# Study of Security Consideration using Anonymous Optimize Authentication Protocol in Cloud Computing

Mr. Deepak Kumar[1], Prof. Avinash Sharma[2]

[1]*PG Scholar,* [2]*Head and Associate Professor*

[1,2]*Dept. of CSE, MITS, Bhopal*

***Abstract:*** ***Security is the most prioritized aspect for any form of computing, making it an obvious expectation that security issues are crucial for cloud environment as well. As the cloud computing approach could be associated with having users sensitive data stored both at clients end as well as in cloud servers, identity management and authentication are very crucial in cloud computing. The execution time from cloud service providers is too high. Due to this reason, process becomes complex in execution. The execution time from cloud user execution time is high. Due to this reason, application responding time to user becomes high. The communication cost is high. Due to this reason, message delivering time becomes more. Cloud computing represents an IT infrastructure in which software and data are stored and processed remotely in the data center of a cloud computing provider or interconnected centers using an excellent bandwidth essential for the fluidity of the system; accessible as a service via the Internet. The operation of the proposed scheme Anonymous Optimize Authentication Protocol (AOAP) is based on some security operations which are presented in three phases: setup, registration, and authentication. The execution time from cloud service providers is reducing upto 21.07%. The execution time from cloud user is reducing upto 21.3%. The communication cost is reducing upto 28.3%.***

***Keywords: IoT, Cloud Computing, Anonymous Optimize Authentication Protocol, Communication Cost.***

## I. INTRODUCTION

Amazon S3, Google Cloud Storage (GCS) and Microsoft Azure as leading CSPs offer different types of storage (i.e., blob, block, file, etc.) with different prices for at least two classes of storage services: Standard Storage (SS) and Reduced Redundancy Storage (RRS). Each CSP also provides API commands to retrieve, store and delete data through network services, which imposes in- and out-network cost on an application. In leading CSPs, in network cost is free, while out-network cost (network cost for short) is charged and may be different for providers. Data transferring among DCs of a CSP (e.g., Amazon S3) in different regions may be charged at lower rate (henceforth, it is called reduced out-network cost).

The object workload is determined by how often it is read (i.e., Get access rate) and written (i.e., Put access rate). The Get access rate for the object uploaded to a social network is often very high in the early lifetime of the object and such object is said to be read intensive and in hot-spot status. In contrast, as time passes, the Get access rate of the object is reduced and it moves to the cold-spot status where it is considered as storage intensive. A similar trend happens for the Put workload of the object; that is, the Put access rate decreases as time progresses. Hence, such applications utilize more network than storage in the early lifetime of the object, and as time passes they use the storage more than network. Therefore, (i) with the given time-varying workloads on objects, and (ii) storage classes offered by different CSPs with different prices, acquiring the cheapest network and storage resources in the appropriate time of the object lifetime plays a vital role in the cost optimization of the data management across CSPs. To tackle this problem, cloud users are required to answer two questions: (i) which storage class from which CSP should host the object (i.e., placing), and (ii) when the object should probably be migrated from a storage class to another owned by the similar or different CSPs.

Recently, several studies take advantage of price differences of different resources in intra- and inter-cloud providers, where cost can be optimized by trading off compute vs. storage [4], storage vs. cache [5], [6], and cost optimization of data dispersion across cloud providers [7], [8]. None of these studies investigated the tradeoff between network and storage cost to optimize cost of replication and migration data across multiple CSPs. In addition, these approaches heavily rely on workload prediction. It is not always feasible and may lead to inaccurate results, especially in the following cases: (i) when the prediction methods are deployed to predict workloads in the future for a long term (e.g., a year), (ii) for startup companies that have limited or no history of demand data, and (iii) when workloads are highly variable and non-stationary.

Recent developments in the field of could compute have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users (Petre, 2012; Ogigau-Neamtiu, 2012;

Singh & jangwal, 2012). Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

• The transmission of personal sensitive data to the cloud server,

• The transmission of data from the cloud server to clients' computers and

• The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one.

There have been a number of different blends that are being used in cloud computing realm, but the core concept remain same – the infrastructure, or roughly speaking, the resources remain somewhere else with someone else's ownership and the users 'rent' it for the time they use the infrastructure (Bisong & Rahman, 2011; Rashmi, Sahoo & Mehfuz, 2013; Qaisar & Khawaja, 2012). In some cases, stored sensitive data at remote cloud servers are also to be counted. Security has been at the core of safe computing practices. When it is possible for any unwanted party to 'sneak' on any private computers by means of different ways of 'hacking'; the provision of widening the scope to access someone's personal data by means of cloud computing eventually raises further security concerns. Cloud computing cannot eliminate this widened scope due to its nature and approach. As a result, security has always been an issue with cloud computing practices.

