



International Journal of Science, Architecture, Technology and Environment

Cloud Security Response Based on Coordinated Cryptographic Mechanisms

Shivam Agarwal^{1*}, Lav Dixit²

^{1,2}Deptt. of Computer Science & Engineering, R.D. Engineering College, Ghaziabad, India

*Corresponding author, veerdharam76@gmail.com

DOI: <https://doi.org/10.63680/ijstate0725013.03>

Abstract

The internet has become an essential part of daily life, used for education, business, trade, and even by young children. Despite its benefits, it poses significant security threats such as phishing, sniffing, hacking, cracking, denial-of-service attacks, and data theft. These risks create a sense of vulnerability among users, highlighting the need for robust network security. As information technology rapidly advances, the demand for effective security measures also grows. Tools like Intrusion Detection Systems (IDS) play a crucial role in identifying suspicious activities on networks. However, detection alone is not sufficient; prevention is also necessary. To address this, we propose a machine learning-based intrusion detection approach targeting threats like SQL injection, cross-site scripting, and DDoS attacks. By applying models such as Random Forest and General Regression Neural Networks, we achieve 69.10% accuracy in securing critical services—mail servers, databases, file systems, FTP servers- hosted via cloud infrastructure.

Keywords: Network Security; Intrusion Detection Systems (IDS); Machine Learning; Cyber Threats; Cloud Infrastructure

1. INTRODUCTION

Cloud computing has rapidly evolved alongside internet technologies, transforming how data is stored and accessed. It relies on distributed data centers and virtualization to offer scalable, on-demand services, allowing users to store and retrieve data from any internet-connected device—eliminating the need for local infrastructure. Key components of cloud systems include servers, storage, software, security frameworks, and user interfaces. The main features—accessibility, scalability, and availability—enable real-time services similar to utilities like electricity or water. Users benefit from reduced hardware costs, lower energy consumption, and minimized software maintenance, as services run remotely through providers. Cloud computing applications are categorized into models such as Software as a Service (SaaS), Platform as a Service (PaaS), Web Services, Utility Computing, Managed Services, and Internet Integration. These services are typically accessed via browsers, while data and software are hosted in the cloud. The term “cloud” symbolizes the abstraction of the complex backend infrastructure. The technology gained major momentum in 2009 with

platforms like Google App Engine, Microsoft Azure, and IBM Smart Business. Market projections showed explosive growth—from \$5.5 billion in 2008 to over \$150 billion by 2020.



Figure 1: Forecast of the size of the public cloud computing market.

2. PROPOSED METHODOLOGY

a. FLOW OF WORK

The core idea of the proposed system is to monitor users, update their medical records in real time, and store this data securely in cloud storage. It ensures data protection and privacy through an enhanced security technique, as illustrated in Figure 2. The system uses a mobile app interface and incorporates a secured hashing method combined with a Role-Based Security (RBS) model to safeguard sensitive user information.

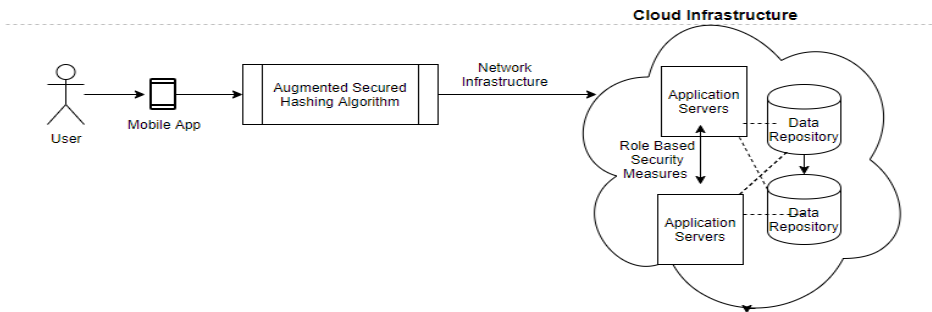


Figure 2: Proposed Scheme depicting the Mobile Based App using Augmented Security Measure in Cloud Infrastructure.

b. PROPOSED ALGORITHM

This proposed approach introduces a cloud-supported security system designed to safeguard sensitive data, particularly in medical environments. It combines cloud computing and security techniques to enhance data accuracy, accessibility, and protection through a dedicated mobile application. The system includes a thorough risk assessment, adherence to security policies, and integration of advanced security technologies. It addresses both proactive and reactive network security through a mobile app and a central cloud-based cluster, leveraging a Role-Based Security (RBS) model. This design reduces database load and ensures secure, efficient data access and storage.

