

A Novel Methodology for Cloud of Things-Based Secure Higher Education Framework Using Zero Knowledge Proof System

Kuntal Mukherjee, Birla Institute of Technology, Mesra, India

Sudhanshu Maurya, Graphic Era Hill University, Bhimtal, India

 <https://orcid.org/0000-0002-1999-1858>

Ranjan Kumar Mandal, Cognizant, India

Mukul Thakur, Accenture, India

Farzana Khatoon, Ranchi University, India

ABSTRACT

The cutting-edge technology, namely cloud of things (CoT), has shaped the existing business process into a new orientation in terms of performance, usability, and reliability. Among different business processes, online education is one of the prime areas where CoT can be used to make it more agile in the context of performance and usability. In this endeavor, a novel methodology has been proposed for an online higher education framework based on CoT. The proposed framework is made agile using service-oriented architecture (SOA). Furthermore, in order to make the proposed framework more reliable, a zero knowledge proof (ZKPF) system has been introduced here. The proposed ZKPF algorithm is based on the Hadamard matrix. Experimental results have been shown to lay bare the effectiveness of the proposed algorithms.

KEYWORDS

Business Process, Cloud Computing, Cloud of Things, Hadamard Matrox, Internet of Things, Service-Oriented Architecture, Spring Framework, Zero Knowledge Proof System

INTRODUCTION

The astonishing formation of information automation has developed a new sight for web studying that its impact has so far escalated to the globe. That is the reason various nations have been recompensing importance to information technology and awaiting and provide studies in different and tempting ways. It is quite familiar, the implementation of computers and online coaching, to the former tutoring needs some sort of alteration. As result, the experimentation and evolution of mannered studying must sincerely mention the returned interconnection among the peers. Implant the Interconnected experiments matters to the upper mention procedure, the outcomes of the energetic experiment than can be waited (Weston, T.J. and Barker, L., 2001). In an online learning atmosphere, self-studying has become a crucial chain to mentor peers by advising the studying roots to peers' requirements in instants time duration (O. R. Zaiane, 2001). Network relied upon studying as a widely used education system gives many probabilities, like reaching a new batch of peers, the liberty of opting the period

DOI: 10.4018/IJWLTT.285565

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

to gain in any duration of period and can be accessed in every place, the option learners choose and combinatory education atmosphere (Rune Pettersson Gary Svensson Yvonne Waern, 2002).

Reciprocity is the hub of tutoring and education. The studying procedure is relied upon the interconnection with the tutor, with the students along the satisfaction. The latest network and the publishing automation lay out the variety of probabilities for peers to reciprocate with satisfaction along with the other students and mentors (Xu Lei, Claus Pahl, and Dave Donnellan, 2003). The network as the base, whilst grows complication for the two grounds. Initially, the instructor gets a little response in return. The second thing is that it ignites the latest and creative ideas of instructing and studying. Developing assessment and the shadows of assessment outcome into the guiding structure and therefore the grounds in the context (Chenn-Jung Huang, et al., 2004).

Moreover, the modern online education atmosphere is occasionally an addition to the primitive bookish studying, in which the student reads the matter from a display despite the papers. Creating an online combinatory education is a sight and difficult task in order to enhance the standard of education and lifetime studying online (Yi Jia, 2005).

In the past years, computer automation, and the world network in specific altered the manner we used to instruct and gain, and this innovation will remain in the following years with more educational institutions along with the elementary education compromising with the online studies of different types into their studying affairs (Harris Wang, 2006).

Individual syllabus series is a crucial experiential issue for network education as no certain education ways would be correct for all the students .so, many workers concentrate on growing online environment chains to persist internet-based education and adopting gives studying ways to support the studying presentation of all students (Chin-Ming Hong, et al., 2007)

The own regulatory education is a worldwide studying rotated styling planning and it very appropriate to be implemented in own managing studying for supporting education presentation of every student in online e-learning. The own studying capacity of students is a crucial point impacting the studying presentation in an online studying atmosphere (Chih-Ming Chen, et al., 2007).

In the experiment task of Agatha and Burd, SWLinker is shown, a format that hopes to raise the capacity of network-based education sources by the unity of Semantic network automation. It grips the alliance of Learning Objects (LOs) on the Semantic network-based actual connection to feed the network papers with semantic piles of additional information. SWLinker is a package of various machinery that gives two tempting paths to support the peers while searching the sources on the network. 1) it works as a styling follower that generally supports the students having a little details f the specific titles. it allows them to search general papers, meanwhile, to have the educational mentoring and key to the additional information sauces valid to the content. 2) it works as a combinatory searching servant that facilities combinatory answers on the grounds of guidance sectors (Iyad AlAgha, Elizabeth Burd, 2008).

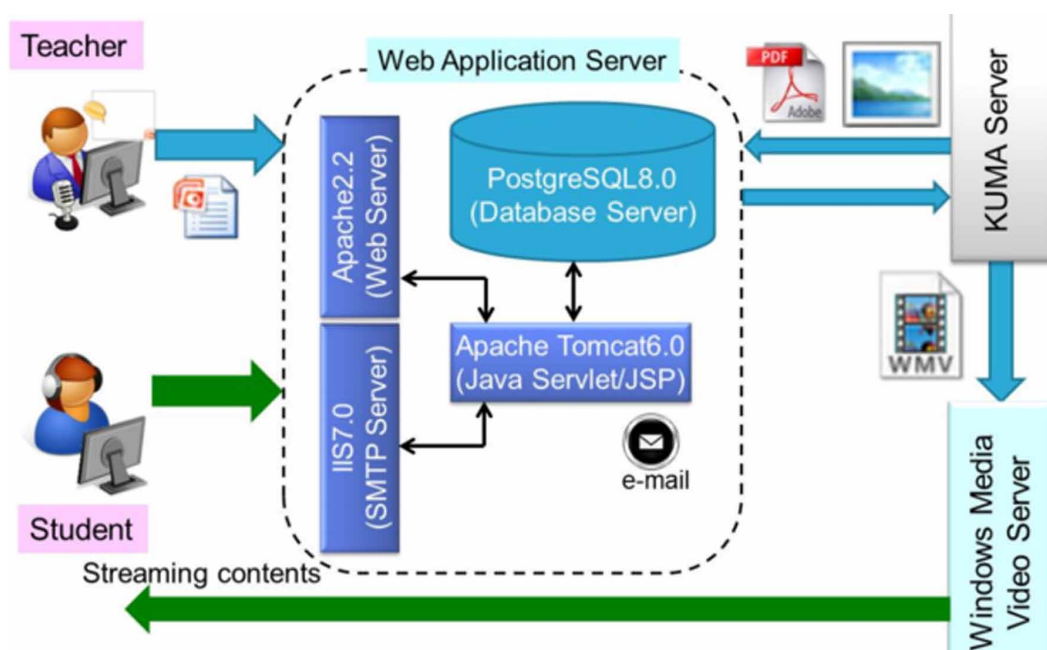
In the past ten years, network automation is modernizing on a greater scale than the time of wise network-based learning jobs is upcoming soon. In specific, the semantic network has changed the growth of network genius through advanced medium capability on the information grounds shown by graded languages on the web. There are the RDF and OWL which are helpful to predict the semantic connections among network grounds (Feng-Hsu, W. and Dai-Yan, C., 2008).

Virtual Learning environments are the crucial partials the web-based stage for studying in the oats few years. Sure, the change in the increment in utilization VLE with the primitive learning system, reusing of the utilities requires to be incremented too. Most recent VLEs are being created with the help of a system of focused reach instead if any learning organization requires a VLE, they require to buy the complete seem and install it in third servers. This resists the self-usage of VLEs in the content of user medium structure bad utilities for both peers' tutors (e.g., studying and education utilities) (Fang-Fang, C. and Eng-Soon, T., 2008).