Robustness of security and a secured computing infrastructure is not a one-off effort, it is rather ongoing – this makes it essential to analyse and realize the state-of-the-art of the cloud computing security as a mandatory practice. Cloud is mainly categorized as private cloud, community cloud, public cloud and hybrid cloud (Ogigau-Neamtiu, 2012; Singh & jangwal, 2012; Rashmi et al., 2013; Qaisar & Khawaja, 2012; Kuyoro, Ibikunle & Awodele, 2011; Suresh & Prasad, 2012; Youssef, 2012) - the discussion in this paper assumes only one category of cloud exists which is public cloud; as this assumption will well satisfy all the characteristics of any other type of cloud. Due to its diversified potentiality, the approach to cloud computing is being thought to be as the 5th utility to join the league of existing utilities water, electricity, gas and telephony (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009) rather than being just another service. The study presented in this work is organized with a view to discuss and indentify the approach to cloud computing as well as the security issues and concerns that must be taken into account in the deployment towards a cloud based computing infrastructure.

Discussion on the technological concepts and approaches to cloud computing including the architectural illustration has been taken into consideration within the context of discussion in this paper. Security issues inherent in cloud computing approach have been discussed afterwards. The exploration in the technological and security concerns of cloud computing has led to the concluding realization on the overall aspects of cloud computing. The approaches to counter security issues inherent in cloud computing are numerous with diversified facets and applications which has been kept out of scope. A discussion on the authentication of cloud computing has been addressed as it forms the holistic basis to embed integrity in the context of cloud computing security.

## II. LITERATURE WORK

Poorvika Singh Negi et. al, 2020, With the rapid increase in the number of users, there is a rise in issues related to hardware failure, web hosting, space and memory allocation of data, which is directly or indirectly leading to the loss of data. With the objective of providing services that are reliable, fast and low in cost, we turn to cloud-computing practices. With a tremendous development in this technology, there is ever increasing chance of its security being compromised by malicious users. A way to divert malicious traffic away from systems is by using Honeypot. It is a colossal strategy that has shown signs of improvement in security of systems. Keeping in mind the various legal issues one may face while deploying Honeypot on third-party cloud vendor servers, the concept of Honeypot is implemented in a file-sharing application which is deployed on cloud server. This paper discusses the detection attacks in a cloud-based environment as well as the use of Honeypot for its security, thereby proposing a new technique to do the same.

Yang Ming et. al, 2019, Vehicular ad hoc networks (VANETs) are an increasing important paradigm for greatly enhancing roadway system efficiency and traffic safety. To widely deploy VANETs in real life, it is critical to deal with the security and privacy issues in VANETs. In this paper, we propose a certificate-less conditional privacy preserving authentication (CCPPA) scheme based on certificate-less cryptography and elliptic curve cryptography for secure vehicle-to-infrastructure communication in VANETs. In the proposed scheme, a roadside unit (RSU) can simultaneously verify plenty of received messages such that the total verification time may be sharply decreased. Furthermore, the security analysis

indicates that the proposed scheme is provably secure in the random oracle model and fulfills all the requirements on security and privacy.

Feifei Wang et. al, 2019, Nowadays, remote user authentication protocol plays a great role in ensuring the security of data transmission and protecting the privacy of users for various network services. In this study, we discover two recently introduced anonymous authentication schemes are not as secure as they claimed, by demonstrating they suffer from offline password guessing attack, de-synchronization attack, session key disclosure attack, failure to achieve user anonymity, or forward secrecy. Besides, we reveal two environment-specific authentication schemes have weaknesses like impersonation attack. To eliminate the security vulnerabilities of existing schemes, we propose an improved authentication scheme based on elliptic curve cryptosystem. We use BAN logic and heuristic analysis to prove our scheme provides perfect security attributes and is resistant to known attacks. In addition, the security and performance comparison show that our scheme is superior with better security and low computation and communication cost.

