An Adaptive Approach for Preserving Privacy in Context Aware Applications for Smartphones in Cloud Computing Platform

H. Manoj T. Gadiyar[1]*, Thyagaraju G. S[2], R.H. Goudar[3]
Assistant Professor, Department of Computer Science & Engineering
Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire – 574240, Karnataka, India[1]
Visvesvaraya Technological University, Belagavi, Karnataka, India[1]
Sri Dharmasthala Manjunatheshwara Institute of Technology, Ujire – 574240, Karnataka, India[2]
Visvesvaraya Technological University, Belagavi, Karnataka, India[3]

***Abstract*—With the widespread use of mobile phones and smartphone applications, protecting one's privacy has become a major concern. Because active defensive strategies and temporal connections between situations relevant to users are not taken into account, present privacy preservation systems for cell phones are often ineffective. This work defines secrecy maintenance issues similar to optimizing tasks, thereby verifying their accuracy and optimization capabilities through a hypothetical study. Many optimal issues arise while preserving one's privacy and these optimal issues are to be addressed as linear programming issues. By addressing linear programming issues, an effective context-aware privacy-preserving algorithm (CAPP) was created that uses an active defence strategy to determine how to release a user's current context to enhance the quality of service (QoS) regarding context-aware applications while maintaining secrecy. CAPP outperforms other standard methodologies in lengthy simulations of actual data. Additionally, the minimax learning algorithm (MLA) optimizes the policy users and improves the satisfaction threshold of the context-aware applications. Moreover, a cloud-based approach is introduced in the work to protect the user's privacy from third parties. The obtained performance measures are compared with existing approaches in terms of privacy policy breaches, context sensitivity, satisfaction threshold, adversary power, and convergence speed for online and offline attacks.**

Keywords*—Context-aware; privacy; active defence; privacy protection and mobile phones

I. Introduction

Mobile phones are used extensively, and apps are commonly produced for smartphones. "Context-aware applications specifically help users by providing contextually relevant tailored services [1], [2]. Context-aware applications may use sensors (e.g., GPS) to determine their owner's location and state. These sensory data may be used to determine a user's context or condition. For example, a user's position may be relayed via GPS, their movement assessed by accelerometers, and their voice and scene captured by cameras and microphones. Context-aware applications may use the inferred context to provide context-aware tailored services [3]. Health Monitor can track daily activity and intelligently mutes the phone without the help of the user. Context-aware applications improve people's lives and convenience yet also compromise privacy. Some untrusted aware applications may be highly prone to leakage of user's context privacy to the adversary. These adversaries may sell the user privacy for commercial purposes, resulting in a reduction of QoS of the context applications. In reality, most users would not object to allowing context-aware applications to access associated sensory data because of its convenience; thus, avoiding the danger of context-privacy exposure while delivering context-related services is becoming more important [4].

Constantly changing human situations and actions in everyday life make it difficult to maintain context-privacy for mobile phones [5]. As a matter of fact, a Markov chain may represent temporal relationships across human settings. By introducing temporal correlation among present contexts can estimate the past and future usage of context applications more efficiently. Because the naïve method ignores temporal connections between user contexts, it fails to secure critical user contexts. With MaskIt [6], sensitive and non-sensitive contexts may be silenced to reduce temporal connections between them. MaskIt's ability to hide additional contexts reduces the QoS given by context aware smartphone applications. This approach uses passive defence, which inevitably reveals some information to opponents determining whether the hidden circumstances are sensitive or not is irrelevant to an opponent. Recent proposals include aggressive defence programmes. To reduce temporal correlations across contexts, the deception approach is introduced in each context called FakeMask. FakeMask releases scenarios that are not genuine but have significance (i.e. the user has a likelihood of being in that context at that moment) [7]. An increased number of actual contexts lead to greater service quality for consumers with such a deception strategy. As a result, it is not suitable for mobile devices [8]. In recent years, many researchers have been fascinated with cloud computing [9, 10] due to the efficient outcome for protecting privacy from the third party.

A. Motivation

With the rapid advances in technology, mobile phones play an important role in users' daily lives. However, privacy leaks are one of the most common problems in smartphones. This research mainly focuses on preserving the privacy of

*Corresponding Author.

smartphone users in context-aware applications using cloud computing. The cloud computing platform can build a firewall between the user and the adversary. Few types of research into optimal policy users have been conducted, but raising the satisfaction threshold remains a challenging approach. However, these approaches do not protect the entire privacy of the user. Mainly location and environment privacy is leaked from the smartphones for commercial purpose. Preventing an adversary's attack requires an efficient approach to better protect user privacy. Although some types of research are taking place in this field, there is also high leakage of users' privacy. These major disadvantages motivate us to develop an efficient approach to protect user privacy from adversary attacks.

A lightweight privacy preservation approach is introduced to develop temporal correlation among every user context to protect one's privacy more effectively. Furthermore, the mobile phone context privacy problem is formulated as an optimization problem and then proves its validity. It is followed by a near-optimum problem (linear programming) to speed up the execution time. By addressing the linear programming issue, an efficient context-aware privacy preserving algorithm (CAPP) is constructed that can select how to release a user's current context to optimize the QoS of context-aware applications with privacy preservation. Extensive simulations are performed to analyze the method performance, and the simulation results show that the proposed algorithm is effective and efficient. This proposed work undergoes the following major contributions to show the better QoS of the developed model:

- This research work mainly focuses on developing a novel approach for preventing leakage of data in context-aware applications for smart phones using cloud computing.
- An effective context-aware privacy-preserving (CAPP) algorithm is introduced to address the linear programming issue.
- Minimax learning algorithm (MLA) is emphasized to optimize the policy users and improve the satisfaction threshold.
- To preserve the user's privacy, the cloud computing approach is evaluated. It mainly creates a firewall between the adversary and the user.
- The evaluation of the proposed work based on privacy policy breaches, context sensitivity, satisfaction threshold, adversary power, and convergence speed for both online and offline attacks are investigated and compared with traditional approaches.

The following sections are organized as follows: Section 2 presents the literature survey related to the developed model; Section 3 describes the proposed method; Section 4 provides results and discussion; Section 5 provides the conclusion of our proposed method.

II. Literature Review

A. Some of the Recently Published Papers are Surveyed below

Wang et al. [11] studied the context-aware implicit authentication of smart phone users based on multi-sensor behaviour. In this method, multi-sensor data like accelerometer, gyroscope, magnetometer, time stamp, pressure and touch size were initially encapsulated to determine one's behaviour. Here, gesture and touch features were drawn from sensed data using a statistical and distance calibration approach. The features are fused using the weighted sum fusion rule, and a one-class support vector machine (SVM) was used to classify the outcome. For experimentation, 1000 sensed data from 80 participants were considered. The overall equal error rate (EER) attained was about 0.0071% in the experimental scenario. However, this method was highly suffered due to leakage of the privacy to the third party.

