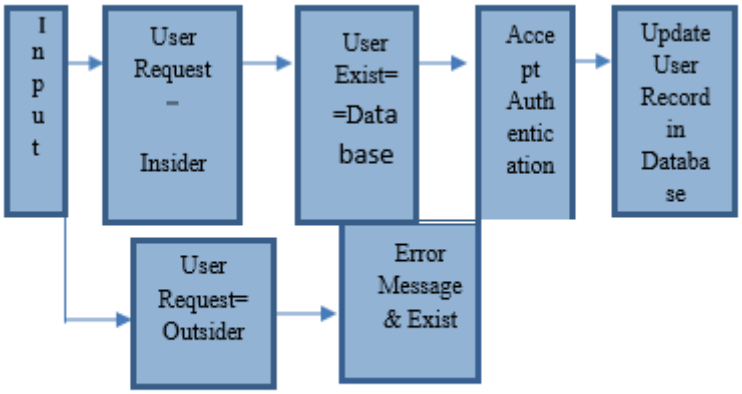

Fig 1: Cloud Database Authentication

Algorithm1 Using the Cloud Database Mechanism for User Authentication.

Input: Cloud Database Server received request P, it determines whether the request is coming from either an insider (Alice) or an outsider.

Output: Access is either allowed or refused

Step 1: If Request == Authenticate user

Step2: If Login ID & User Signature== Valid
{
If the current index value is greater than the Last Stored Index Value, Hash Value, Timestamp Value and Nonce Value are all valid.

Create NewNode and Grant Authentication.

Else
Step 3: If User ## Exist in Cloud Database
{
then Goto Step 1
Else
Add a new Node user
Set the Index Value
Set the Current Timestamp Value
Store Current Hash Value has a predefined value. Save the Data Value
Provide a correct Nonce Value
in the Cloud Database, update the User Record.
}
Else
Give Error Message and Exit
}
Else
If Outsider==User Goto Step2
Else
Goto Step3

Endif

The Algorithm1 Highlights the critical points of the Proposed Cloud Database Authentication Mechanism. It deals with both of inner and outer users. The algorithm demonstrates that it verifies user credentials before examining the proper Cloud Database node specifications. If the cloud database does not include the user's credentials information, the user is prompted to retry or create a new user account to check that Proof that the algorithm is correct.

III. RESULTS & ANALYSIS

The formal method Authentication tool was used for experimental testing with UNSWN15 dataset. The tool makes it easier to experiment with a limited and unlimited number of sessions. All security protocols are automatically verified by authentication tool. The Dolev-Yao model forms the basis of Authentication Advisory model [35].

A promise made by one party to another is referred to as a commitment. Secret is used to achieve confidential user data. A session variable called Nonce Value ensures that no previous value is used again. These security requirements are validated using an authentication tool. It is possible to make the conclusion that the proposed solution overcame the common principal threats, compiled with essential security standards and operated extremely efficient. Additionally, it may show that the proposed user authentication method withstands every security attacks and that no security attacks was observed to be within its bounds. It also make sure that automatic claim has validated the protocol's operation.

Table 1 provides comparisons between the Proposed Cloud Database Authentication and other Cloud Database techniques.

Tools/ Attacks	Guessing Attack	InsiderAttack	Impers onation Attack	ReplayAttack	DOS Attack
Protocol Verificationet al.[8]	75%	78%	80%	75%	74%
MultiFactorAuthentication et.al[9]	78%	75%	73%	73%	75%
Smartcard Authentication et.al[11]	79%	70%	72%	76%	73%
Privacyaware Authentication et.al[12]	74%	79%	74%	70%	70%
Dual Authentication et.al[13]	75%	70%	75%	71%	75%
Proposed Authentication	90%	95%	94%	93%	97%