Yicheng Yu et. al, 2019, The integration of Internet of things (IoT) and cloud computing technology has made our life more convenient in recent years. Cooperating with cloud computing, Internet of things can provide more efficient and practical services. People can accept IoT services via cloud servers anytime and anywhere in the IoT-based cloud computing environment. However, plenty of possible network attacks threaten the security of users and cloud servers. To implement effective access control and secure communication in the IoT-based cloud computing environment, identity authentication is essential. In 2016, He et al. put forward an anonymous authentication scheme, which is based on asymmetric cryptography. It is claimed that their scheme is capable of withstanding all kinds of known attacks and has good performance. However, their scheme has serious security weaknesses according to our cryptanalysis. The scheme is vulnerable to insider attack and DoS attack. For overcoming these weaknesses, we present an improved authentication and key agreement scheme for IoT-based cloud computing environment. The automated security verification (ProVerif), BAN-logic verification, and informal security analysis were performed. The results show that our proposed scheme is secure and can effectively resist all kinds of known attacks. Furthermore, compared with the original scheme in terms of security features and performance, our proposed scheme is feasible.

Xiaoying Jia et. al, 2019, Mobile edge computing (MEC) allows one to overcome a number of limitations inherent in cloud computing, although achieving the broad range of security requirements in MEC settings remains challenging. In this paper, we focus on achieving mutual authentication with anonymity and un-traceability, as this is crucial in ensuring data security and user privacy. Specifically, we design an identity-based anonymous authenticated key agreement protocol for the MEC environment. The proposed protocol achieves mutual authentication in only a single message exchange round, as well as assures both user anonymity and un-traceability. We then evaluate the security and performance of the protocol, and demonstrate that it achieves the required security properties and outperforms prior approaches in terms of communicational and computational costs.

Hamza Hammami et. al, 2019, Cloud computing represents the latest technology that has revolutionized the world of business. It is a promising solution giving companies the possibility of remotely storing their data and accessing services whenever they are needed and at a lower cost. However, outsourcing IT resources also brings risks, especially for sensitive information in terms of security and privacy, since all data and resources stored in the cloud are managed and controlled by cloud service providers. On the other hand, cloud users would like cloud service providers not to know what services being accessed and how often they are using them. Therefore, designing mechanisms to protect privacy is a major challenge. One promising research area is via authentication mechanisms, which has attracted many researchers in this delicate subject. For this, several solutions have been devised and published recently to tackle this problem. Nevertheless, these solutions often suffer from different types of attacks, high computing and communication costs, and the use of complex key management schemes. To address these shortcomings, we propose an approach that ensures the optimal preservation of the privacy of cloud users to protect their personal data including identities. The suggested approach gives the cloud user the ability to access and use the services provided by cloud service providers anonymously without the providers of those services knowing their identity. We demonstrate the superiority of our proposed approach over several anonymous authentication solutions in terms of computation and communication costs.

## III. PROBLEM IDENTIFICATION

The basic objections of my hypothesis work are according to the accompanying:

1. The execution time from cloud service providers is too high. Due to this reason, process becomes complex in execution.

2. The execution time from cloud user execution time is high. Due to this reason, application responding time to user becomes high.

3. The communication cost is high. Due to this reason, message delivering time becomes more.

## IV. OBJECTIVES

The basic objections of my hypothesis work are according to the accompanying:

1. To reduce execution time from cloud service providers.

2. To reduce execution time from cloud user.

3. To reduce communication cost.

## V. PROPOSED METHODOLOGY

The operation of the proposed scheme Anonymous Optimize Authentication Protocol (AOAP) is based on some security operations which are presented in three phases: setup, registration, and authentication. Each phase is detailed as follows:

In this phase, cloud users generate a list of parameters. These latter will allow the other phases to operate securely. The details are as follows:

Table 1: List of Symbols

| **Symbol** | **Description** |
|---|---|
| E | Elliptic curve under reference |
| p and q | Long prime integers |
| e(.) | Bilinear pairing function |
| $G_1$ | Multiplicative group of order q |
| $G_2$ | Additive group of order q |
| $H_1(*)$, $H_2(*)$ | One-way hash functions |
| $x_{uc}$ | The secret key to the user cloud |
| $x_{cp}$ | The secret key to the cloud |
| P | Group generator |
| a, b, n, d | Random numbers |
| $t_{UC}$, $t_{CP}$ | Time stamps |
| $ID_{UC}$ | The identifier of the cloud user |
| $ID_{CP}$ | The anonymous identifier of the cloud |
| $AID_{UC}$ | The anonymous identifier of the cloud user |
| $AID_{CP}$ | The anonymous identifier of the cloud |
| $\oplus$ | Bitwise XOR operation |
| $\|\|$ | Bitwise concatenation operation |
| SK | Session key |
| Enc, Dec | Encryption and decryption functions |

1. At the beginning, they arbitrarily produce two large prime integer p and q. After that, they choose an elliptic curve E($Fp$ ) on $Fp$.