Alawadhi et al. [12] performed the method toward privacy protection in context aware environment. In this method, the decision making process was introduced to monitor privacy behaviour and personal data usage. This method undergoes three stages: service classifier, privacy preference manager, and privacy controller. The privacy preference module places the privacy preference and analyses the user's data usage. The next module uses service providers under trusted, untrusted and under investigation. The privacy controller detects the usage of data based on service providers. The overall false positive rate (FPR) attained was about 1.5% in the experimental scenario. However, this method suffered due to high optimization problems.

Wan et al. [13] investigated privacy preserving blockchain enabled federated learning in 5G beyond networks. This method introduced machine learning (ML) technique to keep the data efficiently. To prevent raw data sharing, a federated learning-based privacy-preserving ML has been proposed. In addition, the Wasserstein Generative Adversial Network (WGAN) with Differential Privacy (DP) was introduced to prevent unwanted malicious attacks by interpreting the context in FL. The WGAN approach has been proposed to construct the controllable random noise that meets the DP requirements. WGAN with DP helps to achieve the trade-off between privacy and data utility. In the experimental scenario, time delay, accuracy and efficiency were calculated. However, this method preserves data for a single user and cannot be used to preserve data for multiple users.

Ghosh et al. [14] developed the context-aware security scheme to preserve the data in an IoT-enabled society. In this method, an encryption policy attribute-based encryption scheme (CP-ABE) was introduced to efficiently preserve the user's context. In addition, a context-aware attribute learning scheme (CASE) has been proposed to learn the user's contextual information and reduce the size of the encryption data by learning the attributes. The CP-ABE technique manually enforces user data by leveraging edge intelligence in

context-aware applications. In the test scenario, the delay was reduced to 33% with a packet loss of 36%. However, this method suffered from the lack of preserving the users' environmental context information.

Sylla et al. [15] investigated secure and trustworthy context management for context aware security and privacy in the IoT (SETUCOM). In this method, device trust management (DTM) was introduced based on context aware and privacy as a service (CASPaaS). The context information was secured using a Bayesian network and fuzzy logic, and it was considered the lightweight hybrid system. The elliptic curve integrated encryption scheme (ECIES) algorithm generated the security. Advanced encryption standard (AES) was evaluated for context information encryption. In the experimental scenario, the overall time taken to protect the information is about 1200ms. However, this method suffered due to insecurity of the user's privacy and it's highly occurs optimization problems.

Meng et al. [16] had defined the privacy-preserving and sparsity aware location based prediction method for collaborative recommender systems. In this method, a location-based collaborative recommendation algorithm was introduced to achieve the compromise between prediction accuracy and privacy protection. A random jamming approach has been proposed to preserve data users' QoS. In addition, the regional aggregation approach was demonstrated to preserve the location of users. Furthermore, a location-based tensor factorization approach was presented to establish a relationship between services and location to develop location-based predictions. In the test scenario, the overall accuracy achieved was about 92%. However, this method suffered from poor QoS quality and takes more time to preserve the user's location.

B. Problem Formulation

Recently, many advanced techniques have been introduced to prevent user privacy leakage in contextual applications. When used context-aware, third-party intrusion is considered unusual. This happens mainly due to the lack of QoS in the existing approaches. In general, both online and offline attacks occur in context-aware applications. However, these attacks are due to attackers for commercial purposes. The literature review mentioned above greatly affects the previous approaches due to major disadvantages; some of the common disadvantages are high leakage, privacy loss and slow process, etc. Some of the existing papers have large gaps and are manipulated in this section. In [11], the author studied the context-aware implicit authentication of smart phone users based on multi-sensor behaviour to the privacy of the user's context. However, this method was highly prone to leakage of users' privacy and lack of firewall. In [12], the author performed the method toward the privacy protection in context aware environment to preserve the environmental context of the user. However, this method suffered due to optimal issues that resulted in leakage of user privacy to the adversary. In [13] the author examined privacy preservation through blockchain-enabled federated learning in 5G beyond networks. In [14] the context-aware security scheme to preserve the data in an IoT-enabled society. However, this method was highly suffered due to user's location privacy leakage. However, this method suffered due to programming complexity to preserve one's context privacy. In [15], the author proposed secure and trustworthy context management for context aware security and privacy in the IoT (SETUCOM) to improve the QoS of the context applications. However, this method suffered due to the high complexity process and the lack of preserving location privacy more effectively. In [16], privacy-preserving and sparsity aware location based prediction method for collaborative recommender systems has been proposed by the author. However, this method is only useful for getting the user's location.

Few researchers were undertaken to protect users' privacy based on cloud computing. The aforementioned related paper is efficient and shows a better outcome in terms of privacy preservation, but there also arises some leakage due to less improvement in the applied strategy. An effective novel approach needs to be introduced to preserve privacy to overcome this issue. This proposed method gives a clear solution for data protection with better accuracy.

III. Proposed Method

Context aware is the computation of the current situation and information about the environment, places, things that anticipate urgent needs, situate awareness, usable contents and experiences. In this work, a novel approach is developed to prevent an attack from an adversary concerning user's privacy. Initially, CAPP algorithm is introduced to enhance the quality of service (QoS) regarding context-aware applications. Then, the MLA algorithm is emphasized to equalize the optimal policy and improve the satisfaction threshold of the proposed work. The proposed work introduces cloud computing to encrypt users' privacy from a third party. Fig. 1 illustrates the framework of the proposed model.

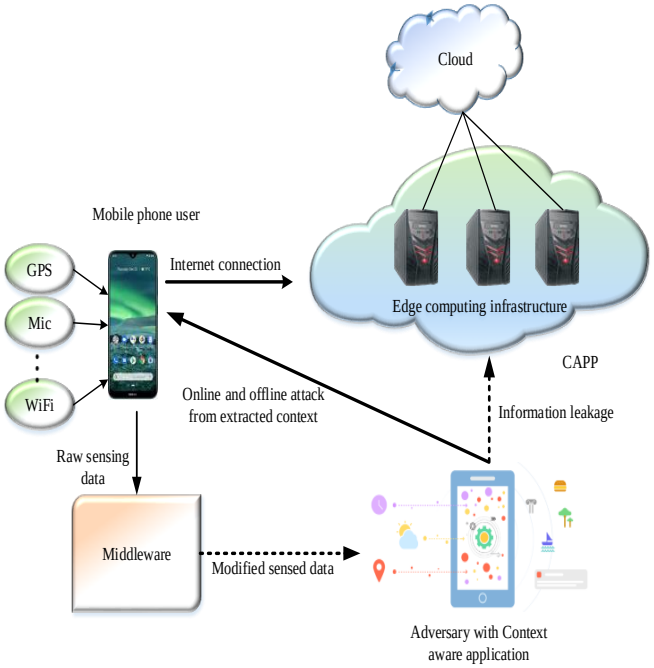


Fig. 1. Framework of the Proposed Method.