A very popular instant studying atmosphere comprises of the network implementation base with the receipt of PowerPoint data, tabulation of network-based classes matter, the identification

governance and jobs to tutors and peers, the KUMA server, and the system made by visual C# with interchanging of PowerPoint file to puff files and various streams in window format, depicted in Figure 1. The motion comprising utility of playing and providing is added to providing matters to various peers. The presentations with the Windows Media Load Simulator reveal the probability to provide to about 100 peers. A genuine duration system of changing from PowerPoint to WMV (window media video) file is created to identify the finishing of alteration. After finishing, an email is sent to a tutor for having a loon on the web-based class matter (Hidenori Akiyama, et al., 2012).

Figure 1. Rapid e-learning system Source: Hidenori Akiyama, et al., 2012



A lot of research has found optimistic answers with the implementation of network-based unit tests for the online learning environment. Wang reveals, network-based unit assignments permit students to feed the atmosphere and solve the problems at any duration of time and from any network linked computer after online lectures (T. H. Wang, 2008). Besides, it also has consequences on network-based studying. Ahead it is advised that instructors could provide personated studying by utilizing the personalized studying techniques', facing the benefits of utilizing personalized studying (T. H. Wang, 2012) (Hamidreza Mahrooian and Dr. Wee Mee Chin, 2013).

MOOCs provides the best-rated learning network-based syllabus at affordable prices to anyone, making upgraded instructing providing to everyone with the connection of worldwide network (Frolov, I., & Johansson, S. 2013), encouraging the learners to utilize their precious time in focused learning (Grunewald, F., et al., 2013), and unfolds the personalized studying and lifetime studying (SRI Education, 2014). An educating increment area is one of the useful and impactful elements. It is a statically way that enables the users to have a look at their performance through thru method of an activity, return a response on finishing the activity or a performance display which develops more with the more competition of activity (Conrad, F. G., et al., 2010), and a time governing utility to the peers that shows their performance in tasks (Filv , D. A., 2014). It is necessary for today's user medium. It has numerous sight displays e.g., histograms, Courser (Te-Lien Chou and Sufen Chen, 2015).

BACKGROUND

We reside in an era where information and communication automation is an uncarpeted part of around all grown nations. ICT furnishes and aids the standard of living in various environments including tablets, learning procedures, and safety (Sari, P. W. C. R. H. H. M. W., 2017). Internet of things supports ICT to add the given utilities for things approach and reshaping from anywhere to any individual globally (A. Abuarqoub, et al., 2017). IoT comprises four pillars, things, people, process, and data. In today's world of IoT tools are attached to the web but in the future would be connected to more advanced devices that will have internet connectivity (Azamat Zhamanov, et al., 2017).

In the research paper of Majored and Ali, it is said about recasting the smart classrooms and campus with the Internet of Things (Iota) implementations. The Iota program is been classified into various parts that specify the specific effect on campuses and classrooms. With the coming of Iota applications the higher studies organization Havel has been drastically altered which allows different things to have a connection between them for the central base of interconnection. Various object varies from controllers to sensors. various learning parameters can be detected using big data, wearable automation, interconnected truth, and cloud computing. This automation has developed a new connection between the educational atmosphere and the peers to provide useful details. The implementation of Iota in studies is divided into the mentioned terms of classroom access control, enhancing instructors, and studying, looking on leaner's healthcare, true ecosystem, and energy governance (Asim M. & Mahmood A., 2018).

A little IoT testbed is known as IoT PEER (IoT platform for engineering education and research) was structured at Tennessee Tech for research no education. Recently this testbed is used in learning safety and modern manufacturing-based matters (Terry G., et al., 2018). Studying skills play a crucial part in gripping and having a deep knowledge of a learner. if the tasks, assessments, lectures, etc are made as per the preferred requirements of peers that can turn into good furnishing and the knowledge of the subject by the learner (Saxena, A., et al., 2019).

Internet of things is emerging tech automation. It is considered more innovative. The device's interconnection out-breaking emergence is altering the globe. The IoT experiments result from numerous institutions that have adopted IoT as their automating planning (Williams, Z. D. et al., 2020). The reason resides in the splendid caliber of interconnected IoT automation and the lasting modernization of its tempting utilization in the structure of various standards (Scully, P., 2020). However, these mediums' information is huge, customers are facing problems in the right decision of which medium is best for the usage between the three. This search reveals the difference between the three major centers of analytics and safety (Muhammed, A. S. & Derya U., 2020).

The worldwide network and the net extension into the physical truth is made probability through several criteria which are categorized in a roof of the extensively utilized terms i.e., internet of things for IoT which is an emerging subject of finance social and automation needs (Krajjak, S., & Tuwanut, P., 2015).

It is revealed that 85% of institutions globally will use IoT smart tools in various parts according to (Meola, A., 2016) and nearly 90% of the businesses are not sure about their safety (Waseem I., et al., 2020). In the research work of J Steven Perry, the author reveals the various strike that can be applied to the number of IoT answers that are striker needed weakness on the personalized device's food having a path to the whole web (Perry, J. S., 2017).

The dangers of IoT comprises the topic like weak password dearth to assess back doors and web execution. Detail of endangers can be seen in the attack surface area. When a striker intrudes into the web, he tries to figure out an IP address, find out web activities and send bitter messages to them. Similar activities performed in striking and IoT web is to change devices in two boats are for the usage for DDoS strikes. Data secrecy is a matter as a striker under the web could call you could intentionally light personal data such as secret passwords, card details, and other personalized information (Lilla N. & Adrian C., 2019)

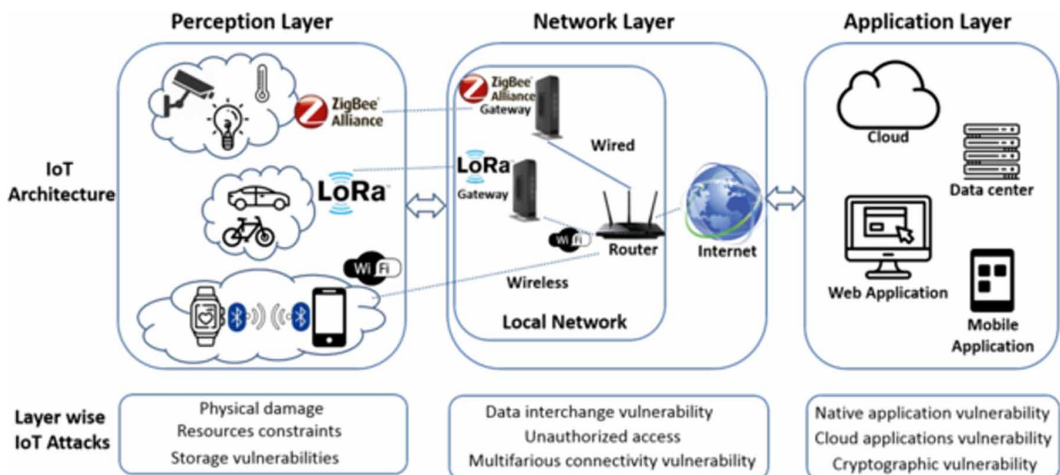
The major automation enablers of IoT format are descriptive, also finding the open safety and secrecy terms (Luigi A., et al., 2010). The authors supply test of secrecy lacking IoT formats Vidyut three-dimensional design to show the interconnection of IoT safety hub whereas the result of countermeasures is lost (Md Mahmud H., et al., 2015). Weber stated that secrecy and safety valid IoT issues are raised on a juridical sight (Rolf, H. W., 2010). Giri capsulation of privacy answers to IoT organizations is discussed in the research work of Sabrina Sicari (Sabrina S., et al., 2015).

It has been immersed in many a factory such as healthcare system traffic organization every governess studying atmospheric looking after digital homes and metropolitan cities. Authorities and studying institutions are utilizing IoT to reshape procedures uses data and supports durability. The utilization of digital tools and wearable tools is built in various institutions (Johnson, L., et al., 2015).