Proposed Encryption Algorithm:

1. Initialize encryption key parameters.
2. Define variables $Tz0$, $Tz1$, $Tz2$, and $Tz3$.
3. Define variables $Tx0$, $Tx1$, $Tx2$, and $Tx3$.
4. Define variables $Tv0$, $Tv1$, $Tv2$, and $Tv3$.
5. Use a secure substitution box (Secured-box) to generate encoded values.
6. Compute a confidential parameter for encryption.
7. Encrypt data using a hash-based encryption model.
8. Apply asymmetric encryption to the message post-hashing.

More mathematically speaking, these three terms can be summed up using exponential values by comparing the best known attacks on these properties with optimal generic attacks. The length of the hash output is a key security parameter because it determines the overhead of generic attacks. For the minimum required security level of 120 bits in this scheme, because of the paradox for a hash function $H: \{0, 1\}^n \rightarrow \{0, 1\}^n$ at least the condition $rn = 8$ between 65536. It is not necessary to make a case distinction according to the time of use of the method because the hash methods recommended in this scheme have digest length of $rn = 2^8$ to 2^{64} .

3. SIMULATION AND RESULTS

This enhanced signature scheme is a novel hash-based algorithm designed to secure communications between parties, resources, and systems in cloud environments—leveraging Shielded Virtual Resources. By combining modern authentication and digital-signature techniques, it guarantees data integrity and availability. Our approach uses sandboxed substitution alongside an embedded descriptor key within the hashing process, strengthening tamper resistance and improving performance of automated timestamping. Although our evaluation data are synthetic, they demonstrate the scheme's potential. Future work will involve embedding the algorithm into real-world firmware and communication stacks, employing dynamic parameter tuning and automated validation to further reinforce system security.

3.1 WORK FLOW INCORPORATION OF ABOVE MENTIONED SCHEME UNDERBAR CODE BASED CAR PARKING SYSTEM USING CLOUD RESOURCE

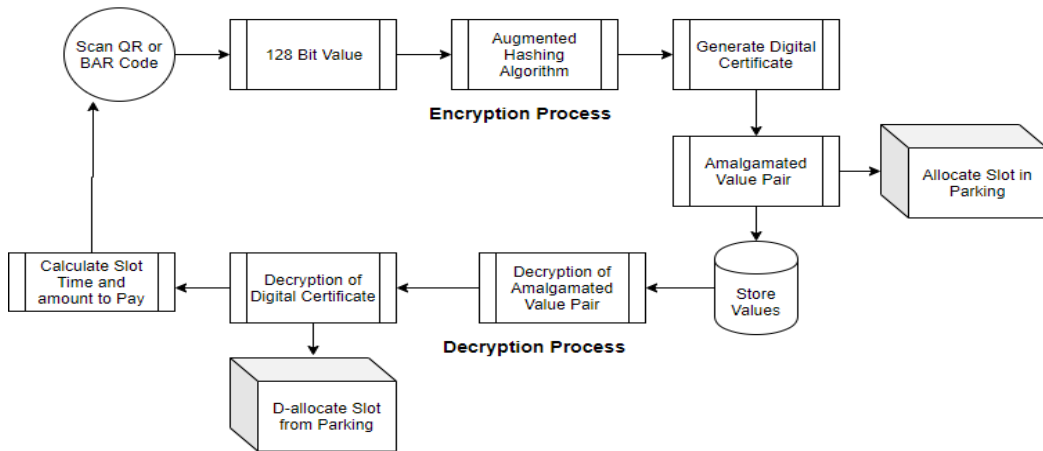


Figure 3: Workflow Diagram of Proposed Algorithm and Cloud App on Shielded Virtual Resource using Cloud Resource