Cloud computing is the collection of network servers coordinated with the aid of the internet. The cloud uses firewalls as privacy protection around assets to prevent intruding of third parties. To carry out this evaluation, real smartphones with traces of 94 users to find out the convergence speed of the algorithm. This paper mainly focuses on online and offline attacks due to continuous changing times and user variability.

A. Privacy Problems in Context Aware Privacy Preservation

The private contexts are said to be the context subsets in which leakage is considered the major drawback for the smartphone user. In order to prevent the leakage of privacy, the user must control the emitted information using middleware privacy preservation. Many existing approaches are introduced to overcome the leakage of the user's privacy. Privacy-preserving middleware is used to access the context-aware middleware for the users, but this middleware does not require any permission to access the user's data. Usually, the released data with granularity leaks the privacy of the user. Hence the accuracy of the context recognition is also reduced. The context-aware apps are mainly used for commercial purposes and are considered the adversary. The adversary is a third party intrusion, mainly focusing on reducing the user's utility by adding multiple attacks. The attacks mainly undergo two stages offline and online attacks.

The third party gets the user's personal information such as behavioral contexts, GPS location information, etc. These third parties sell the information for commercial purposes, and users are unaware that the attack leads to a privacy breach. In online attacks, the third party collects the sensed data from the user and understands the user's behavior based on the collected data. According to the behavior, the third party forces the user or makes the user indulge in blackmail or leads to violence.

1) State transition for online attacks: For the online attack, the adversary's strategy is unknown to the user, and the user blindly believes the adversary's strategy from the existing attacks. There are many reasons for the dependence on previous attacks. The third party collects the last context based on the previous approach. Then the present information is coordinated with the past information based on the proposed algorithm. Hence the user should encapsulate the adversary's attacks and which information has been attacked. The attacked time is denoted by n, which clearly shows the time the data gets leaked. The attack of the previous information is indicated as Wr^n, the value of Wr^n is 1 or 0. If the adversary successfully collects the information is denoted as D_{n-1}. The state transitions for the online attacks at the time n is given by, $R^n = \{Wr^n, D_{n-1}\}$.

2) State transition for offline attacks: In an offline attack, the adversary gets the user's personal data such as personal behavior contexts, environmental context, GPS location etc. The adversaries sell one's personal information for money and lead to a privacy breach, and it is unknown to the user. The time n of the user's action is given by, $a^n{}_h = \{a^n{}_{h,1}, ..., a^n{}_{h,E}\}$, the granularity of the sensor's data is denoted as $a^n{}_{h,E} \in [0,1], \forall E = 1, ..., E$. Here, E denotes the complete sensors for the purpose of recognition. The recognition of the context in terms of accuracy with the limit ranges from $t\ (0 \le t \le 1)$ is given by,

$$t = \sum_{E=1}^{E} E_e a_{h,E}{}^n \tag{1}$$

Here, $\{E_e : \forall E\}$ denotes the weight of the context sensitivity based on context recognition accuracy.

The adversary's attacking capability needs to choose the correct subset of regretting the sensed data. A formula gives the time n with the adversary actions as,

$$a^n{}_b = \{a^n{}_{a,1}, a^n{}_{a,E}\} \tag{2}$$

Here, $a^n{}_{b,e}$ denotes the *E*th sensor of the retrieved data. The adversary actions with limited power adversary given mathematically as,

$$\sum_{E} a^n{}_{b,j} \le L, 0 \le a^n{}_{a,j} \le 1, \forall E \tag{3}$$

Here, L denotes the adversary power limitations. Based on the limit $L \le E$, the third party can capture the sensed data. Hence this adversary is said to be an unlimited power adversary.

The behavior of the adversary in online attacking the user can be determined in a probabilistic manner, and it is given by,

$$Pb[R^n \mid a^n{}_h, a^n{}_a] = Pb[Wr^{n+1} \mid Wr^n, a^n{}_h, a^n{}_a] Pb[D^{n+1} \mid D^n] = Pb[Wr^{n+1} \mid a^n{}_h, a^n{}_a] Pb[D^{n+1} \mid D^n] \tag{4}$$

The offline attack in case of adversary based on the probabilistic manner is given by,

$$Pb[R^{n+1} \mid a^n{}_h, a^n{}_a] = Pb[D^{n+1} \mid D^n] \tag{5}$$

B. Proposed Context Aware Privacy Preservation Algorithm

The optimization problem gets converted into a linear programming problem to improve the convergence speed. To overcome the linear programming problem, the CAPP algorithm is introduced. It generates the active policy users and increases the service quality for context aware applications with user privacy.

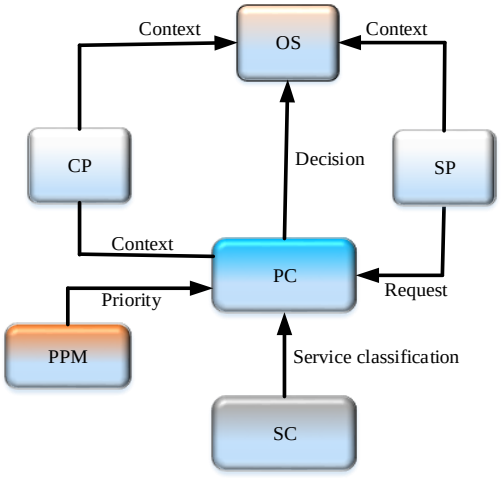


Fig. 2. Architecture of Privacy Aware.

Fig. 2 shows the architecture for privacy aware. The service provider gives a request to the PC about the priority. The PC does not request permission from the user directly and sends the requests through the PC module. The module provides the decision and notifies it to the OS that communicates with the SP consecutively. The user's privacy is stored in the privacy preference manager (PPM). It enables the user to set the privacy and sensitivity to context aware apps.

- Dividable.
- Not dividable.
- To be established.
- Cannot be established.

Dividable means the user feels comfortable for giving one's personal information. Not dividable denotes that the user feels insecure in sharing one's information. The data to be established depicts that when the user uses the application source for the first time; he sets the location permission to be dividable or cannot be dividable to the application. It cannot be established indicates that the user is unable to express to set the context priority that is sharable or not. The SC module describes the category of the service provider based on the context request and how it is divided among the SP. SP undergoes 3 stages: hopeful, hopeless, and examining. The hopeful SP is the one who asks only necessary information from the user. The hopeless SP is the one who asks for unnecessary that are not required for the adversary. The adversary is tested for hopeful or hopeless SP in the investigation category.