2. Then, they firstly generate two groups of order q: a first additive group $G1$ and a second multiplicative $G2$ . Secondly, they generate (P; *e:* $G1 \times G1 \longrightarrow G2$). We note here that P represents a generator of the additive group and *e* denotes a bilinear pairing.

3. Next, the cloud user chooses two secure hash functions:

– $H1$: $\{0, 1\}^* \times G1 \longrightarrow G1$

– $H2$: $\{0, 1\}^* \times G2 \longrightarrow Zq^*$

4. After that, they generate a random number. The latter will be considered as a secret key $x_{UC} \in Zq^*$. Then, we find: $YUC = x_{UC} \cdot P$

5. Finally, they send {E($Fp$ ), $G1$ , $G2$ , $H1$(.), $H2$(.), $YUC$ } to the cloud and keep its secret $x_{UC}$.

Once the setup phase is completed, during which the cloud user has generated a list of parameters, these parameters will allow the other phases to operate in the best safety conditions. During the registration phase, cloud computing securely records its users so that they can receive and store them safely. The stages of registration between the cloud and its users are detailed as follows:

1. After receiving the parameters generated by the cloud user terminal, the cloud will generate a random number that will be considered as its secret key $x_{CP} \in Z_{q^*}$. Then it will calculate $Y_{CP} = x_{CP} \cdot P$. Once the calculation is complete, the cloud sends its user $ID_{CP}$ identity with $Y_{CP}$. This sending is done via a secure communication channel while using a Secure Socket Layer (SSL). We indicate by UC cloud user and CP cloud remote platform.

2. Once $ID_{CP}$ with $Y_{CP}$ is received by the cloud user, the latter will check the validity of the received cloud identity. In case the validity check result is not correct, the user will declare that it is a conflict. Otherwise, the user will produce a $t_{UC}$ time stamp as well as two ephemeral (lasts for a very short time) secrets a and b $\in Zq^*$. After that, the user computes $A_{UC} = a \cdot P$, $B_{UC} = b \cdot P$, $Q_1 = A_{UC} \oplus Y_{CP}$, $Q_2 = B_{UC} \oplus Y_{CP}$.

3. Subsequently, thanks to the secret numbers generated and the secret keys calculated, the users will hide their real identity as well as the cloud. Subsequently, they will calculate their corresponding anonymous identities in the following way:

– $AID_{UC} = H_1(ID_{UC} \| t_{UC} \| x_{UC} \| A_{UC} \| B_{UC})$ and

– $AID_{CP} = H_1(ID_{CP} \| Q_1 \| \| Q_2)$

Afterwards, the cloud user calculates $C_{CP} = a + b + AID_{CP} \cdot x_{UC}$ and sends to the cloud

$\{AID_{CP}, AID_{UC}, A_{UC}, B_{UC}, C_{CP}\}$

4. After having received $\{AID_{CP}, AID_{UC}, A_{UC}, B_{UC}, C_{CP}\}$ by the cloud, the latter will produce a time stamp $t_{CP}$ and computation $Q_1 = A_{UC} \oplus Y_{CP}$, $Q_2 = B_{UC} \oplus Y_{CP}$ and $AID_{CP} = H_1 (ID_{CP} \oplus Q_1 \oplus Q_2 )$. Next, the cloud will send $AID_{CP}$ and $t_{CP}$ to its user.

5. Once $AID'_{CP}$ and $t_{CP}$ are received by the cloud user, the latter will check the freshness and validity of $t_{CP}$ and then

check whether $AID_{CP} = AID'_{CP}$ and $C_{CP} \cdot P = A_{UC} + B_{UC} + AID_{CP} \cdot Y_{UC}$. If the result of the check is verified by the cloud user as invalid, there will be an error message returned to the cloud. Otherwise, the registration phase is performed successfully.