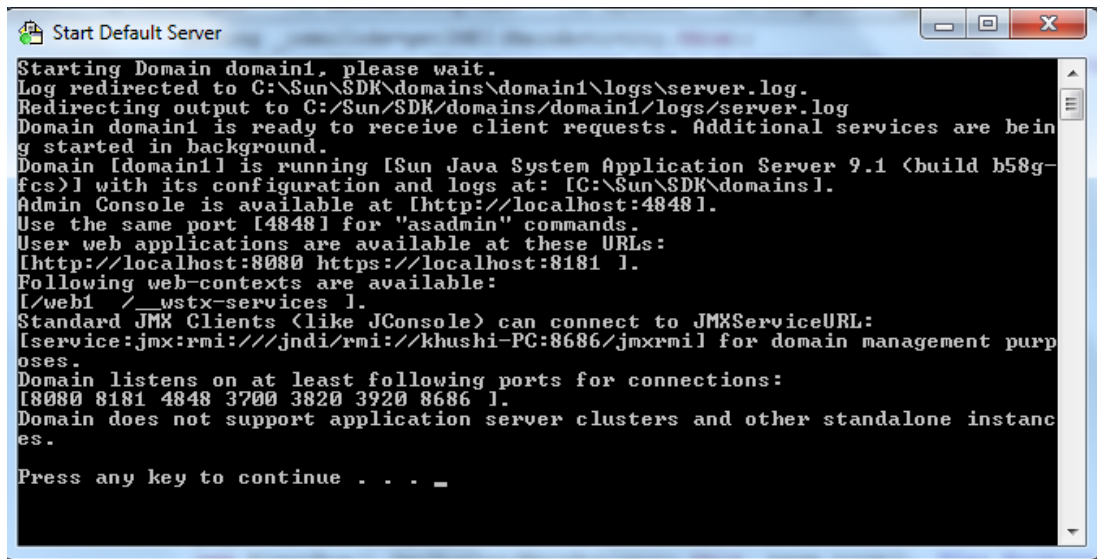


Figure 4: Starting Sun One Web Application Server

Above Application Web Server will communicate with Shielded Cloud Based App and the values captured will be stored in data repository. The server side Java Server Page is responsible to interact with mobile app and storing the values in data vault.

3.2 TEST ENVIRONMENT

To test the proposed conspire we have plotted the below mentioned ecosystem for calculation and evaluation.

Machines	Processing Speed	Cache Memory	Processors	RAM	Bit	Processor Description	Virtual Machine
1	2.1 GHZ	1.4 MB	4	4 GB	32	i3	NO
2	2.5 GHZ	2.4 MB	4	8 GB	64	i3	NO