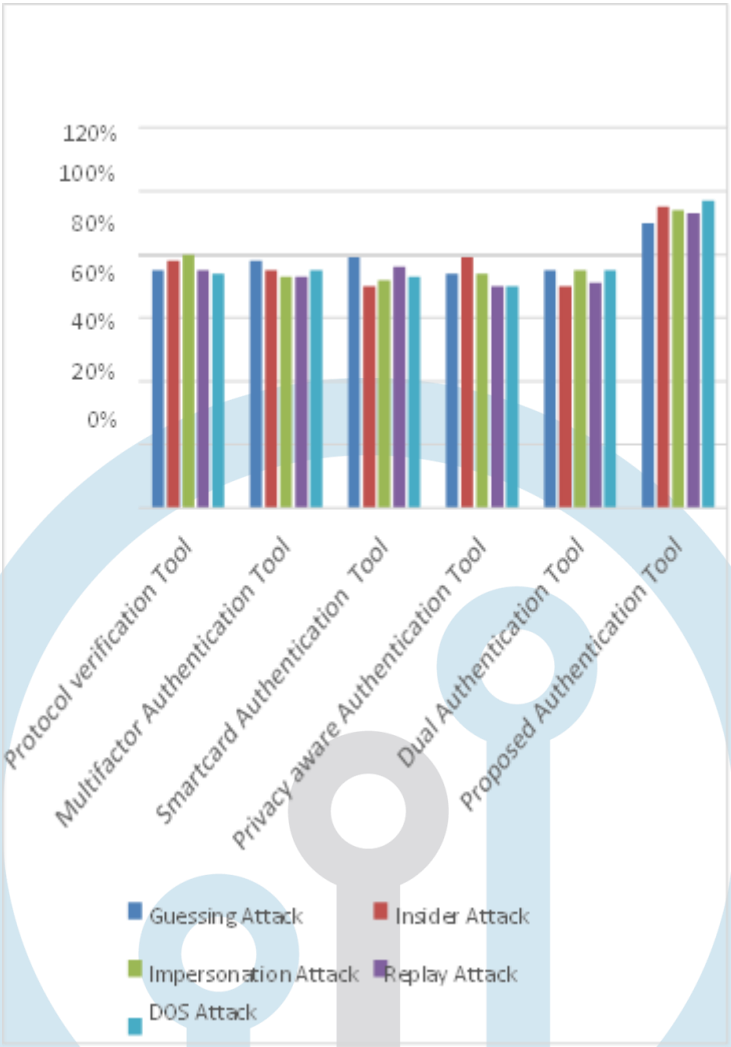

Fig. 2. Comparative analysis of existing algorithms with proposed system

From this it is proved that, the table and graph describes that the proposed method overcomes the well known primary attacks and security requirements are highly efficient in operation.
It is also proved that the proposed solution withstands above mentioned attack whereas the existing method do not focus in all the attack simultaneously. It also verifies that the working of the authentication protocol has successfully achieved the automatic affirmations.

IV .CONCLUSIONS

The research paper identified security attacks and proved that insiders and outsiders can able to bypass Cloud database Authentication systems. Furthermore, a Cloud Database authentication mechanism to counterfeiting both internal and outsider threats is proposed. Cloud databases provide a variety of advantages in terms of authentication, because it is unchangeable and user data is preserved in a protected list. Cloud Database is a promising technology that will likely find new additional applications in the future. [36–38].

The authentication formal system tool is used to test the proposed system's to evaluate the performance against a variety of attacks. The outcomes indicate that the proposed strategy is extremely effective and benefical in eliminating a variety of internal and external threats.It also increases the cloud environment Depending on the user privileges, a distinct set of authorization rules can be issued to each group of users. In the future, development will be more focused on authorization policies that combine with authentication rules to provide the necessary user privileges and improve user access control by enabling user control and monitoring.

The proposed authentication system is robust used in real time working situations using the claims.