The IoT objects of things are emerging as more advanced curing is wiser and communications have become guiding. However, IoT is preferred in nearly all sectors studying house course health care tourism transportation (Vermesan O. & Friess, P., 2014). The resolved factories studies and persons are aiming to engage the stream of quick advertising with solar Li consideration to IoT tools and network's security. The threat done by those interlinked gadgets harms the safety of devices as well as the whole environment comprising network search, implementations, and social web and hub through a smart tool such as aeronautics devices. In short including a single part or talking mediums in an IoT system can freeze a portion of the complete network system (Nadia C., et al., 2018).

The IoT systems defer and are experiencing various threats and dangers can be categorized into two parts. Initially, it is all about categorizing relying on the files of the IoT organization structures whereas the second handle with the IoT and dangers classification is based on the structural tasks (Krushang, S., & Upadhyay, H., 2014). IoT systems form physical atmospheric relation to the virtual. The polity illustration of IoT structures are shown in Figure 2 IoT comprises three main piles which our perception physical layer web transportation layer and implementation layer.

Figure 2. IoT architecture & layer-wise attacks Source: I. B. Ida, A. Jemai, and A. Loukil, 2016) (S. Babar, et al., 2011)

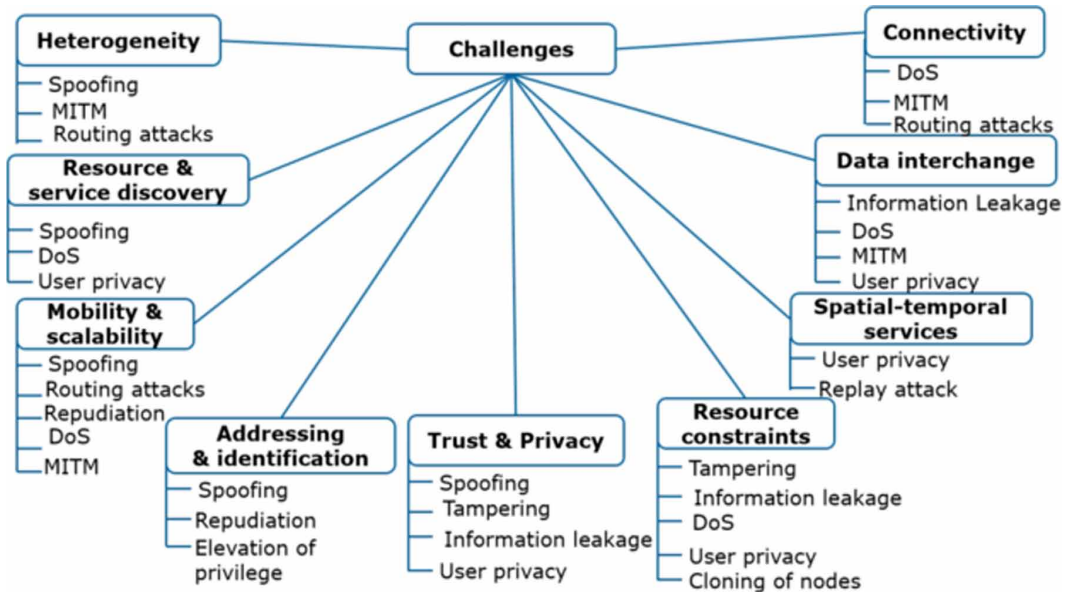


Firstly, the first layer is the physical layer full stop it is made up of different kinds of actuators and sensors that deliver and have data using quality products such as RFID, Bluetooth, and 6LowPan. Secondly, the second layers are a part that sure about the tempting routing sending of data and details. It uses communications files such as Wi-Fi 3G GSM IPv6 etc. The last layer is additionally known as the software layer. It supports a system with the enterprise terms and provides a user interface

(traffic monitoring digital classrooms). Every layer may short different kinds of weaknesses (Ida, I. B., Jemai, A., & Loukil, A., 2016) (Babar, S., et al., 2011).

IoT threats classification by challenges are depicted in Figure 3, and discussed below:

Figure 3. Threat Classification of IoT Source: Nadia, C., et al., 2018



- Heterogeneity and Interoperability:** The backend IoT arrangements consider the utilize of sensors, actuators, and portals given by distinctive sellers and may have distinctive adaptations. To do so, the utilize of dispositive overseeing interoperability between heterogeneous gadgets is needed.
- Connectivity:** A network among distinctive elements of the framework is necessary.
- Mobility and Scalability:** Gadgets of IoT frameworks may be in persistent versatility within the field range; consequently, may alter the bridges they are associated with. This regularly causes disturbance of brokenness and/or associations to unapproved facilities.
- Addressing and Identification:** Field gadgets in IoT applications utilize ordinarily moo control radios for brief remove association (less than 1 kilometer). For that, facilitator hubs distribute neighborhood addresses that do not take after a normal specification, to cohort devices.
- Spatio-temporal services:** Occasions may be categorized by the plentifulness of Spatio-temporal motivation. As a result, information from IoT gadgets of the same frameworks ought to have sensible transient behavior and spatial geolocation.
- Resource constraints:** Nearly All gadgets are little, which implies that they are asset compelled in terms of computing control, onboard memory, arrange transmission capacity, and vitality accessibility. Altering, data spillage and hub cloning are conceivable assaults since the shrewd gadgets and sensors are asset constrained.
- Data Interchange:** Some time recently information compatibility starts, it must be scrambled at the source IoT hubs. The encryption components depend on the sort of equipment, its computational capability, and capacity. Unseemly choice leads to security vulnerabilities such as data leakage.
- Resource and service discovery:** Instruments of asset and benefit revelation ought to be conveyed to empower independence and auto-finding of the devices.

- i. *Trust and privacy*: Savvy sensor gadgets oversee touchy client data (e.g., client propensities, patient's information, gracious assurance information, etc.); consequently, secrecy and information assurance are amazingly important.

Ida et al. proposed an orderly think about the security issues within the IoT for a framework on cloud computing stages. This thinks about given an investigation of IoT security vulnerabilities by illustrating security challenges in eHealth frameworks associated with cloud stages and examined arrangements to basic security dangers commonly emerging in these situations. They too proposed a novel cloud-based IoT framework (Ida, I. B., Jemai, A., & Loukil, A., 2016). The gadgets in IoT encourage the today's life of individuals. In any case, IoT has a gigantic danger to security and security due to its diverse and energetic nature. Confirmation is the foremost difficult security necessity in an IoT ecosystem, where a client (outside party) can straightforwardly get to data from the gadgets, given the common confirmation between client and gadgets happens (Sravani, C., et al., 2017).

The cyber-attack for IoT will bring awesome misfortune to inhabitants and businesses. The IoT framework is defenseless to a few cyber-attacks like Refusal of Benefit (DoS) assault, particular sending, fake directing data, and listening in (Zhao, K., & Ge, L., 2013). Among the cyber-attack, DOS assault may be a broadly utilized strategy. Due to the danger of cyber-attack, the security examination of the IoT framework is essential. The clients need gadgets that fair work, that requires negligible interaction in arrange to operate properly and they do not take into thought the security issues (Alanazi, S., et al., 2015). Vitality utilization and adaptability issues are exceptionally imperative cross-platform concerns. Most of the gadgets are planned without security best-practice in intellect, and issues show up both at the program and equipment levels. After a security exploit is distinguished, the method of upgrading is not mounting in a sensible time, and in some cases, it is missing (Cristian, S., Octavian, G., Răzvan, R., 2018).

Since IoT includes associated gadgets, it is basic to have confirmation at the gadget level moreover. Subsequently, security is to be protected whereas picking up get to savvy IoT scenarios. Believe-related issues also exist in IoT applications. As belief may be a complex idea, it is challenging to depend on trust-based choices. Especially believe the administration is related to get to control and personality administration. Believe-based conventions or dependability examination components are in this manner essential (Niraja, K. S., & Sabbineni S. R., 2020).