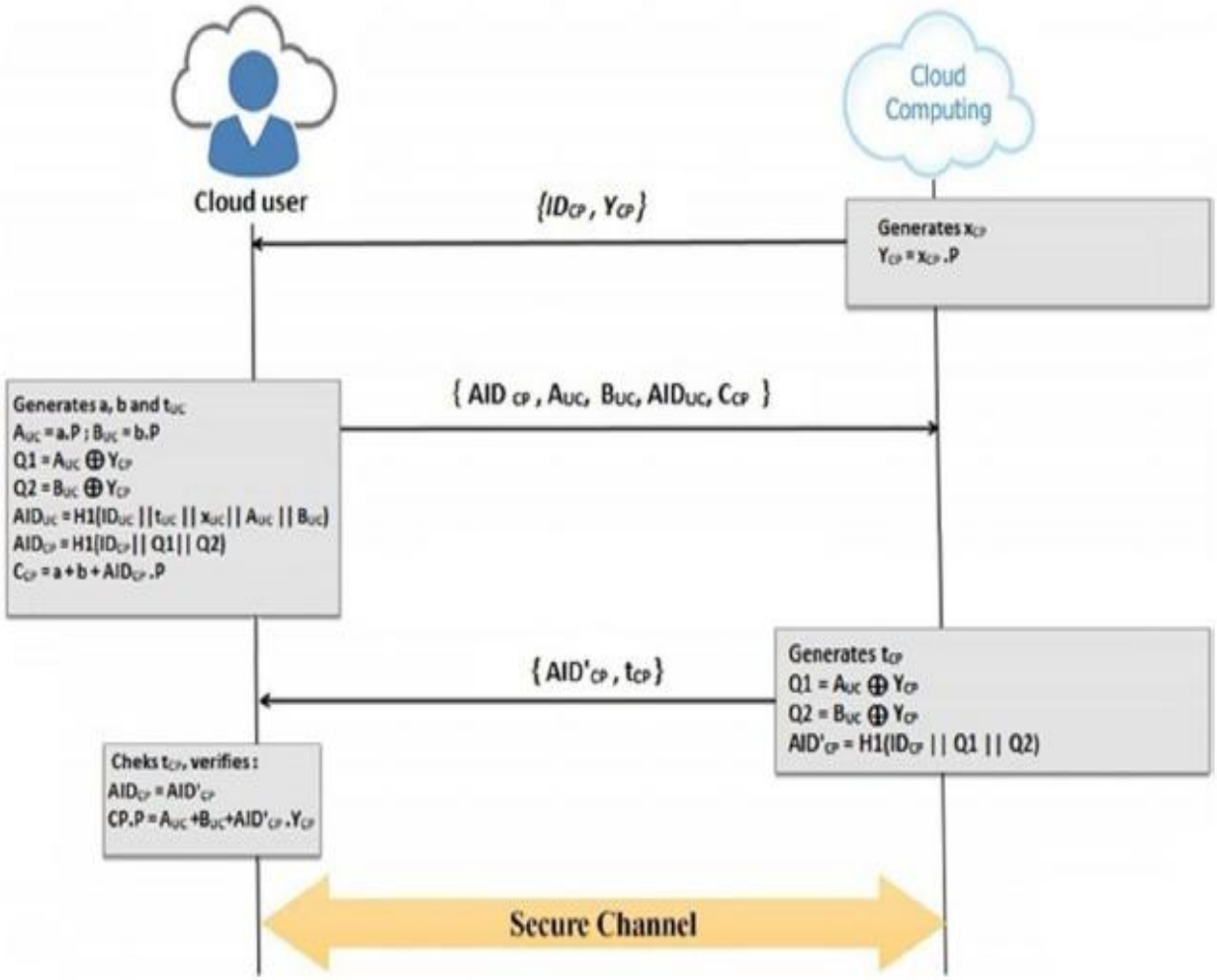


Figure 1: Registration phase

As soon as the registration step is completed, the utilize will become a cloud user and can perform anonymous authentication. The details of this phase are described by the following steps:

1. First, the cloud generates a second time stamp $t'_{CP}$. After that, it generates n ∈ $Zq*$, which is an arbitrary number to be used once. Then, the cloud calculates $N_{CP} = n \cdot P$, $M_{CP} = n \cdot Y_{UC}$, $K_{CP} = H_1(N_{CP} \| M_{CP} \| t'_{CP})$, $U_{CP} = e(M_{CP}, K_{CP})$, $Z_{CP} = x_{CP} +$

$H_1(AID'_{CP} \| U_{CP} \| t'_{CP})^{n.xCPmodq}$ and cipher = $Enc(AID'_{CP} \| Z_{CP})$. Subsequently, the

cloud sends { $N_{CP}$ , cipher, $t'_{CP}$ } to its user.