REFERENCES

1. Ashok Gupta, Shams Tabrez Siddiqui, Shadab Alamand Mohammed Shuaib "Cloud Computing Security using Cloud Database" in Journal of Emerging technologies and innovative research ,Vol 6, June 2019
2. Zondga Wu,Guandong Xu,Enhong Chenb,Guiling Lid,"An Efficient approach for the protection of privacy text data in the Cloud DB World Wide Web 2018,21,915-938.
3. Adam james Hall,Nikolaos Pitropakis,William J Buchanan," Predicting malicous Insider Threat Scenarios Using Organizational Data and a Heterogeneous Stack Classifier", arXiv: 1907.10272v1[CS.CR] 24 Jul 2019.
4. Insider threat 2018 Report. Availabel online: https:www.ca.com/content/dam/ca/us/files/book/insiderthreat-report.pdf (access on June 2019).
5. Tarunpreet Bhatia,A.K.Verma,Data Security in mobile Cloud Computing paradigm:A survey taxonomy and open research issues in the Journal of SuperComputing 73,2558-2631 in Jan 2017.
6. Bhatia.T,Verma A.K,Data security in mobile cloud computing paradigm.A survey ,taxonomy and open research issuses.Journal of SuperComputing 2017,73,2558- 2631[CrossRef].
7. Current state of Cybercrime 2018. Availabel online: https://www.rs.com/content/dam/premium/en/whitepaper/201 6-current-state-of-cybercrime.pdf(access on march 2019)
8. Jia-Lun-Tsai,Nai-Wei Lo,"A Privacy -Aware Authentication Scheme for Distributed Mobile Cloud Computing Services in IEEESystem Journal DOI:10.1109/JSYST.2014.2322973.
9. [9].Ta-Chih Yang,Nai-Wei Lo,Horing-Twu Liaw & Wei ChenWu,"A Secure smart card Authentication and Authorization framework using in Multimedia Cloud.In Multimedia tools Applications 76,11715-11737 in April 2016.
10. Saru Kumari,Karuppiah ,Ashok Kumar Das,"A Secure Authentication Scheme based on Elliptic Curve photography for IoT and Cloud Servers in Journal of Supercomputing 74,6428- 6453 in April 2017.
11. Shajina A.R,Varalakshmi .P,"A Novel Dual Authentication Protocol(DAP) for Multi-Owners in Cloud Computing in ClusterComputing 20,507-523 in Feb 2017.
12. Anakath A.S,Rajkumar.S,Ambika .S,"Privacy-Preserving multi- factor authentication using trust management " in Cluster Computing in Sep 2017,1-7
13. Chaudhry S.A,Kim I.L,Rho S,Farash ,M.S,Shon T,"An Improved anonymous scheme for Distributed Mobile Cloud Computing Services" in Cluster Computing 22,Pages1595-1609 in 2019.
14. Cresitello Dittmar B,"Application of the Cloud Database For Authentication and Verification of Identity "In Cluster Computing 2016.
15. Zheng Z,Xie S,Dai H,Chen X,Wang H,"An Overview of Cloud Data base technology: Architecture, Consensus and future trends" in 2017 IEEE International Congress on Big Data IEEE:Piscatway,NJ,USA,2017;pp.557-564.
16. Minoli D,Occhiogrosso B,"Cloud Database Mechanisms for IoT Security ", in Internet of Things 2018,1,1-13.
17. Niranjanamuruthy,Nithya B.N,Jagannatha S,"Analysis of Cloud Database technology Pros,Cons,and SWOT " in Cluster Computing 2018,1-15.
18. Zheng B.K,Zhu L.H,Shen M,Gao F,Zhang C,"Scalable and Privacy-Preserving data sharing based on Cloud Database " in Journal of Computer Science Technology in 2018,33,557-567.
19. Tian H,He J,Ding Y,"Medical Data Management on Cloud Database with Privacy", in Journal of Medical System in 2019.43,26.
20. Ryu J.H,Sharma P.K,Jo J.H,Park J.H,"A Cloud Database- based decentralised efficient investigation framework for IoT digital forensics,"In Journal of SuperComputing in 2019,1-16.
21. Knirsh F,Unterweger A,Engel D,"Privacy-Preserving Cloud Database -based electric vehicle charging with dynamic tariff decisions" in Computer Science-Research and Development in 2108,33,71-79.
22. Mengelkamp E,Notheisen B,Beer C,Dauer D,WEinhardt C,"A Cloud Database-based smartgrid:Towards sustainable local energy markets" in computer Science-Research and Development in 2018,33,207-214.
23. Zegzhda D.P,Moskvin D.A,Myasnikov A.V,"Assurance of Cyber Resistance of the Distributed Data Storage Systems Using Cloud Database Technology " in Automatic and Control Computer Science in2018,52,1111-1116.
24. Dasgupta D,Shrein J.M,Gupta K.D,"A survey of Cloud Database from the Security perspective" in Journal of Bank and Finance Technology in 2019,3,1-17.
25. Huh Jun,Seo K,"A Cloud Database-Based Mobile Fingerprint verification and automatic login Platform for Future " in Journal of Super Computing in 2019,75,3123-3139.
26. Naga Subramanian G,Sakthivel R.K,Patan R,Gandomi A.H,Sankayya M,Balusamy B,"Securing e-health records using keyless Signature infrastructure Cloud Database in the Cloud" in Neural Computing in Applications in 2019,1-9.