CyExec is, accepting the presentation of higher instruction teach and little and medium-sized ventures is the work out a framework to memorize the fundamental procedures of cyber-attack and defense (S. Toyoda, S., et al., 2018). The underneath records appeared the characteristics of the CyExec (Maki, N., et al., 2020):

- Highly convenient work out the environment at a moo fetched.
- Exercise environment of appropriate joint advancement and utilization CyExec upgrades the usage of workout programs by joint improvement and utilize of not as it were a single organization but to a related organization.

In arrange to realize joint improvement and utilize numerous higher instructions to educate, it is essential to create and utilize workout programs between distinctive education productively employing a holder innovation like Docker (Sanggyu, S. and Yoichi, S., 2020).

PROPOSED FRAMEWORK

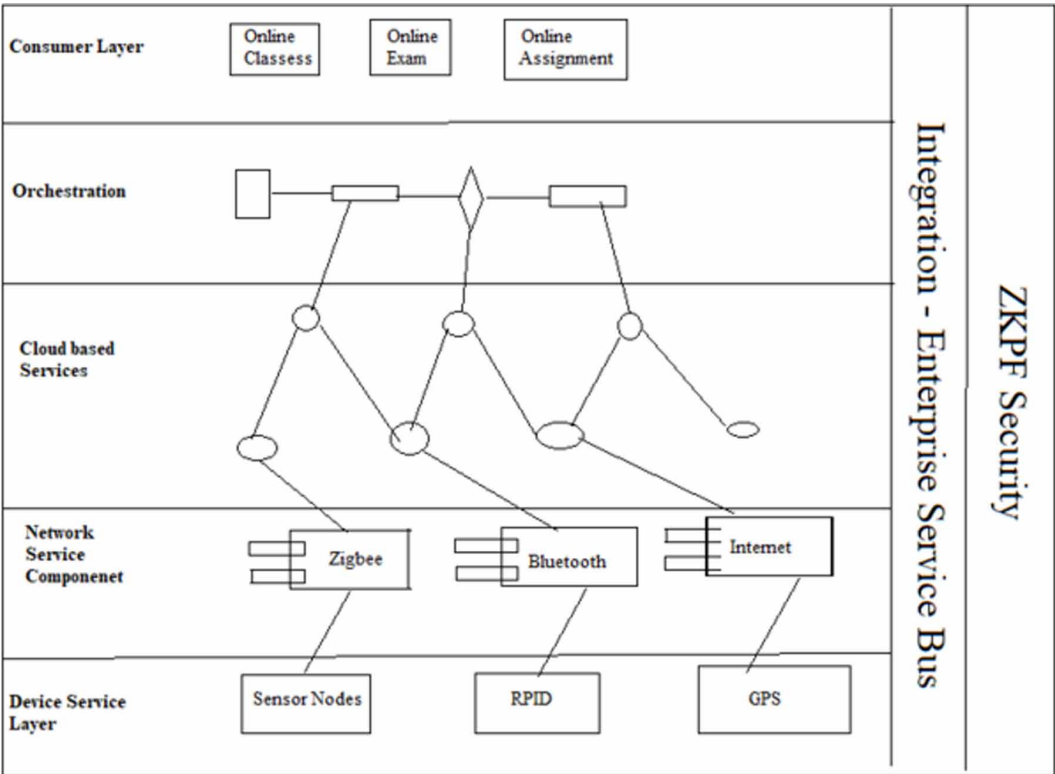
In this manuscript, a robust CoT and service-oriented architecture (SOA) (Josuttis, N. M., 2007) based framework for an online learning system has been proposed, which is shown in Figure 3. In Figure 3, the loosely coupled platform-independent, technology-independent services address the different

tasks of online education services. Starting from the bottom, the device service layer comprises sensor nodes, RFID, GPS, etc. This service layer captures raw data from the real-world and provides it to its upper layer, namely Network Service Components. The Network Service Components comprises of different network component services, namely Zigbee, Bluetooth, Internet, etc. to provide the raw data as captured by Device Layer to Cloud-based service Layer.

The Cloud-based service Layer provides the cloud storage service, computational services, etc. to process the raw data from the device layer. The business request, applications, data, and infrastructure are properly configured at the orchestration layer. After the orchestration process, the different online education services, namely online classes, online exams, online assignment submission, etc. services are available at the consumer layer. The Integration Enterprise Service bus integrates all services. To make the proposed framework to be more agile, a Zero-knowledge Proof Security System(ZKPF) has been introduced. The proposed framework based on SOA is shown in Figure 4.

Thus as said above in Figure 4, the role of the device layer is to access raw data from environment and after that the said data is passed to its upper layer, namely Network Service Component. The different components of this layer, namely Zigbee, Bluetooth, Internet, etc. passes the said data to cloud storage services offered by cloud-based services that exist above this layer. Furthermore, the automated configuration, management, and coordination are done at the above layer it. Consumers can

Figure 4. Proposed Framework based on SOA



access the different services provided they have to prove them as authorized users using the proposed ZKPF security mechanism. Furthermore, the proposed framework, which is a Smart Web-Based Learning and Teaching Platform, has been implemented using the concept of Angular technology for the development of the frontend. Spring Boot has been used for the development of the back-end, whereas MySQL has been used as the database system. The controller XML for the same is shown in Figure 5. In Figure 5, dependency 'spring-boot-starter-thymeleaf' initiates the execution of thymeleaf, with the help of frontend Angular. Thymeleaf is a modern server-side Java template engine for both web and standalone environments, this helps for the development and execution of frontend technologies. For the initialization of the entire client-side tools and technologies 'spring-boot-starter-web' dependency has been used, whereas for the purpose of management 'spring-boot-devtools' has been used here. Furthermore, in this endeavor Project Lombok has been used. Project Lombok is a Java library tool that generates code for minimizing boilerplate code. The library replaces boilerplate

Figure 5a. The Controller xml

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/mo
  <modelVersion>4.0.0</modelVersion>
  <parent>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-parent</artifactId>
    <version>2.1.8.RELEASE</version>
    <relativePath/> <!-- lookup parent from repository -->
  </parent>
  <groupId>com.eduClasses</groupId>
  <artifactId>platform</artifactId>
  <version>0.0.1-SNAPSHOT</version>
  <name>platform</name>
  <description>Edu Classes platform</description>

  <properties>
    <java.version>1.8</java.version>
  </properties>
```

Figure 5b. The Controller xml

```
</dependency>
<dependency>
  <groupId>org.projectlombok</groupId>
  <artifactId>lombok</artifactId>
  <optional>true</optional>
</dependency>
<dependency>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-starter-data-jpa</artifactId>
</dependency>
<dependency>
  <groupId>com.h2database</groupId>
  <artifactId>h2</artifactId>
  <scope>runtime</scope>
</dependency>
<!-- MySql dependency -->
<dependency>
  <groupId>mysql</groupId>
  <artifactId>mysql-connector-java</artifactId>
</dependency>
```

Figure 5c. The Controller xml

```

</dependency>
<dependency>
    <groupId>org.projectlombok</groupId>
    <artifactId>lombok</artifactId>
    <optional>true</optional>
</dependency>
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-data-jpa</artifactId>
</dependency>
<dependency>
    <groupId>com.h2database</groupId>
    <artifactId>h2</artifactId>
    <scope>runtime</scope>
</dependency>
<!-- MySql dependency -->
<dependency>
    <groupId>mysql</groupId>
    <artifactId>mysql-connector-java</artifactId>
</dependency>

```

Figure 5d. The Controller xml

```

</dependency>

<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-test</artifactId>
    <scope>test</scope>
</dependency>
</dependencies>

<build>
    <plugins>
        <plugin>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-maven-plugin</artifactId>
        </plugin>
    </plugins>
</build>