The PC module senses the user when the hopeless SP attacks the personal data. The deciding operation is done by three operation:

- Allow – allow access to context request.
- Deny – prevent access from context requests.
- Approximation- allow access to approximate the value based on the context request.

Algorithm For Context Aware Privacy Preservation
Step 1: Initialize service provider (SC) Step 2: Allow request for PC to preference Step 3: if, users data is sharable Allow PC to get service provider from SC Step 4: else, users data not sharable Send decision to OS End Step 5: if, SP is trusted Allow permission to access users data Send decision to OS. End Step 6: else, SP is not trusted Access deny Send decision to OS End Step 7: do, investigation and approximate range of SP Send decision to OS End Step 8: else, Allow request for PC to preference Step 9: if, SP is trusted Suggest to user to access the data Gets users decision from PC Send decision to OS End Step 10: else, Suggest not to user to access the data Gets users decision from PC Send decision to OS End Step 11: else, Suggest to user to set the approximate range Gets users decision from PC Send decision to OS End

The algorithm selects how to reveal a user's context while protecting their privacy. Even if an opponent knew the Markov model with associated probability matrices of emissions, they couldn't determine the original context from CAPP's output context sequence. Because privacy ensures a condition with which an adversary can never know the user when within the sensitive environment.

C. Mini Max Learning Algorithm

The minimax algorithm is a step by step process that aids the computer in working intelligently instead of not learning automatically. It mainly helps to improve the satisfaction threshold for the proposed approach.

The pair of the optimal policy is given by, $\phi^* = \{\phi^*_h, \phi^*_a\}$ for the game based context privacy is achieved by overcoming the convergence problem.

$$\tilde{U}^{n+1}(Wr) = (1-\beta^{n+1})\tilde{U}^n(Wr) + \beta^{n+1} G_t[s_h(r, a^n{}_h, a^n{}_a) + \lambda \tilde{U}^n(Wr')] \quad (6)$$

Based on the eqn (1), using the learning approach, the $\tilde{U}^{\phi^*}{}_h(Wr)$ is obtained, and this can be obtained using upgraded rule based on the Q-learning approach.

$$\phi^* = \arg\max_{\phi_h} \min_{\phi_a} \{s_h(r, a^{\phi^*}) + \lambda \sum_{Wr'} (Tr[Wr' / a^{\phi^*}] \tilde{U}^{\phi^*}(Wr'))\} \quad (7)$$

The algorithm of minimax learning is shown below:

Mini-max learning algorithm

Input: the stochastic game for context aware privacy given by, Ψ
Output:
// (i) Start
1. $n \leftarrow 0, Wr^n = 0;$
2. $\tilde{U}^n(Wr=0) \leftarrow 1, \tilde{U}^n(Wr=1) \leftarrow 1;$
3. Start the pair for policy ϕ^n : distributed based on uniform
$a^n{}_{h,j} = \frac{1}{P}, a^n{}_{aj} = \frac{L}{P}, \forall_j;$
// (ii) Recursion
4. Iterate
5. Choose the action pair $\{a^n{}_h, a^n{}_a\}$ according to ϕ^*;
6. Upgrade Wr^{n+1} after each user's taken into consideration as
$\{a^n{}_h, a^n{}_a\}$
7. Upgrade $\tilde{U}^{n+1}(Wr)$ convergence state notation as, based on equation (2).
8. Upgrade the optimized policy as ϕ^{n+1} based on the equation (1) with upgraded stated notations;
9. $n \leftarrow n+1;$
10. Until equalize

The learning rate is indicated as, $\beta^n \in [0,1)$ for the convergence of learning algorithm, must degrade the high time operation. Set $\beta^n = \frac{1}{n}\tilde{U}^{n+1}(Wr)$ that is used as an approximate value and updated continuously until it equalizes.

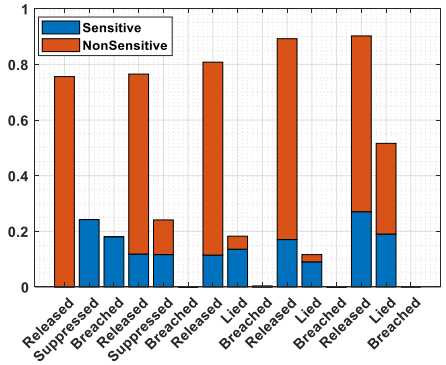
Algorithm 1 evaluates the learning algorithm in an equivalent state, denoted as, $\tilde{U}_h^{\phi^*}(Wr)$. Initially, set the equalization state values as 1 and make the uniform distribution among the players of each policy. After that, the equivalent state values are continuously repeated based on equations (1) and (2). This repetition helps to occur optimal policy among the policy pair.

IV. Results and Discussion

The context-aware privacy-preserving algorithm (dubbed CAPP) was developed and compared with currently present algorithms of privacies such as EfficientFake [8] and MaskSensitive, MaskIt (using the hybrid check) [7]. Basic method's MaskSensitive, which hides or suppresses all sensitive circumstances during the release of a non-sensitive one. The entire simulation was done using MATLAB. Initially, an effective context-aware privacy-preserving (CAPP) algorithm is introduced to address the linear programming issue. Then, minimax learning algorithm (MLA) is emphasized to optimize the policy users and to improve the satisfaction threshold. The performance measures such as privacy policy breaches, context sensitivity, satisfaction threshold, adversary power, and convergence speed for both online and offline attacks are investigated.

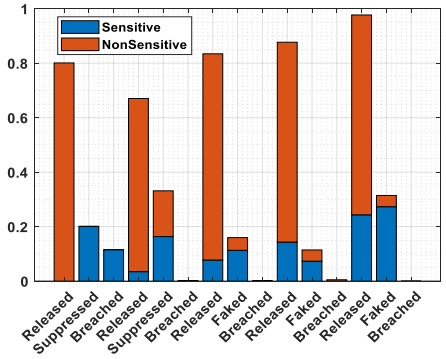
A. Analysis of Performance Metrics for the Proposed Model

To analyze the performance of the proposed method, a Markov chain is given to each user to train and assess protect the privacy context for every user. Because of the inadequacy of previous beliefs and the probability of emission, privacy may not be ensured while gathering the user's trace. To ensure user privacy is maintained, the privacy value, which is set to 0.1, is used as the simulation parameter. It was to be noted as a higher privacy parameter, and then lower will be user privacies guarding levels with additional actual sensitive information being revealed. Selecting sensitive environments may be done in one of two ways. Unless, sensitive circumstances pertaining to every user is selected randomly, referred to as sensitive, unless otherwise noted. Alternatively, for each user, a random place is selected with the greatest probability of prior as the user's house, marking that sensitive, dubbed home as sensitive. Because the expected amount in released real context was utility about privacy-preserving technique, normalized utility is utilized as evaluation, defined as the proportion of release actual context. It's worth noting that context-aware applications give better service when their utility is greater. Identically, the amount of sensitivity contextual is splitted within the user's context sequence, which got discontinued by the user's context sequence length in evaluating privacy breaches. Three Methods: MaskIt [6], CAPP [16] and Efficient Fake [17], and everyone guarantee no violation of privacy, according to the definition. Mask because of the lack of assumption for the presence of temporary connections across the user's context, Sensitive is unlikely to be able to ensure the desired privacy.