Table 2: Resources Used for Performance Evaluation

Resource	Processing Time in Seconds
1	1.127
2	0.723

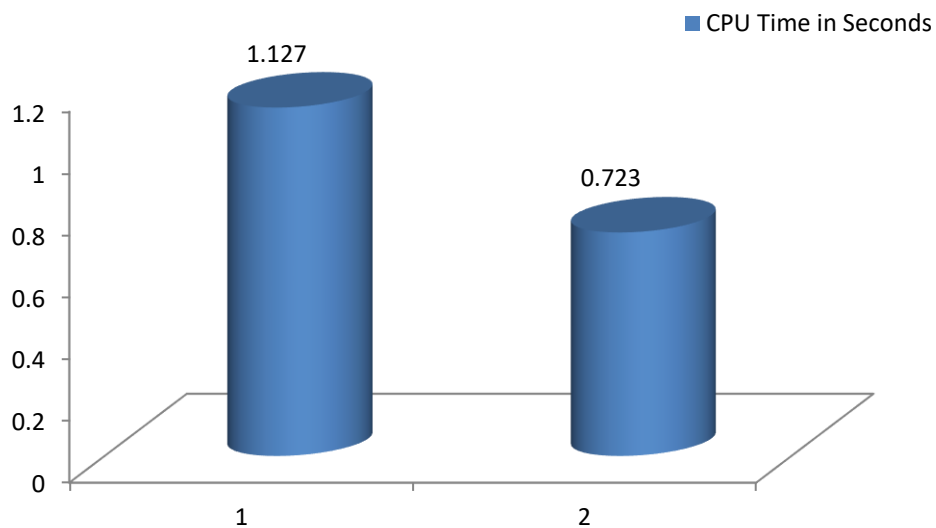


Figure 5: Results Depicted using Bar Graph

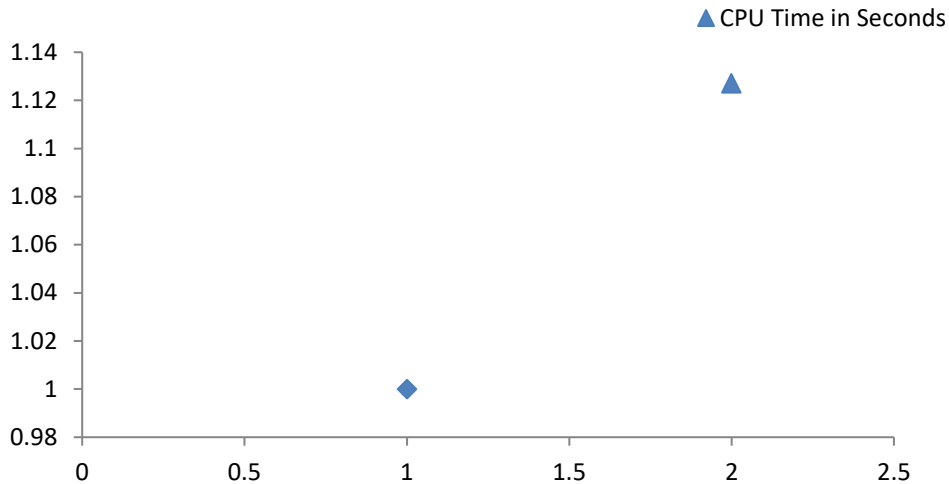


Figure 6: Results Depicted using Surface Model

From a theoretical standpoint, a major challenge in cloud computing is ensuring secure data storage with confidentiality and integrity under standard security models. Cryptographic methods like digital signatures, hashing, and fingerprinting offer effective protection against data tampering. The proposed scheme, built on an XOR-based hashing algorithm, enhances security by resisting unauthorized access and malicious activity. Future work will focus on deploying this fully encrypted model at the SaaS layer to provide comprehensive, end-to-end data protection.

4. CONCLUSION AND FUTURE SCOPE

4.1 Conclusion

This paper explored the role of cryptography in securing data stored on cloud servers. We began by introducing the fundamentals of cloud computing, including its definition, architecture, deployment models, and key characteristics. We also discussed the opportunities, challenges, and barriers to adoption—particularly security concerns in professional environments. A review of existing literature highlighted current cloud security strategies, standards, and threats. Building on this, we proposed a security framework focused on ensuring data confidentiality, integrity, and availability during transmission between internal and external resources. Our approach uses a hashing-based encryption algorithm to enhance communication security and system performance. While hash-based encryption in cloud services is still in its early stages, the proposed model offers stronger protection against both internal and external threats to sensitive data.

4.2 Future Scope

For the future scope, the proposed scheme can be inculcated as firmware in cloud architecture for better security parameters for authorization and authentication.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