:/project>

```

code with easy-to-use annotations. Here a dependency for Java Persistence API (JPA) has been used. Spring Boot JPA is a Java specification for managing relational data in Java applications. It allows accessing and persisting data between Java object or class and relational database. JPA follows Object-Relation Mapping (ORM). The implementation of all details is shown in controller XML(Figure 5).

PROPOSED ZERO KNOWLEDGE PROOF (ZKPF) ALGORITHM

The concept of the Zero-Knowledge proof (ZKPF) algorithm as found in the literature (Eli, B. S et al.,2015) (Alex, B. G. et al. 2019) is shown using the activity diagram in Figure 6.

Figure 6. The Zero Knowledge Proof System (Eli, B. S et al. 2015) (Alex, B. G. et al. 2019)

In Figure 6, a user has to prove that he or she is an authorized user. For this, his or her credentials would be checked by the verifier. The verifier (in Figure 6, it is shown by authenticated server) challenges the user (i.e. prover) by asking question from the question data bank (which is shown in Figure 6). If user gives the correct answer for a large number of iteration, then it is assumed that he or she is an authorized user otherwise not. In this manuscript, the existing ZKPF algorithm has been modified and a new approach has been proposed. Here, the proposed ZKPF algorithm is based on the concept of Hadamard matrices. The concept of Hadamard matrices was first introduced by Hadamard, J. (1893) (Hadamard, J. (1893). A Hadamard matrix of order n is a matrix denote by H_n comprises of “1” and “-1”, so that the product $H_n * H_n^T = n I_n$ (K. J., 2007). It is observed that Hadamard matrices exist for $n=1,2$ or $4k$, where k belongs to a set of Natural Number N .

Henceforth, the different types of Hadamard matrix as found in the literature are given below:

$$H_1 = [1]_{1 \times 1}$$

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}_{2 \times 2}$$

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}_{4 \times 4}$$

and so on.

Some properties of Hardmard matrices as observed in the literature (Horadam, K.J, 2006) are given below:

- a) The inner product of any two rows or columns of Hardmard Matrix follows the Orthogonal property i.e $R_i * R_j = 0$, for all R_i, R_j

Where R_i represents an i^{th} row of the Hardmard matrix, R_j represents the j^{th} row of the Hardmard matrix.

Similarly, it can be implemented for columns of the Hadamard Matrix.

- b) Hardmard matrix remains invariant under transposition.

$$\text{i.e } H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}_{2 \times 2}$$

$$\text{Again } H_2^T = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}_{2 \times 2}$$

Here H_2^T is also a Hardmard matrix.

- c) If two rows or columns of a Hardmard matrix is permuted then the resultant matrix is also a Hardmard matrix.
- d) If a row or column of a Hardmard matrix is multiplied by “-1” then the resultant matrix is also Hardmard Matrix.

- e) Two Hadamard matrices are equivalent if they are converted into each other using the above properties c) and d).
- f) If H_1 be Hadamard matrix of order n_1 and H_2 be another Hadamard matrix of order n_2 then the

Kronecker product or tensor product $H_1 \otimes H_2$ is also a Hadamard matrix of the order $n_1 \times n_2$.

- g) Furthermore, the Sylvester Hadamard matrices belong to the family $\{S_k = S_1 : \otimes^t k \geq 1\}$

The Hypothesis of the proposed ZKPF algorithm is given below :

Hypothesis 1: For the formation of the Hadamard code, the Hadamard matrix of the form H_2^n , where $n \in \mathbb{N}$ (Sylvester – Hadamard matrix) are only considered.

Hypothesis 2: The entity ‘1’ of the Hadamard matrix is denoted by “White Colour”.

Hypothesis 3: The entity ‘-1’ of the Hadamard matrix is denoted by “Black Colour”.

Hypothesis 4: Proposed algorithm must follow orthogonal property of Hadamard matrix, ie.

$$R_i * R_j = 0, \text{ for all } R_i, R_j.$$

Where R_i represents the i th row of Hadamard matrix

R_j represents the j th row of the Hadamard matrix.

Hypothesis 5: $\mathbf{H}_n \mathbf{H}_n^T = n \mathbf{I}_n$, where $\mathbf{I}_n$ is an identity matrix of order n .

Hypothesis 6:

$$A = \begin{bmatrix} a_{11}, a_{12} & \dots & a_{1n} \\ a_{21}, a_{22} & \dots & a_{2n} \\ \vdots & & \vdots \\ a_{m1}, a_{m2} & \dots & a_{mn} \end{bmatrix}_{m \times n}$$

If A be a Hadamard matrix of order $m \times n$ and B is another Hadamard matrix, then Kronecker product of matrices A and B is defined as (Hadamard, K.J., 2007)

$$A \otimes B = \begin{bmatrix} a_{11}B, a_{12}B & \dots & a_{1n}B \\ a_{21}B, a_{22}B & \dots & a_{2n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B, a_{m2}B & \dots & a_{mn}B \end{bmatrix}_{m \times n}$$

Hypothesis 7: Every Hadamard matrix would be represented using the row-major technique. Each '1' would be represented by 'white' color and '-1' by 'black' color, whereas the row separation by any color apart from white and black. Here red cooler has been used for row separation.

The process is illustrated as:

For

$$H2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}_{2 \times 2}$$

The color pattern would be



For

$$H4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}_{4 \times 4}$$

The color pattern would be



Hypothesis 8: After receiving the color pattern, it is again reconstructed as a Hadamard matrix.

For example, for color pattern



The matrix color pattern would be



And the corresponding Hadamard matrix would be

$$H2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}_{2 \times 2}$$