(a) MaskSensitive (b) MaskIt (c) NaiveFake
(d) CAPP (e) Proposed

Fig. 3. Comparison for Privacy Policy Breaches (Home as Sensitive).



(a) MaskSensitive (b) MaskIt (c) NaiveFake (d) CAPP
(e) Proposed

Fig. 4. Comparison for Privacy Policy Breaches (Sensitive as Random).

In the first example, comparisons are made for the privacy of CAPPs and MLA to violate the use of these alternative techniques. With certain conditions, three contexts were chosen by us randomly as sensitive about every user, whereas, in the other, each user's house is selected as sensitive. It's worth noting that a user's house has the greatest previous belief, indicating that the user must spend most of their time inside the house rather than elsewhere. In the preceding two instances, Fig. 3 and 4 shows released and repressed contexts in average proportions by different methods. All sensitive circumstances were surpassed by Mask Sensitive in entire instances, as can be seen in the images. Even though not every sensitive context was revealed within Mask Sensitive, opponents that understand the contexts of the Markov chain can predict around 40–60% sensitive contexts out of suppressed ones in both cases. The major reason is that the temporal connection across contexts gives an adversary enough information to conclude a greater post belief that can surpass correspondingly preexisting belief by privacy parameter. On the other hand, CAPP, EfficientFake, and MaskIt ensure that -privacy is maintained. Some sensitive and non-sensitive contexts are repressed and released in CAPP, EfficientFake, and MaskIt. CAPP also releases a higher percentage of genuine situations than MaskSensitive, MaskIt, or EfficientFake. MaskIt compromises less than 20% of Mask Sensitive's functionality to ensure anonymity, as seen in the numbers.

However, compared to Mask Sensitive, both EfficientFake and CAPP boost usefulness by about 20% while ensuring anonymity. The fundamental reason for this is that the new deception strategy makes it harder to antagonist in deriving posterior beliefs, allowing more genuine contexts to be released. Despite the fact that CAPP and EfficientFake were both formalized in linear programming problems, the proposed CAPP outperforms Efficient Fake techniques with both instances in terms of average utility. There are two primary reasons for this. The first difference is that in EfficientFake, the aim is to optimize emission probability solely. Still, with CAPP, the aim was to maximize the value of utility for a provided period of time. Secondly, Efficient Fake's space of resolution has shrunk significantly. The emission probability matrix' Shape in EfficientFake was reduced to a vectored representation, thereby significantly reducing the solution's precision in EfficientFake, resulting in lower utility than CAPP. On the other hand, CAPP does not shrink the solution space, allowing us to find a superior optimized solution.

The usefulness of the proposed CAPP is then compared to that of other techniques with various privacy settings ranging from 0.05 to 0.3. Separate sensitive settings are selected in the trials, just as in the previous ones: the sensitive environment for one person is their home, while the other is chosen at random. With the reduction in the privacy requirement, anticipate utility need to be rise. Fig. 5 and 6 shows that utility grows slowly as the number of people rise in both circumstances.

Moreover, the experimental analysis shows that, for similar privacy values, every solution executes in the best way within 2nd case. The context of random was designated sensitive, compared with the first situation, when the home was designated as sensitive. Because locations of every having greatest belief of prior were picked sensitive context in the first scenario in Fig. 5, the number of sensitive contexts was greater than the 2nd situation in Fig. 6, in which sensitive context was selected at random. CAPP and Efficient Fake should release more fake contexts in the first case to give identical privacy levels. However, when related to other methods, the proposed CAPP outperforms them all due to its close approximation of the problem's optimum solution.

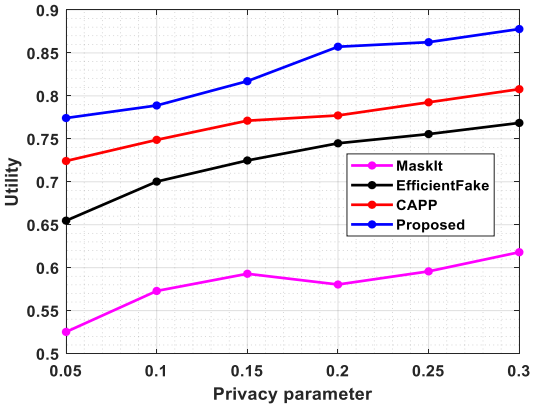


Fig. 5. Tradeoff for Privacy-utility (Home as Sensitive).

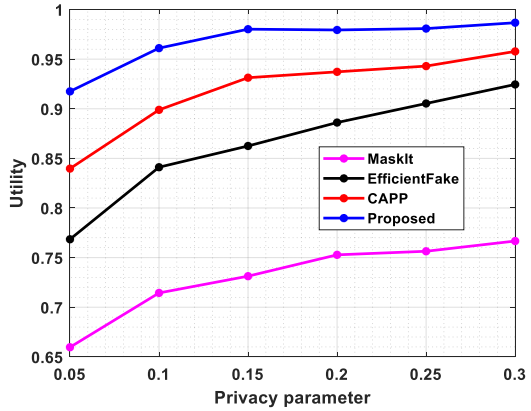


Fig. 6. Privacy-utility Tradeoff (Sensitive as Random).

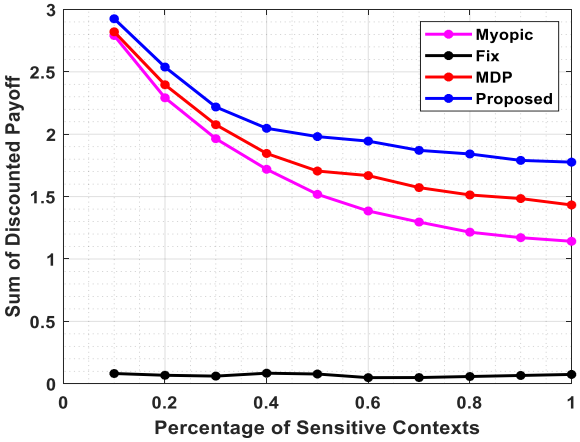


Fig. 7. Comparison of Sensitive Context and Payoff Discount.