- [1] National Research Council. 1999. Funding a Revolution: Government Support for Computing Research. Washington, DC: The National Academies Press. <https://doi.org/10.17226/6323>.
- [2] Qi, Lianyong&Khosravi, Mohammad & Xu, Xiaolong& Zhang, Yiwen& Menon, Varun. (2021). Cloud Computing. 10.1007/978-3-030-69992-5.
- [3] Beri, Rydhm& Singh, Jaspreet. (2020). Cloud computing.
- [4] P, Krishna Sankar& N P, Shangaranarayane&Saravanan, K.. (2020). CLOUD COMPUTING.
- [5] Manvi, Sunilkumar&Shyam, Gopal. (2021). Cloud Computing: Concepts and Technologies. 10.1201/9781003093671.
- [6] Kumar, Abhishek &Sanjeevikumar, P. &kumar, vishal. (2021). Blockchain Security in Cloud Computing. 10.1007/978-3-030-70501-5.
- [7] P, Krishna Sankar& N P, Shangaranarayane&Saravanan, K.. (2020). CLOUD COMPUTING.
- [8] <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france>
- [9] FRAUD THE FACTS 2019 | THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD
- [10] <https://www.cloudtp.com/doppler/cloud-economics-getting-bigger-picture/>
- [11] <https://www.vxchnge.com/blog/different-types-of-cloud-computing>
- [12] Hayes, Patrick & Morgenstern, Leora. (2007). On John McCarthy's 80th Birthday, in Honor of His Contributions. AI Magazine. 28. 93-102. 10.1609/aimag.v28i4.2063.
- [13] David W Cearley, Cloud Computing: Key Initiative Overview, Gartner Report, 2010
- [14] Peter Mell and Tim Grance, The NIST Definition of Cloud Computing, version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory, www.csrc.nist.gov, 7 Oct 2009
- [15] Dustin Amrhein and Scott Quint, Cloud Computing for the Enterprise: Part 1: Capturing the Cloud, DeveloperWorks, IBM, 8 Apr 2009
- [16] John Rhoton, Cloud Computing Explained: Implementation Handbook for Enterprises, Recursive Press, 3 May 2010
- [17] Kartit, Zaid &Azougaghe, Ali &Idrissi, H. & El marraki, Mohamed & Mustapha, Hedabou&Belkasmi, Mostafa & Ali, Kartit. (2016). Applying Encryption Algorithm for Data Security in Cloud Storage. 10.1007/978-981-287-990-5_12.
- [18] Saichyshyna, Nataliia. (2020). ELGAMAL ENCRPTION. 10.36074/11.12.2020.v2.02.
- [19] Mohit, Prerna& Biswas, G.. (2021). Modification of ElGamal Cryptosystem into Data Encryption and Signature Generation. 10.1007/978-981-33-4788-5_10.
- [20] <https://cloudnine.com/ediscoverydaily/electronic-discovery/according-to-idc-big-data-is-only-getting-bigger-ediscovery-trends/>
- [21] MihailDimitrov, Ibrahim Osman, The Impact of Cloud Computing on Organizations in Regard to Cost and Security, Department of informatics, <https://www.diva-portal.org/smash/get/diva2:728880/FULLTEXT02>
- [22] Bennett, David & Mason, Jeffrey. (2014). Secure cloud computing infrastructure.
- [23] Komarek, Ales &Pavlik, Jakub &Sobeslav, Vladimir. (2017). Performance Analysis of Cloud Computing Infrastructure. 303-313. 10.1007/978-3-319-65515-4_25.
- [24] Britannica, The Editors of Encyclopaedia. "John McCarthy". Encyclopedia Britannica, 20 Oct. 2020,

- <https://www.britannica.com/biography/John-McCarthy>. Accessed 1 April 2021.
- [25] Saurabh Chauhan, Dharamveer Singh, Atul Kumar Singh (2022) "Artificial Intelligence In The Military: An Overview Of The Capabilities, Applications, And Challenges", *Journal of Survey in Fisheries Sciences*, Vol 9 (2) pp 984-991. <https://doi.org/10.53555/sfs.v9i2.2911>
- [26] Kiran, Dharamveer Singh, Nitin Goyal, (2023) "Analysis Of How Digital Marketing Affect By Voice Search", *Journal of Survey in Fisheries Sciences*, Vol. 30 (2) 407-412. <https://doi.org/10.53555/sfs.v10i3.2890>
- [27] Yukti Tyagi, Dharamveer Singh, Ramander Singh, Sudhir Dawra (2024) "Analysis Of The Most Recent Trojans On The Android Operating System", *Educational Administration: Theory and Practice*, Vol. 30(2) 1320-1327. <https://doi.org/10.53555/kuey.v30i2.6846>
- [28] Shivane Singh, Dharamveer Singh, Ravindra Chauhan (2023) "Manufacturing Industry: A Sustainability Perspective On Cloud And Edge Computing", *Journal of Survey in Fisheries Sciences*, pp 1592-1598. <https://doi.org/10.53555/sfs.v10i2.2889>