And so on.

The above-mentioned Hypothesis from 1 to 8 are provided to valid users by the online education service provider through private channels.

Now, when anyone requests for online education service from the online education service provider then the proposed ZKPF will check the authorization of users using a series of challenge-response patterns. By this challenge-response pattern, the user (prover) is checked whether he/she is an authorized user or not by the proposed ZKPF (verifier).

Here, the proposed algorithm comprises of two parts, one for verifier, which is given in Algorithm1, and the other for prover, which is given in Algorithm 2. Algorithm1 and Algorithm2 are given in Figure 7 and Figure 8 respectively. Algorithm 1 (which is shown in Figure 7) checks the authenticity of a user (i.e. prover) by the process of a challenge-response pattern after getting a request from the user. For this, the verifier generates a random number, say, n and after that computes a number, say, $m = 2^n$. Now a Hadamard matrix of order $m \times m$ i.e. H_m is chosen from the set of Hadamard matrices and then after it is converted into a color pattern, say, k as per Hypothesis 7. After that the proposed Algorithm1 generates another whole number, say $m1$ such that $m1$ is greater than m , and then calculates $s = 2^{m1}$. Now it sends $\langle k, s \rangle$ as challenge to user(prover). It then accepts a response from the user, say, $k1$. Now, $k1$ is converted into Hadamard matrix as per Hypothesis 8 and then after checks its orthogonal property as per the Hypothesis 4. If an orthogonal property is not satisfied then the user is considered as authorized user and Algorithm1 ends otherwise verification process would continue for a large number of iteration and if user credentials are maintained throughout the iteration then the user would be declared as an authorized user otherwise not.

The proposed Algorithm 2 (which is shown in Figure 8) accepts $\langle k, s \rangle$ from verifier converts k into Hadamard matrix, H_m using Hypothesis 8. After that a Hadamard matrix of order $s \times s$, say, H_s , is considered from the set of Hadamard Matrices. Now a new Hadamard matrix is generated, say, H as per Hypothesis 6. After that H is converted into a color pattern, say, $k1$ as per Hypothesis 7, and then it is sent to the verifier by the user(prover) to check the credentials of user.

Figure 7. Proposed Algorithm1 for Verifier

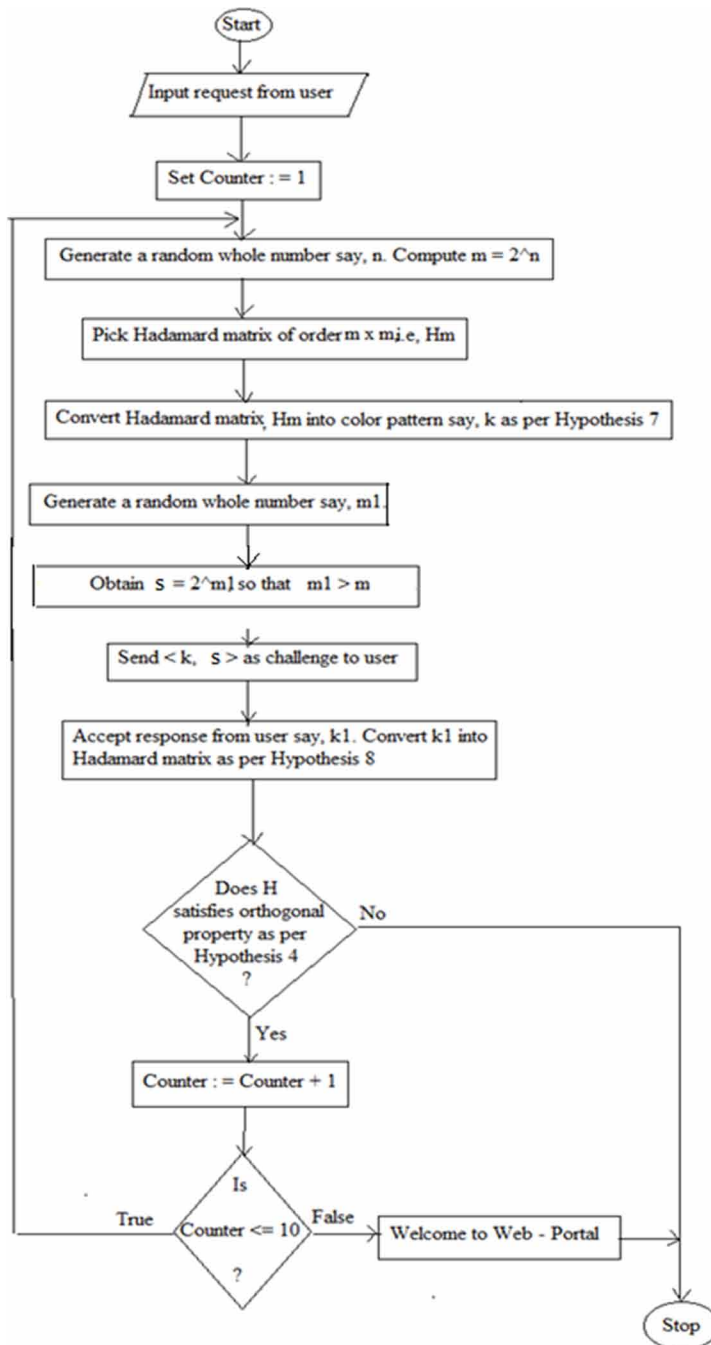
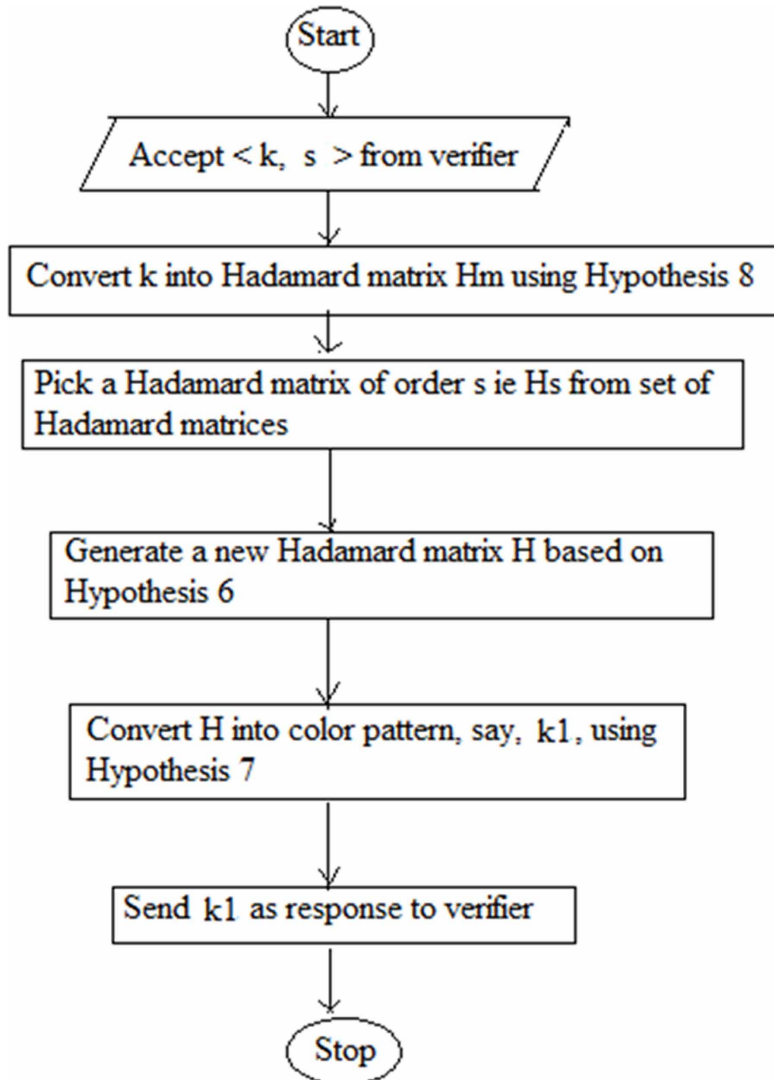


Figure 8. Proposed Algorithm2 for the prover



Robustness of the Proposed Algorithm

Due to the combinatorial nature of the formation of the Hadamard matrix based on Sylvester's construction of the Hadamard matrix, the proposed algorithms are very reliable and robust against any brute force attack as compared to the existing approaches.

Experimental Setup and Result

The proposed algorithms, namely Algorithm 1 and Algorithm 2 have been implemented using the Python programming language. The numerical evaluation of proposed Algorithm1 is shown in Table 1. Its corresponding graph is shown in Figure 9. Moreover, the numerical evaluation of the proposed Algorithm 2 is shown in Table 2 and its corresponding graph is shown in Figure 10. Figure 9 and Figure 10 imply the combinatorial nature of the proposed algorithms and hence are more robust by nature against any brute force attack.

Table 1. Time required for algorithm 1

Iteration	Time taken for verifier(in ms)
1	1
2	4
3	9
4	16
5	25
6	36
7	49

Obviously, the time complexity of proposed Algorithm1 consists of the time complexity for the generation of the random numbers, time complexity for converting the Hadamard Matrix into color pattern. By inspection the time complexity of proposed Algorithm1 is $O(n^2)$. Furthermore,

Figure 9. Graphical representation of Algorithm 1

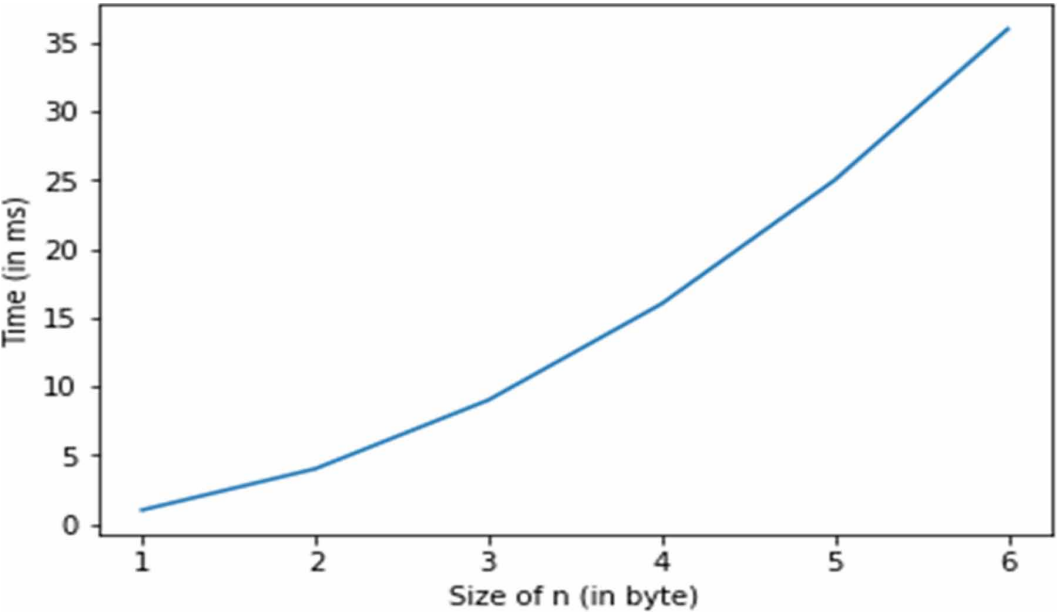
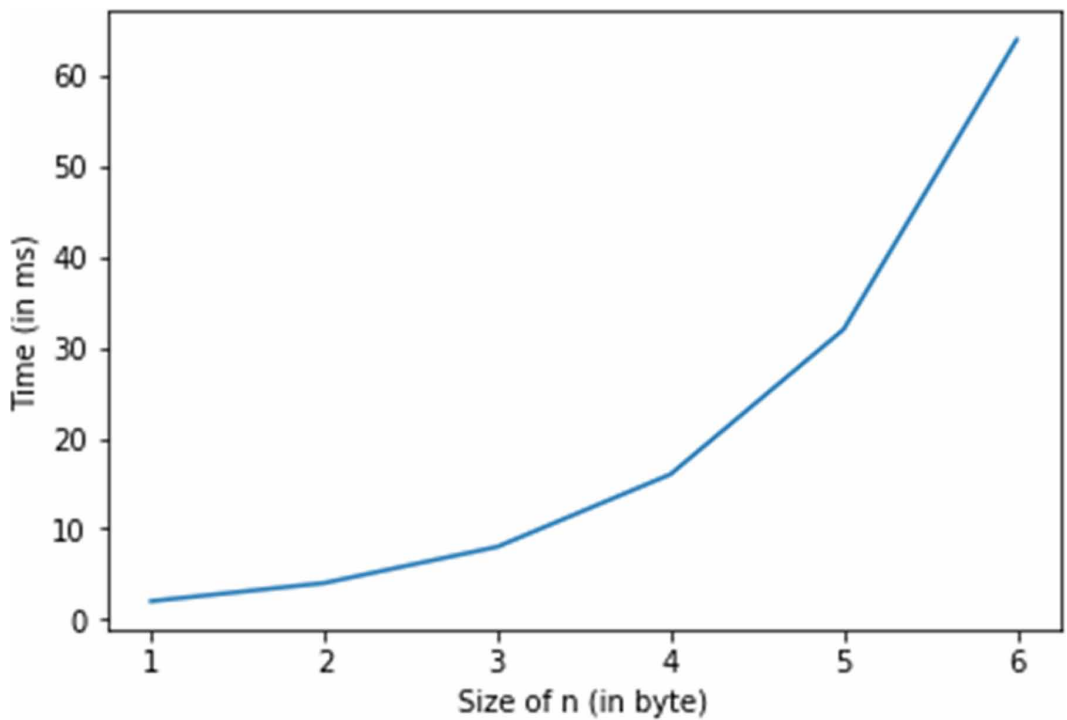


Table 2. Time required for algorithm 2

Iteration	Time taken for prover (in ms)
1	4
2	16
3	64
4	256
5	1024
6	4096
7	16384

Figure 10. Graphical representation of Algorithm 2



by inspection the time complexity of proposed Algorithm2 is found to be $O(2^{2n})$. The graphical representation of the simulated result of proposed Algorithm1 and Algorithm2 are shown in Figure 9 and Figure 10 respectively.

CONCLUSION

In this manuscript, a novel cloud of things (COT) based online education system framework has been introduced. To make the proposed framework to be more agile, the concept of service-oriented architecture (SOA) has been incorporated in the proposed framework. Furthermore, for the security of the proposed framework, the concept of the zero-knowledge proof (ZKPF) system concept has been incorporated in the proposed framework. In this endeavor, a more robust concept of ZKPF has been introduced based on the Hadamard matrix. Experimental results have been shown to lay bare the effectiveness of the proposed approach.

REFERENCES

- Abuarqoub, A., Abusaimh, H., Hammoudeh, M., Uliyan, D., Abu-Hashem, M. A., Murad, S., Al-Jarrah, M., & Al-Fayez, F. (2017). A survey on Internet of Things Enabled Smart Campus Applications. *Proceedings of ICFNDS '17: International Conference on Future Networks and Distributed Systems*.
- Alanazi, S., Al-Muhtadi, J., Derhab, A., & Saleem, K. (2015). On resilience of Wireless Mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications. *Proceedings of International Conference on EHealth Networking, Application & Services*.