2. Once {$N_{CP}$, cipher, $t'_{CP}$} are received by the user, the latter will check both the validity and the freshness of $t'_{CP}$. After that, the user will calculate $M'_{CP} = x_{UC} \cdot N_{CP}$, $K_{UC} = H_1(N_{CP} \| M'_{CP} \| t'_{CP})$ and $U'_{CP} = e(K_{UC}, M'_{CP})$. Using the $K_{UC}$ key, the user decrypts the cipher to get the clear = $Dec_{KUC}$(cipher). Next, this user calculates $Z'_{CP}$ = clear $\oplus$ $AID_{CP}$ and checks whether the following equation holds:

$Z'_{CP} \cdot P = Y_{CP}+P(H_1(AID_{CP} \| U'_{CP} \| t'_{CP}))M'_{CP} \cdot Y_{CP}/Y_{UC}$. If the result of the equation is verified by the user as incorrect, the authentication phase will be stopped, and an authentication error message will be sent to the cloud. Otherwise, the user has successfully passed the authentication phase. Next, the cloud user will generate a variable d ∈ $Zq*$ and will calculate $D_{UC} = d \cdot P$, Pass = $H_2(D_{UC} \| M'_{CP} \| Z'_{CP} \cdot P \| t'CP)$, and the session key SK= $H_2(Pass \| d \cdot N_{CP})$. Subsequently, the user will send {Pass, $D_{UC}$} to the cloud.

3. Finally, the cloud will calculate $H_2(D_{UC} \| M_{CP} \| Z_{CP} \cdot P \| t'_{CP})$. Afterwards, it will check the result of the calculation with Pass. If the verification result sent by the user is not correct, then the session will be suspended. Otherwise, the calculation of the session key is done in the following way: $S_K = H_2(Pass \| n \cdot D_{UC})$.

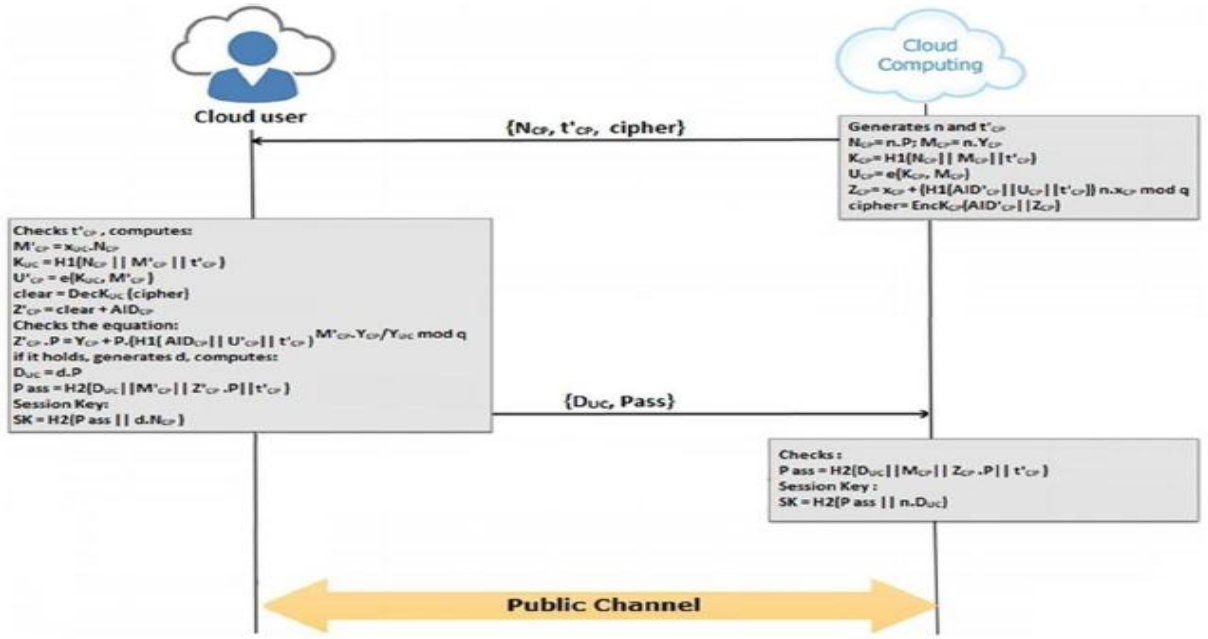


Figure 2: Authentication and key agreement phase

## VI. RESULTS AND ANALYSIS

Analysis performs on the basis of number of cloud providers and users. These numbers of cloud providers and users are listed below

Table 1: Computation time (ms) as per cloud service providers

| No. of Providers | LAAP[1] | AOAP (Proposed) |
|---|---|---|
| 2 | 2176 | 1614 |
| 4 | 2408 | 1982 |
| 6 | 2711 | 2219 |
| 8 | 2907 | 2428 |
| 10 | 3218 | 2716 |
| 12 | 3613 | 3011 |