Fig. 7 represents the comparison of sensitive context and the sum of the discounted payoff for an online attack. When the sensitive context percentage increases, the myopic strategy [18] gets highly decreased. The users of high sensitive contexts result in more privacy leakage. But this strategy shows high leakage in the case of the privacy policy. In the fixed strategy [19], the same percentage of sensitive context results in the same sum of the discounted payoff. However, this strategy shows poor outcomes because of its insecure privacy. It is due to the constant quality of service, and it controls the payoff discount in case of a fixed strategy. In the case of the MDP approach [20], it is the same as the myopic strategy.

However, this approach works more efficiently in the case of privacy preservation than the myopic strategy. But, this method shows a lie outcome based on context aware privacy preservation. The proposed model shows better results in protecting the privacy of the user. By increasing the percentage of the sensitive context to 1, the sum of the payoff discount gets very much increased to 2.9 because of using an optimal algorithm with cloud computation.

Fig. 8 compares the satisfaction threshold and sum of the discounted payoff. The satisfaction threshold is compared with the existing application based on the sum of discounted payoff. From the graph, it is shown that if sum of the discounted payoff gets lower, the satisfaction threshold gets very much lower. If the satisfaction threshold gets increased, the quality of service gets lower. The existing approach results in low-quality service by comparing the proposed model with the myopic strategy. If the service quality decreases, it is harder to better accuracy in the outcome. Hence the satisfaction threshold must be lower to prevent the loss of leakage in privacy. In the case of the MDP approach, there attains a better quality of service. However, this method shows some drawbacks in hiding the information from the third party. The proposed model shows better privacy protection as the satisfaction threshold is only 0.15.

Fig. 9 represents the different context sensitivity based on optimal police based on online policy. Here, a, b illustrated in the graph denotes the released and leaked data. With the smaller context sensitivity of 0.25, the optimal policy achieves 1. When the context sensitivity becomes higher by about 0.87, the optimal policy attains a negligible value. In the case of smaller context sensitivity, the service quality variance improves, and vice versa, the loss of privacy dominates. Suppose both a and b go down, the context sensitivity increases. Due to this, the user chooses a more optimized strategy to protect their privacy efficiently. From the graph, it is clear that if the satisfaction threshold increases, the context sensitivity decreases. Suppose the user receives only low-quality service if the threshold becomes lower. Understanding the satisfaction threshold is considered an important parameter while developing context-aware privacy protection approaches.

Fig. 10 illustrates the different adversaries with optimal policies for the offline attack. Here, L denotes the adversary power of the privacy policy. Considering, at L=1, attains poor adversary power due to high leakage of privacy of the user. In myopic strategy, the discounted payoff with different adversary power is higher than the proposed work. For efficient usage of context aware applications, the sum of discounted payoff should be too low. From the graph, it is shown that the sum of discounted payoff gets degraded, resulting in no leakage. In existing approaches, compared with the limited adversary power, the performance of the adversary power with unlimited power gets very worse. Mainly, the adversary with unlimited power occurs more leakage, and hence the user selects another strategy to protect their privacy.

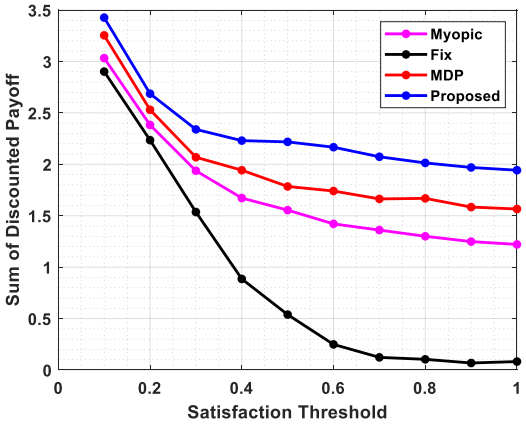


Fig. 8. Comparison of Satisfaction Threshold and Payoff Discount.

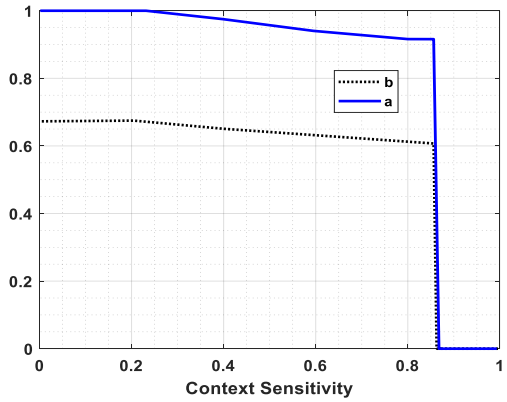


Fig. 9. Different Context Sensitivity based on Optimal Policies.

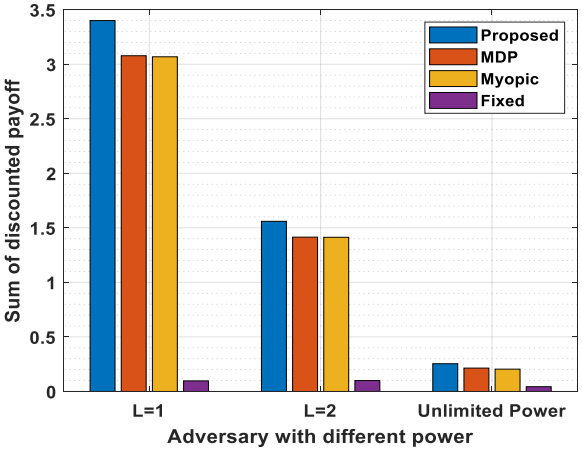


Fig. 10. Different Adversaries with Optimal Policies.

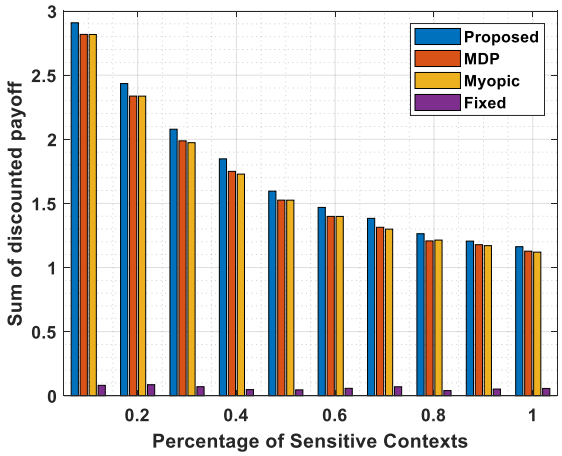


Fig. 11. Comparison of Sensitive Context and Payoff Discounts.