- Alex, B. G., William, S., & Henry, Y. (2019). Perfect zero knowledge for quantum multiprover interactive proofs. *Proceedings of IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, 611-635.
- Asim, M., & Mahmood, A. (2018). How Internet-of-Things (IoT) Making the University Campuses Smart? QA Higher Education (QAHE) Perspective. *Proceedings of IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*.
- Azamat, Z., Zhulduz, S., Rassim, S., & Zhazira, K. (2017). IoT smart campus review and implementation of IoT applications into education process of university. *Proceedings of 13th International Conference on Electronics, Computer and Computation (ICECCO)*.
- Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for Internet of Things (IoT). *Proceedings of 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE)*, 1-5.
- Chenn-Jung, H., Ming-Chou, L., San-Shine, C., & Chin-Lun, C. (2004). Application of Machine Learning Techniques to Web-Based Intelligent Learning Diagnosis System. *Proceedings of Fourth IEEE International Conference on Hybrid Intelligent Systems (HIS'04)*.
- Chih-Ming, C., Ting-Chun, H., Tai-Hung, L., & Chia-Meng, H. (2007). Personalized E-Learning System with Self-Regulated Learning Assisted Mechanisms for Promoting Learning Performance. *Proceedings of Seventh IEEE International Conference on Advanced Learning Technologies (ICALT 2007)*.
- Chin-Ming, H., Chih-Ming, C., Mei-Hui, C., & Shin-Chia, C. (2007). Intelligent Web-based Tutoring System with Personalized Learning Path Guidance. *Proceedings of Seventh IEEE International Conference on Advanced Learning Technologies (ICALT 2007)*.
- Conrad, F. G., Couper, M. P., Tourangeau, R., & Peytchev, A. (2010). The impact of progress indicators on task completion. *Interacting with Computers*, 22(5), 417-427.
- Cristian, S., Octavian, G., & Răzvan, R. (2018). Why IoT security is failing. The Need of a Test Driven Security Approach. *Proceedings of 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*.
- Education, S. R. I. (2014). *Research on the use of Khan Academy in schools*. http://www.sri.com/sites/default/files/publications/2014-03-07_implementation_briefing.pdf
- Eli, B. S., Alessandro, C., Matthew, G., Eran, T., & Madars, V. (2015). Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs. *Proceedings of IEEE Symposium on Security and Privacy*, 287-304.
- Fang-Fang, C., & Eng-Soon, T. (2012). Developing Virtual Learning Environment 2.0 Using Web Services Approach. *Proceedings of 12th IEEE International Conference on Advanced Learning Technologies*.
- Feng-Hsu, W., & Dai-Yan, C. (2008). A Knowledge Integration Framework for Adaptive Learning Systems Based on Semantic Web Languages. *Proceedings of Eighth IEEE International Conference on Advanced Learning Technologies*.
- Filvà, D. A., Guerrero, M. J. C., & Forment, M. A. (2014). *Google Analytics for Time Behavior Measurement in Moodle* [Paper presentation]. The Information Systems and Technologies (CISTI), 9th Iberian Conference on, Barcelona, Spain.
- Frolov, I., & Johansson, S. (2013). *An adaptable usability checklist for MOOCs. A usability evaluation instrument for Massive Open Online Courses* [Unpublished doctoral dissertation]. Umeå University, Sweden.
- Grunewald, F., Meinel, C., Totschnig, M., & Willems, C. (2013). Designing MOOCs for the Support of Multiple Learning Styles. *Lecture Notes in Computer Science*, 8095, 371-382.

- Hadamard, J. (1893). Resolution d'une question relative aux determinants, *Bulletin des Sciences Mathematiques. Gauthier-Villars, Paris*, 17, 240–246.
- Hamidreza, M., & Chin, W. M. (2013). An analysis of web-based formative assessment systems used in elearning environment. *Proceedings of IEEE 13th International Conference on Advanced Learning Technologies*.
- Harris, W. (2006). An Access Control Scheme for Web-Based E-Learning Systems. *Proceedings of 7th International Conference on Information Technology Based Higher Education and Training*.
- Hidenori, A., Tsuyoshi, K., Seiichi, K., & Mariko, A. (2012). Evaluation of Lecture Using Web-based e-learning and Development of Rapid e-learning System. *Proceedings of IEEE International Conference on Information Technology Based Higher Education and Training (ITHET)*.
- Horadam, K. J. (2006). *Hadamard Matrices and Their Applications*. Princeton University Press.
- Ida, I. B., Jemai, A., & Loukil, A. (2016). A survey on security of IoT in the context of eHealth and clouds. *Proceedings of 11th International Design Test Symposium (IDT)*, 25–30.
- Iyad, A., & Elizabeth, B. (2008). Empowering Web-based Learning with Semantic Web Technologies: The Case of SWLinker. *Proceedings of Eighth IEEE International Conference on Advanced Learning Technologies*.
- Johnson, L., Becker, S., Estrada, V., & Freeman, A. (2015). *The NMC horizon report: 2015 higher education edition*. The New Media Consortium.
- Josuttis, N. M. (2007). *SOA in Practice: The Art of Distributed System Design*. O'Reilly Media.
- Kraijak, S., & Tuwanut, P. (2015). A survey on iot architectures, protocols, applications, security, privacy, real-world implementation and future trends. *Proceedings of 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*.
- Krushang, S., & Upadhyay, H. (2014). A Survey: DDOS Attack on Internet of Things. *International Journal of Engineering Research and Development*, 10(11), 58–63.
- Lei, Pahl, & Donnellan. (2003). An Evaluation Technique for Content Interaction in Web-based Teaching and Learning Environments. *Proceedings of 3rd IEEE International Conference on Advanced Learning Technologies (ICALT'03)*.