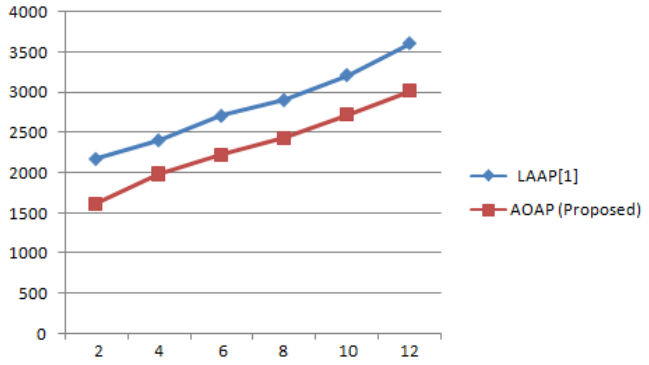


Figure 3: Graphical analysis of computation time (ms) as per cloud service providers

In above figure, x-axis shows the number of providers and computation cost (ms) evaluate on the basis of utilization of cloud provider bandwidth. The value of computation cost (ms) become decrease for AOAP (proposed) as compare then LAAP[1]. Hence resource utilization becomes improve as compare than LAAP[1].

Table 2: Computation time (ms) as per cloud user

| No. of Users | LAAP[1] | AOAP (Proposed) |
|---|---|---|
| 2 | 0352 | 0277 |
| 4 | 0411 | 0361 |
| 6 | 0572 | 0428 |
| 8 | 0682 | 0511 |
| 10 | 0802 | 0718 |
| 12 | 1022 | 0981 |

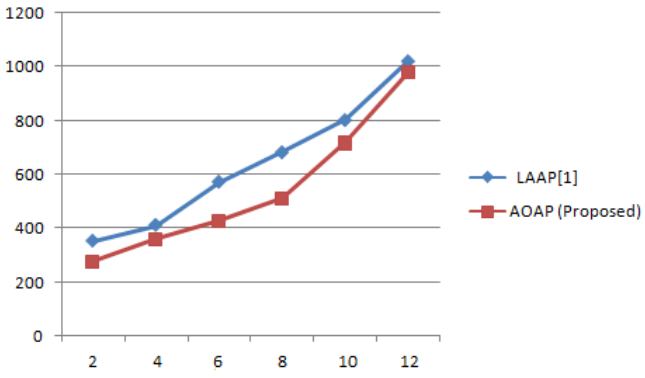


Figure 4: Graphical analysis of computation time (ms) as per cloud users

In above figure, x-axis shows the number of users and computation cost (ms) evaluate on the basis of utilization of cloud user. The value of computation cost (ms) become

decrease for AOAP (proposed) as compare then LAAP[1]. Hence resource utilization becomes improve as compare than LAAP[1].

Table 3: Communication Cost (bits)

| No. of Users | LAAP[1] | AOAP (Proposed) |
|---|---|---|
| 2 | 1088 | 718 |
| 4 | 1463 | 1121 |
| 6 | 1769 | 1392 |
| 8 | 2011 | 1785 |
| 10 | 2358 | 1907 |
| 12 | 2694 | 2261 |

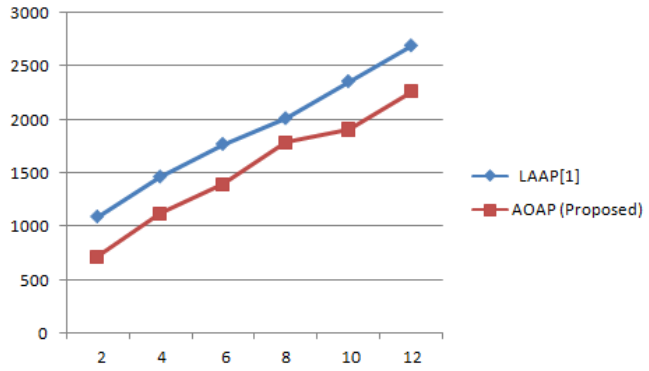


Figure 5: Graphical analysis of communication cost (bits) as per cloud users

In above figure, x-axis shows the number of users and computation cost (bits) evaluate on the basis of utilization of cloud user. The value of computation cost (bits) become decrease for AOAP (proposed) as compare then LAAP[1]. Hence resource utilization becomes improve as compare than LAAP[1].