Fig. 11 illustrates the comparison of sensitive context and payoff discounts. As per the graph, when the sensitive context percent increases, the discounted payoff's sum gets degraded. This denotes that sensitive users have to use the more encrypted forms to preserve user privacy. When the sensitive context percent increases in myopic strategy, the discounted payoff's sum gets degraded slowly. But this approach does not show better accuracy in preserving the user's privacy under offline attacks. In fixed strategy, the sum of discounted payoff gets diminished gradually with an increase in sensitive contexts. But this approach uses high complexity in protecting one's privacy from the third party. The MDP approach is also the same as the other existing approach because of the lack of new approaches to protect the privacy of the user. The proposal shows a better outcome because it performs effectively in preserving the privacy of the user.

Fig. 12 compares the satisfaction threshold and sum of the discounted payoffs. As per the graph, when the satisfaction threshold (accuracy) increases, the sum of the discounted payoff gets decreases slowly in the case of myopic strategy. This shows that this strategy is not suitable for preserving the privacy of the user due to low service quality. In the case of fixed strategy, the sum of discounted payoff decreases significantly with increased accuracy. This approach shows a lack of service quality due to the absence of a slow encryption process. Considering the MPD approach, the sum of the discounted payoff gets decreased with an increase in accuracy but is not efficient due to a lack of preserving privacy from the third party. When the sum of the discounted payoff gets decreased, the accuracy is very high. This shows that the proposed method with cloud computing helps the user protect their privacy effectively.

Fig. 13a, 13b, 13c shows the sum of discounted payoff at L=1, L=2 and with unlimited power. As per the graph, the discounted payoff gets reduced when the adversary's power gets increased. It is due to the increase of L, and the adversary can access more data. Hence it is influenced by the adversary to attack the user successfully. Considering the releasing data with less granularity shows the lower service quality or the user should depend on the same approach to protect user's privacy. This leads to more loss in privacy of the user and less payoff. The existing approaches like myopic, fixed and MDP approach more leakage in the privacy of user due to low satisfaction threshold. The proposed method shows good encryption in protecting the user's privacy because of high satisfaction threshold.

Fig. 14 illustrates the cumulative distribution function (CDF) of various iterations in order to learn the optimal policy of the reality mining dataset. The operating speed of the proposed work is analyzed for 220 iterations. For the MPD process, the convergence speed is analyzed with 10^5 iterations. This shows that the proposed algorithm has a higher convergence speed than the MDP process. The proposal algorithm's equivalent state value helps reduce the high dimensionality for learning the process efficiently.

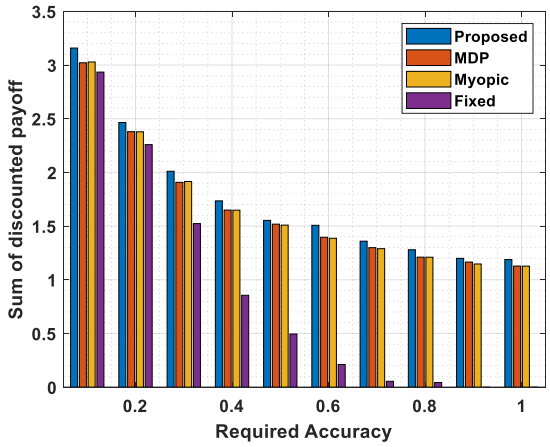
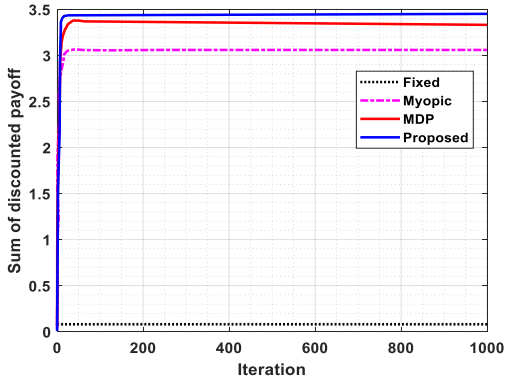
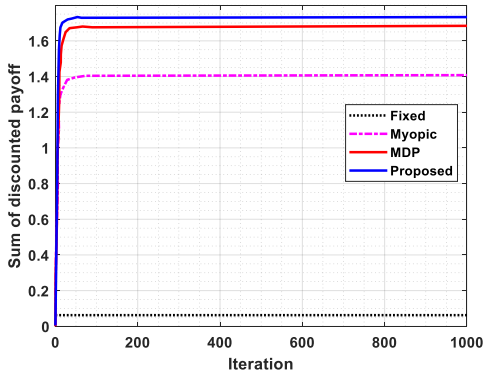


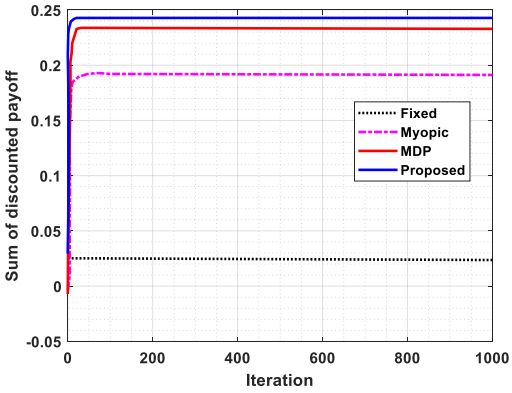
Fig. 12. Comparison of Satisfaction Threshold and Payoff Discounts.



(a)



(b)



(c)

Fig. 13. Comparison of Payoff Discount and for Varying Iteration. (a) Sum of Discounted Payoff at L=1. (b) Sum of Discounted Payoff at L=2. (b) Sum of Discounted Payoff for Unlimited Power.

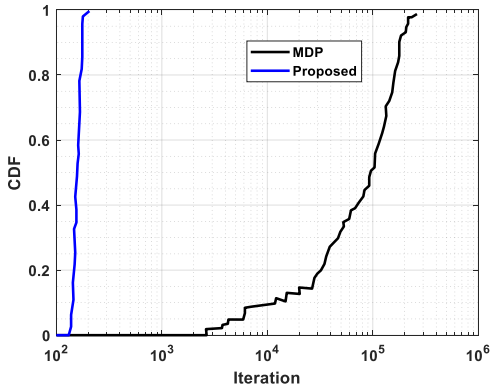


Fig. 14. Convergence Speed based on CDF.

B. Discussion

This research mainly focuses on developing a novel approach for preventing data leakage in context aware applications for smart phones using cloud computing. An effective context aware privacy preserving (CAPP) algorithm is introduced to address the linear programming issue. Minimax learning algorithm (MLA) is emphasized to optimize the policy users and improve the satisfaction threshold. To preserve the privacy of the user, the cloud computing approach is evaluated. It mainly creates a firewall between the adversary and the user. The performance of the proposed work is compared with existing approaches like Naivefake, MaskIt, EfficientFake and CAPP models. But this method suffered due to multiple drawbacks. To protect the privacy of the user is not an easy task. Many issues like the third party intrude and cracking may occur due to the lack of advancements in sensor networks.