- Lilla, N., & Adrian, C. (2019). Router-based IoT Security using Raspberry Pi. *Proceedings of 18th RoEduNet Conference: Networking in Education and Research (RoEduNet)*.
- Luigi, A. (2010). The internet of things: A survey. *Computer Networks*, 54(15), 2787–2805.
- Maki, N. (2020). An Effective Cybersecurity Exercises Platform CyExec and its Training Contents. *International Journal of Information and Education Technology (IJIET)*, 10(3), 215–221.
- Md Mahmud, H. (2015). Towards an analysis of security issues, challenges, and open problems in the Internet of Things. *Proceedings of IEEE World Congress on in Services (SERVICES)*, 21–28.
- Meola, A. (2016). *How the internet of things will affect security & privacy* (Vol. 8). Business Insider.
- Muhammed, A. S., & Derya, U. (2020). Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users' Perspectives. *Proceedings of 8th International Symposium on Digital Forensics and Security (ISDFS)*.
- Nadia, C., Mohamed, M., Akka, Z., Cyrille, S., & Parvez, F. (2018). Network Intrusion Detection for IoT Security based on Learning Techniques. *IEEE Communications Surveys and Tutorials*, 00(0).
- Niraja, K. S., & Sabbineni, S. R. (2020). Security Challenges and Counter Measures in Internet of Things. *Proceedings of IEEE International Conference on Computer Communication and Informatics (ICCCI -2020)*.
- Perry, J. S. (2017). *Anatomy of an IoT malware attack (2017)*. <https://developer.ibm.com/articles/iot-anatomy-iot-malware-attack/>
- Rolf, H. W. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23–30.

- Rune, P. G., & Svensson, Y. W. (2002). On Web-Based Learning - Experiences from Teaching and Learning Online. *Proceedings of 34th Annual Conference of the International Visual Literacy Association*. doi:10.1109/ICALT.2003.1215090
- Sabrina, S. (2015). Security, privacy, and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.
- Sanggyu, S., & Yoichi, S. (2020). Development of IoT Security Exercise Contents for Cyber Security Exercise System, *Proceedings of 13th International Conference on Human System Interaction (HSI)*, 281-286.
- Sari, P. (2017). Study of Smart Campus Development Using Internet of Things Technologies. *Proceedings of 2nd International Conference on Computational Fluid Dynamics in Research and Industry (CFDRI 2017)*, 243(2), 1-5.
- Saxena, A., Shinghal, K., Misra, R., & Agarwal, A. (2019). Automated Enhanced Learning System using IOT, *Proceedings of 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*.
- Scully, P. (2020). *IoT Platforms Market Report 2018-2023*. <https://iot-analytics.com/wp/wp-content/uploads/2018/07/IoT-Platforms-Market-Report-2018-2023-June-2018-SAMPLE-NEW-vf2.pdf>
- Stravani, C., Mohammad, W., Das, A. K., & Kumar, N. (2017). Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. *IEEE Access*, 5, 1-16.
- Te-Lien, C., & Sufen, C. (2015). The effects of progress bars on diverse learning styles in web-based learning. *Proceedings of IEEE 15th International Conference on Advanced Learning Technologies*.
- Terry, G., Damon, K., Michael, C., & Marbin, P. R. (2018). IoT Platform for Engineering Education and Research (IoT PEER)—Applications in Secure and Smart Manufacturing. *Proceedings of IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation*.
- Toyoda, S. (2018). Proposal of Cyber-attack and defense Exercise system CyExec composed of ecosystem. *CSS2018*.
- Vermesan, O., & Friess, P. (2014). *Internet of Things Applications - From Research and Innovation to Market Deployment*. River Publishers.
- Wang, T. H. (2008). Web-based quiz-game-like formative assessment: Development and evaluation. *Computers & Education*, 51(3), 1247–1263. doi:10.1016/j.compedu.2007.11.011
- Wang, T. H. (2012). Developing Web-based assessment strategies for facilitating junior high school students to perform self-regulated learning in an e-Learning environment. *Computers & Education*, 57, 1801–1812.
- Waseem, I., Haider, A., Mahmoud, D., Bilal, R., & Yawar, A. (2020). An In-Depth Analysis of IoT Security Requirements, Challenges and their Countermeasures via Software Defined Security. *IEEE Internet of Things Journal*, 7(10).
- Weston, T. J. (2001). Implementing, and Evaluating Web-Based Learning Modules for University Students. *Educational Technology*, 41(4), 15–22.
- Williams, Z. D., Scully, P., & Lueth, K. L. (2020). *IoT Analytics Market Insights for the Internet of Things*. <https://iot-analytics.com/>
- Yi, J. (2005). Building a Web-Based Collaborative Learning Environment. *Proceedings of 6th Annual International Conference ITHET*.
- Zaiane, O. R. (2001). Web usage mining for better Web-based learning environment. *Proceedings of Conference on Advanced Technology for Education*, 60-64.
- Zhao, K., & Ge, L. (2013). A Survey on the Internet of Things Security. *Proceedings of International Conference on Computational Intelligence & Security*, 663-667.
- Kuntal Mukherjee is working as Assistant Professor at the Department of Computer Science & Engineering in Birla Institute of Technology, Mesra, Ranchi, India. He has 30 publications with 227 citations, h-index of 07, i10-index of 07.
- Sudhanshu Maurya, Post-Doctoral Researcher, School of Computer & Communication Engineering, Universiti Malaysia Perlis (UniMAP), Malaysia. Currently, he is designated as Assistant Professor, School of Computing, Graphic Era Hill University, Bhimtal Campus, Uttarakhand. His area of research is Cloud Computing, IoT and Machine Learning.