## VII. CONCLUSION

To overcome the security loopholes, we present an efficient authentication scheme using elliptic curve cryptosystem. In our scheme, the security of session key is fully guaranteed. It prevents all the possible session key exposure, forward secrecy attack included. We give both formal analysis and informal analysis to prove the completeness and security of the proposed scheme. Furthermore, the outcomes of security and performance comparison show that the proposed scheme is superior with better security and low computation and communication cost. Besides, the proposed scheme has good expansibility. A secure authentication protocol for IOT and cloud servers based on ECC. They claimed that their framework is safe against different attacks and provides all security needs. But by reviewing their scheme in this work we prove that their work is not safe against different attacks such as stolen - verifier password attack, stolen - verifier identity attack, no protection for session key, many login attack and insider attack.

The goals of this thesis work are as per the following:

1. The execution time from cloud service providers is reduce upto 21.07%.

2. The execution time from cloud user is reducing upto 21.3%.

3. The communication cost is reducing upto 28.3%.

## VIII. FUTURE SCOPE

We plan to design an efficient biometrics-based remote user authentication scheme for multi server environment based on our current work. we propose an improved authentication and key agreement scheme for IoT-based cloud computing environment, and provide ProVerif tool verification and formal security analysis via BAN-logic. The comparisons of security and performance show that the computational cost of our proposed scheme is slightly higher but is much safer than the original scheme.

## REFERENCES

[1] Poorvika Singh Negi, Aditya Garg and Roshan Lal, "Intrusion Detection and Prevention using Honeypot Network for Cloud Security", IEEE Conference on data security, 2020.

[2] Yang Ming and Hongliang Cheng, “Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs”, Hindawi Mobile Information Systems, 2019.

[3] Feifei Wang , Guoai Xu and Lize Gu. “A Secure and Efficient ECC-Based Anonymous Authentication Protocol”, Security and Communication Networks Volume 2019.

[4] Yicheng Yu, Liang Hu and Jianfeng Chu, “A Secure Authentication and Key Agreement Scheme for IoT-Based Cloud Computing Environment”, www.mdpi.com/journal/symmetry, 2019.

[5] Xiaoying Jia, Debiao He , Neeraj Kumar and Kim-Kwang Raymond Choo, “A Provably Secure and Efficient Identity-Based Anonymous Authentication Scheme for Mobile Edge Computing”, IEEE SYSTEMS JOURNAL, 2019.

[6] Hamza Hammami, Sadok Ben Yahia, Mohammad S. Obaidat, “A lightweight anonymous authentication scheme for secure cloud computing services”, The Journal of Supercomputing, 2019.

[7] Adesh Kumari, Vinod Kumar, M. Yahya Abbasi, Mansaf Alam, “The Cryptanalysis of a Secure Authentication Scheme Based on Elliptic Curve Cryptography for IOT and Cloud Servers”, International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018), 2018.

[8] Linmei Jiang, Xiaochao Li, L.L. Cheng and Donghui Guo, "Identity Authentication Scheme of Cloud Storage for User Anonymity via USB Token", IEEE International Conference on Cloud Computing, 2018.

[9] Qi Xie, Duncan S. Wong, Guilin Wang, Xiao Tan, Kefei Chen, Liming Fang, "Provably Secure Dynamic ID-based Anonymous Two-factor Authenticated Key Exchange Protocol with Extended Security Model", IEEE Transactions on Information Forensics and Security, 2017.

[10] Yaser Mansouri, Adel Nadjaran Toosi and Rajkumar Buyya, "Cost Optimization for Dynamic Replication and Migration of Data in Cloud Data Centers", IEEE Transactions on Cloud Computing, 2017.

[11] F. Abundiz-Pérez, C. Cruz-Hernández, M. A. Murillo-Escobar, R. M. López-Gutiérrez and A. Arellano-Delgado, "A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler Map", Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2016.

[12] Kuo-Hui YEH, "A lightweight authentication scheme with user un-traceability", Frontiers of Information Technology & Electronic Engineering, 2015.

[13] Preeti Chandrakar, Hari Om , "A Secure Two-Factor Mutual Authentication and Session Key Agreement Protocol using Elliptic Curve Cryptography", IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS), 2015.

[14] Shehzad Ashraf Chaudhry, Husnain Naqvi, Taeshik Shon, Muhammad Sher, Mohammad Sabzinejad Farash, "Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems", Springer Journal (10.1007/s10916-015-0244-0), 2015.

[15] Yanrong Lu, Lixiang Li, Haipeng Peng, Yixian Yang, "An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography", Springer Journal of Multimedia Tools Application, 2015.