27. Xue J,Xu C,Zhao J,ma J,"Identity -Based public auditing for Cloud Storage Systems against malicious auditors Via Blockchain in China Information Science in 2018,62,32104.
28. Lee B,Lee J.H"Cloud Database Secure firmware update for Embedded devices in an Internet of Things Environment " in Journal of SuperComputing in 2017,73,1152-1167.
29. Yu Q,Meeuw A,Wortman F,"Design and Implementation of a Cloud Database multi Energy System", in Journal of Energy Information 2018,1,17.
30. Malomo O.O,Rawat D.B,Garuba M,"Next Generation Cybersecurity through a Cloud Database -enabled federated Cloud Framework" in Journal of SuperComputing 2018,74,5099-5126.
31. Alltulyan M,Yao L,Kanher S.S,Wang X,Huang C,"A unified Framework for Data integrity Protection in people -Centric Smart Cities" in Multimedia Tools and Applications in 2019,1-14.
32. Reyna A,martin C,Chen J,Soler E,Diaz M,"On Blockchain and its Integration with IoT.Challenges and opportunities " in Future Generation Computer Systems in 2018,88,173-190
33. Reyna A,martin C,Chen J,Soler E,Diaz M,"On Blockchain and its Integration with IoT.Challenges and opportunities " in Future Generation Computer Systems in 2018,88,173-190.
34. Chen G,Xu B,Lu M,Chen N.S " in Exploring Cloud Database Technology and its potential applications for Education "in Smart Learning Environment in 2018.
35. Amadio R M,Charatonik W,"On Name Generation and Set- Based analysis in the Dolev-Yao-Model" in International Conference on Concurrency TheorySpringer:Berlin/ Heidelberg, Germany,2002.
36. Singh S.P,Nayyar A,Kumar R,Sahrma A,"Fog Computing :From Architecture To Edge Computing and Big Data Processing" In Journal Of SuperComputing in 2018,75,1-36.
37. Pramanik P.K,Pareek G,Nayyar A,"Security and Privacy in Remote Healthcare: Issues, Solutions and Standards" in Telemedicine Technologies ;Academic Press:Cambridge MA,USA,2019;pp.201-225.
38. Nayyar A,Jain R,Mahaputra B,Singh A.Q,"Cyber Security Challenges for Smart Cities in Driving the Development Management of Cognitive Cities " in Global Hershey USA,2019;PP.