In the context-aware implicit authentication of smartphone users based on the multi-sensor behaviour, this method was suffered due to leakage of the privacy to the third party. EER attained was about 0.0071%. In the method towards the privacy protection in context aware environment; however, this method suffered due to high optimization problems in context aware scalable authentication (CASA). However, this method suffered due to high attacks from the adversary. FPR) attained was about 1.5%. An aware access control framework for software services (PO-SAAC) was introduced in the purpose-oriented situation. However, this method suffered due to high computational complexity and increased memory size. The memory size utilized about 1600 KB based on the response time in the secure and trustworthy context management for context aware security and privacy in the IoT (SETUCOM). However, this method suffered due to insecurity of the user's privacy and it's highly occurs optimization problems. The overall time taken to protect the information is about 1200ms. The evaluation of the proposed work based on privacy policy breaches, context sensitivity, satisfaction threshold, adversary power, and convergence speed for both online and offline attacks are investigated and compared with traditional approaches. Because of its outstanding performance avoids leakage and privacy loss in smartphones because of its outstanding performance.

V. Conclusion

The challenge of context-aware privacy preservation for cellphones is addressed in this study. The validity and optimality is verified by theoretical analysis by formalizing the problem of contextual privacy preservation as an optimization problem. To further speed up the computation, an effective, near-optimized strategy involving the linear programming problem was developed. A context-aware privacy preserving algorithm (CAPP) was presented due to the linear programming issue being solved. The experimental analysis proves that the suggested CAPP provides much more value than existing techniques while respecting the user's δ-privacy policy via thorough experimental evaluations on actual mobility traces. A cloud-based approach is introduced in this work to protect the privacy of the user from a third party. In addition to this, a minimax learning algorithm is emphasized for improving the accuracy of the context aware application and improving the optimal policy of the users. The performance measures obtained are compared with existing approaches in terms of privacy policy breaches, context-sensitivity, satisfaction threshold, adversary power, and convergence speed for online and offline attacks.

A. Future Scope

An exciting future project would be the development of an online context released judgment system that can generate faster and most effective judgments depending just on the user's current context while maintaining anonymity. Because this research focuses on preserving privacy for a single user, a future project will provide a privacy preservation technique that considers user interactions, given that people have group mobility.

Acknowledgment

I sincerely thank Thyagaraju G. S, R H Goudar, for their guidance and encouragement in carrying out this research work.

References

[1] T. Hussain, and R. Alawadhi, "A Privacy Protection System in Context-aware Environment The Privacy Controller Module," Proceedings of the 22nd International Conference on Information Integration and Web-

Based Applications & Services, 2020.

[2] J. Shu, R. Zheng, and P. Hui, "Cardea: Context-aware visual privacy protection for photo taking and sharing," Proceedings of the 9th ACM Multimedia Systems Conference, 2018.

[3] W. Ali, R. Kumar, Z. Deng, Y. Wang, and J. Shao, "A federated learning approach for privacy protection in context-aware recommender systems." The Computer Journal vol. 64, no. 7, pp. 1016-1027, 2021.

[4] L. Gao, T.H. Luan, B. Gu, Y. Qu, and Y. Xiang, "Context-Aware Privacy Preserving in Edge Computing." In Privacy-Preserving in Edge Computing, Springer, Singapore, pp. 35-63, 2021.

[5] Y. Zhang, J. Pan, L. Qi, and Q. He, "Privacy-preserving quality prediction for edge-based IoT services." Future Generation Computer Systems vol. 114, pp. 336-348, 2021.

[6] J. Al-Muhtadi, K. Saleem, S. Al-Rabiaah, M. Imran, A. Gawanmeh, and J.J.P.C. Rodrigues, "A lightweight cyber security framework with context-awareness for pervasive computing environments." Sustainable Cities and Society vol. 66, pp. 102610, 2021.

[7] V. Stephanie, M.A.P. Chamikara, I. Khalil, and M. Atiquzzaman, "Privacy-preserving location data stream clustering on mobile edge computing and cloud." Information Systems vol. 107, pp. 101728, 2022.

[8] A. A. Ahmed, "A privacy-preserving mobile location-based advertising system for small businesses." Engineering Reports vol. 3, no. 11, pp. e12416, 2021.

[9] T. N. Phan, et al, "A context-aware privacy-preserving solution for location-based services," 2018 International Conference on Advanced Computing and Applications (ACOMP). IEEE, 2018.

[10] E. Ezhilarasan and M. Dinakaran, "Privacy preserving and data transpiration in multiple cloud using secure and robust data access management algorithm." Microprocessors and Microsystems vol. 82, pp. 103956, 2021.

[11] R. Wang and D. Tao, "Context-aware implicit authentication of smartphone users based on multi-sensor behavior," IEEE Access, vol. 7, pp. 119654-119667, 2019.

[12] R. Alawadhi and T. Hussain, "A Method Toward Privacy Protection in Context-Aware Environment," Procedia Computer Science, vol. 151, pp. 659-666, 2019.

[13] Y. Wan, Y. Qu, L. Gao, and Y. Xiang, "Privacy-preserving blockchain-enabled federated learning for b5g-driven edge computing." Computer Networks vol. 204, pp. 108671, 2022.

[14] T. Ghosh, A. Roy, S. Misra, and N.S. Raghuwanshi, "CASE: A context-aware security scheme for preserving data privacy in IoT-enabled society 5.0." IEEE Internet of Things Journal 2021.

[15] T. Sylla, M.A. Chalouf, F. Krief and K. Samaké, "SETUCOM: Secure and Trustworthy Context Management for Context-Aware Security and Privacy in the Internet of Things," Security and Communication Networks, vol. 2021, 2021.

[16] S. Meng, L. Qi, Q. Li, W. Lin, X. Xu, and S. Wan, "Privacy-preserving and sparsity-aware location-based prediction method for collaborative recommender systems." Future Generation Computer Systems vol. 96, pp. 324-335, 2019.

[17] H. Vahdat-Nejad, S. Izadpanah and S. Ostadi-Eilaki, "Context-aware cloud-based systems: design aspects," Cluster Computing, vol. 22, no. 5, pp. 11601-11617, 2019.

[18] X. Ding, R. Lv, X. Pang, J. Hu, Z. Wang, X. Yang, and X. Li, "Privacy-preserving task allocation for edge computing-based mobile crowdsensing." Computers & Electrical Engineering vol. 97, pp. 107528, 2022.

[19] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu and M.S. Hossain, "PPCS: An Intelligent Privacy-Preserving Mobile-Edge Crowdsensing Strategy for Industrial IoT," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10288-10298, 2020.

[20] B. D. Deebak, and A-T. Fadi, "Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements." Journal of Information Security and Applications vol. 58, pp. 102749, 2021.